Cyber- Physical Robustness Enhancement Strategies for Demand Side Energy Systems

Author:
Zhang, Fangfei

Publication Date:
2022

DOI:
https://doi.org/10.26190/unsworks/1957

Cyber- Physical Robustness Enhancement Strategies for Demand Side Energy Systems

Fangfei Zhang

B.E. M.E.

A thesis in fulfillment of the requirements for the degree of Doctor of Philosophy

School of Electrical Engineering and Telecommunications

Faculty of Engineering

July 2021

Thesis submission for the degree of Doctor of Philosophy

Thesis Title and Abstract | Declarations | Inclusion of Publications Statement | Corrected Thesis and Responses

Thesis Title

Cyber-Physical Robustness Enhancement Strategies for Demand-Side Energy System

Thesis Abstract

Driven by the ongoing increasing power demand and extreme weather days caused by the climate change, energy issues have become essential challenges to achieve s ustain development for human beings. The large-scale deployment of Advanced Metering Infrastructure (AMI) and two-way communication facilities enable the multi-sourc e data can be monitored and collected in real time in demand side, and makes the grid system evolved into a strong interaction and highly coupled cyber- physical syste m (CPS). As a comprehensive energy participant, demand side plays an important role in the integrated CPS energy system, which affects energy production, transportati on, distribution, storage, distribution, trading and many other links. The robustness of CPS demand-side system is the basis of the reliable operation of integrated CPS ene rgy system. The thesis contributes to the robustness of CPS demand-side energy system.The overview of state-of -the -art, and analyses of the system robustness require ments is conducted.There are four aspects considerations for system robust.First,the outage management in two levels is studied. A resilient energy management system on communities level is proposed by scheduling co-ordinately the battery energy storage system and energy consumption of houses/units; Moreover, a hierarchical resilie nt energy management system by fully considering the appliance-level local scheduling; with considering the customer satisfactions and life style preference sufficiently; T hirdly, a complex multi-hop wireless remote metering network model for communication layout in CPS demand side was proposed, which decreased the number and locati ons of data center in demand side and reduce the security risk of communication and the infrastructure cost of the smart grid for residential energy management. Also, a n ovel evolutionary aggregation algorithm (EAA) was proposed. Finally, the system facing virus attacks has been studied in this paper. A novel risk management approach to confront viruses in the system with numerous network nodes is proposed. It is a trade-off scheme for double- virus problem, which enable to determine the allocation of an tivirus programs to avoid system crash and achieve the minimum potential loss. A DOWNHILL algorithm is proposed to address appropriate allocation strategy under the ti me evolution of the expected state of the network.

Thesis submission for the degree of Doctor of Philosophy

Thesis Title and Abstract | Declarations | Inclusion of Publications Statement | Corrected Thesis and Responses

ORIGINALITY STATEMENT

COPYRIGHT STATEMENT

AUTHENTICITY STATEMENT

Thesis submission for the degree of Doctor of Philosophy

Thesis Title and Abstract | Declarations | **Inclusion of Publications Statement** | Corrected Thesis and Responses

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in the candidate's thesis in lieu of a Chapter provided:

- The candidate contributed **greater than 50%** of the content in the publication and are the "primary author", i.e. they were responsible primarily for the planning, execution and preparation of the work for publication.
- The candidate has obtained approval to include the publication in their thesis in lieu of a Chapter from their Supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis.

☑ The candidate has declared that **some of the work described in their thesis has been published and has been documented in the relevant Chapters with acknowledgement**.

A short statement on where this work appears in the thesis and how this work is acknowledged within chapter/s:

> 1.Fangfei. Zhang, F. Luo, Z.Y.Dong, G. Ranzi, and Yan Xu" Resilient energy management for residential communities under grid outages," 2019 9th International Conference on Power and Energy Systems (ICPES2019)
> 2.Fangfei. Zhang, F. Luo, Z.Y.Dong, G. Ranzi, "Hierarchically Resilient Energy Management- Scheme for Residential Communities under Grid Outages", IET Smart Grid. Vol. 3, Iss. 2, pp. 174-181.
>
> My thesis studies the Cyber-Physical robustness enhancement strategies for the demand-side energy system, these two papers are parts of robust management under the outage environment. The established models and simulation results are used in my thesis.

Candidate's Declaration

I declare that I have complied with the Thesis Examination Procedure.

ACKNOWLEDGEMENT

After almost four years of hard work, I am finally about to complete my PhD journey. The Covid-19 outbreak has caused panic all over the world, and the period between 2020 and 2021 has been a really tough time for individuals. I was no exception; Australian travel bans meant I had to complete lots of work at home. As such, I sincerely appreciate all the people who helped me to finish my doctoral study.

Firstly, and most deeply, my thanks go to my primary supervisor, Professor ZhaoYang Dong. He has profound professional knowledge, serious scientific attitude, rigorous academic spirit, and excelsior style. He has not only set an example for me in my lifelong learning but has also given me a model for life. I would like to thank him for giving me the opportunities to participate in research programs. These allowed me to learn both hands-on industrial practices and research skills.

In addition, I would also like to show my profound appreciation for my co-supervisor, Dr. Fengji Luo, whose scientific thinking and serious academic attitude helped give my research, studies—and life in general—some perspective that allowed me to cultivate my thinking. Dr. Luo was a great help throughout my Ph.D. journey.

My thanks, too, go to another co-supervisor, Dr. Guo Chen, who encouraged me greatly during my research work and always helped me when I encountered any difficulty. Furthermore, I want to acknowledge Dr. Ziyuan Tong for her selfless help in my study. She has been one of the best mentors I have worked with in my life.

Finally, I give great appreciation to my parents and friends with whom I have spent so much cherished time during my life. They have been my biggest motivation during my research study. I thank my parents for supporting my study, both financially and psychologically. My best friends, Danlin Li, Yuxuan Wang, Zhiheng Zhao, Jichao Bi and Shunxiang Wu, accompanied me through my study overseas, and gave me a lot of support in study and life. Because of them, I didn't feel alone while I was abroad.

The period of my Ph.D. has undoubtedly been the most meaningful and essential time of my life. I feel very honored to have studied at the University of New South Wales. It is undoubtedly the best university and provides lots of help for its students.

I love my doctoral life!

LIST OF PUBLICATIONS

The following publications as the major Ph.D. research results for this candidate:

Fangfei Zhang, Fengji Luo, Zhao Yang Dong, Gianluca Ranzi, and Yan Xu, "Resilient energy management for residential communities under grid outages," in *Proc. 2019 9th International Conference on Power and Energy Systems (ICPES)*, 2019, pp.1-6, doi: 10.1109/ICPES476393.2019.9105455.

Fangfei Zhang, Fengji Luo, Zhao Yang Dong, and Gianluca Ranzi, "Hierarchically resilient energy management scheme for residential communities under grid outages," *IET Smart Grid*, vol.3, no. 2, pp. 174-181, April 2020, doi: 10.1049/iet-stg.2019.0150.

Shunxiang Wu, **Fangfei Zhang** and Danlin Li, "User-centric peer-to peer energy trading mechanisms for residential microgrids," 2018 2nd *IEEE Conference on Energy Internet and Energy System Integration (E12),* 2018, pp. 1-6, doi:10.1109/E12.2018.8582548.

Fangfei Zhang, Bozhi Wang, Danlin Li. Li, Fengji Luo, and Zhao Yang Dong, "A secure distributed energy trading mechanism based on innovative smart contract," *IEEE Transactions on Power System*, under review

Jichao Bi, **Fangfei Zhang**, A. Dorri, C. Zhang and C. Zhang, "A risk management approach to double-virus tradeoff problem," *IEEE Access*, vol. 7, pp.144472-144480, 2019, doi: 10.1109/ACCESS.2019.2944985.

Hui Miao, Guo Chen, **Fangfei Zhang**, and Zhiheng. Zhao, "Evolutionary aggregation approach for multi-hop energy metering in smart grid for residential energy management", *IEEE Transactions on Industrial Informatics*, vol.17, no. 2, pp. 1058-1068, Feb. 2021, doi: 10.1109/TII.2020.3007318.

Bingcheng Chen, **Fangfei Zhang**, Zhiheng Zhao, Guo.Chen, Zhaoyang Dong, "Cybersecurity in home energy management system, challenges and solutions," *Special Issues in Electronics*, submitted.

It is acknowledged that permission from the copyright owners have been obtained for Fangfei Zhang to use and for refining with the suggestions of the co-authors of those published papers documented in this thesis. Fangfei Zhang is responsible for design and validation of the developed approaches for papers whereas Fangfei Zhang is the primary author. The papers quoted in this thesis whose copyright belongs to a third-party are reproduced and the copyrights have been obtained to use in this thesis.

ABSTRACT

An integrated Cyber-Physical System (CPS) system realizes the two-way communication between end-users and power generation in which customers are able to actively re-shaped their consumption profiles to facilitate the energy efficiency of the grid. However, large-scale implementations of distributed assets and advanced communication infrastructures also increase the risks of grid operation. This thesis aims to enhance the robustness of the entire demand-side system in a cyber-physical environment and developing comprehensive strategies about outage energy management (i.e., community-level scheduling and appliance-level energy management), communications infrastructure development and the cybersecurity controls that encounter virus attacks. All these aspects facilitate the demand-side system's self-serve capability and operational robustness under extreme conditions and dangerous scenarios.

The research that contributes to this thesis is grouped around and builds a general scheme to enhance the robustness of CPS demand-side energy system with outage considerations, communication network layouts, and virus intrusions.

Under system outage, there are two layers for maximizing the duration of self-power supply duration in extreme conditions. The study first proposed a resilient energy management system for residential communities (CEMS), by scheduling and coordinating the battery energy storage system and energy consumption of houses/units. Moreover, it also proposed a hierarchical resilient energy management system (EMS) by fully considering the appliance-level local scheduling. The method also takes into account customer satisfaction and lifestyle preferences in order to form the optimal outcome.

To further enhance the robustness of the CPS system, a complex multi-hop wireless remote metering network model for communication layout on the CPS demand side was proposed. This decreased the number and locations of data centers on the demand side

and reduced the security risk of communication and the infrastructure cost of the smart grid for residential energy management. A novel evolutionary aggregation algorithm (EAA) was proposed to obtain the minimum number and locations of the local data centers required to fulfil the connectivity of the smart meters.

Finally, the potential for virus attacks has also been studied as well. A trade-off strategy to confront viruses in the system with numerous network nodes is proposed. The allocation of antivirus programs and schemes are studied to avoid system crashes and achieve the minimum potential damages. A DOWNHILL-TRADE OFF algorithm is proposed to address an appropriate allocation strategy under the time evolution of the expected state of the network. Simulations are conducted using the data from the Smart Grid, Smart City national demonstration project trials.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CPS	Cyber-Physical System
PMU	Phasor Measurement Unit
AMI	Advanced Metering Infrastructure
CEMS	Community Energy Management System
EMS	Energy Management System
EAA	Evolutionary Aggregation Algorithm
HEMS	Home Energy Management System
BESS	Battery Energy Storage System
CHP	Combines Heat and Power
AC	Alternating Current
MPC	Model Predictive Control
DRE	Demand Response Event
TOU	Time-of-Use
MDMS	Meter Data Management System
SM	Smart Meter
PLC	Power Line Communication
GPRS	General packet Radio Service
HAN	Home Area Network
WAN	Wide Area Network

NAN	Neighbor Area Network
NILM	Non-Invasive Appliance Load Monitoring
HMM	Hidden Markov Model
FSM	Finite State Machine
MLD	Mixed Logic Dynamic
LTL	Linear Time Temporal Logic
NCS	Network Control System
SVS	Support Vector Method
PSO	Particle Swarm Optimization
RTU	Remote Terminal Unit
FTI	Feeder Terminal Unit
V2H	Vehicle-to-Home
ICTs	Intelligent Communication Technologies
PEV	Plug-in Electric Vehicle
ICS-EM	Inexact Community-Scale Energy Model
SI	Susceptible-Infected
DASD	Double-Antivirus-Strategy Development
DT	DOWNHILL- TRADEOFF Algorithm
WSN	Wireless Sensor Network
PDV	Packet Delay Variance
DOS	Denial of Service

SMC	Secure Multi Parties Computing
MPC	Model Predictive Control
MDMS	Meter Data Management System
RF	Radio Frequency
GPRS	General Packet Radio Service
HMM	Hidden Markov Model
NCS	Networked Control System
FTU	Feeder Terminal Unit
ICS-EM	Inexact Community-Scale Energy Model
SVM	Support Vector Machine
IEDs	Intelligent Electronic Devices

LIST OF NOMENCLATURE

Sets	
Ω_n^{CA1}	Set of the non-interruptible, controllable appliances of the *n*th house;
Ω_n^{CA2}	Set of the interruptible, controllable appliances of the *n*th house;
Ω_n^{CA3}	Set of the controllable appliances of the *n*th house that are with adjustable; power consumption;
S_s	Transmission scope of each node of the s house;
Fi	Multiple node clusters of the *i* cluster
N_g	Set of residential nodes
N_m	Set of local data centers
DC	Set of processing of data collections
CD	Set of processing of data outputs
Constants	
N	Number of houses in the community;
T^{oh}	Total number of time intervals of the outage horizon;
T^{lsh}	Total number of time intervals of the life scheduling horizon;
Δt	Duration of scheduling time interval (hour);
$L_{n,t}^{dsr}$	Originally desired load of the *n*th house at time *t* (kW);
$L_{n,t}^{sch}$	Load of the *n*th house at time *t* scheduled by the CEMS (kW);
$P^{bess,rate}$	Forecasted Photovoltaic (PV) solar power of the *n*th house at time *t* (kW);
$P^{bess,rate}$	Rated power of the BESS (kW);

$E^{bess,rate}$	Energy capacity of the BESS (kWh);
λ_n^{ls}	Load shifting threshold of the *n*th house (kWh);
λ^{lr}	Load reduction threshold of the *n*th house (kWh);
$E_{a,n}^{req}$	Required energy consumption of the appliance *a* of the *n*th house to accomplish its task (kWh);
$P_{a,n}^{rate}$	Rated power of the controllable appliance *a* of the *n*th house (kW);
$L_{n,t}^{mr}$	Must-run load of the nth house at time *t* (kW);
$\delta_{a,n}^{begin}, \delta_{a,n}^{end}$	Begin and end time of the allowable operation time ranges of the controllable appliance *a* of the *n*th house;
$SOC^{\min}$	Lower SOC limit of the BESS (%);
$SOC^{\max}$	Upper SOC limit of the BESS (%);
η^c, η^l	Charging loss (%) and leakage loss factors (%/month) of the BESS;
$P_{a,n}^{\lim}$	Lowest power consumption limit of the controllable appliance *a* ($a \in \Omega_n^{CA3}$) of the *n*th house (kW);
$P_{a,n}^{dsr}$	Desired power consumption of the controllable appliance *a* ($a \in \Omega_n^{CA3}$) of the *n*th house (kW);
α	Penalty factor for balancing the upper and lower scheduling models;
$\tau_{\min,a}^{on}, \tau_{\min,a}^{off}$	Minimum online and offline limits of the controllable appliance *a* at time *t* (hour);
g_k	Geometry location of the *k*th residential node;
m_{n}	Number of local data center;
	Number of population;
	Number of initial solution in generation;
g_k	The *k*th residential node’s geometry location
	Time computational complexity is represented;

θ1	Node n without Virus α may tainted by tainted neighbor m with the θ1 constant rate
θ2	Node n without Virus β may tainted by tainted neighbor m with the θ2 constant rate
Variables	
$s_{a,n,t}$	Status of the controllable appliance *a* of the *n*th house at time *t*: 1-ON, 0-OFF;
$P_{a,n,t}^{ca}$	Power consumption of the controllable appliance *a* of the *n*th house at time *t* (kW);
P_t^{bess}	Charging/discharging power of the community BESS at time *t* (kW): Negative-charging, Positive-discharging;
E_t^{bess}	Remaining energy in the BESS at time *t* (kWh);
SOC_t	SOC of the RBESS at time *t*;
$\tau_{a,t}^{on}$ $\tau_{a,t}^{off}$	Accumulated online and offline durations of controllable appliance *a* at time *t* (hour);
$\mathbf{L}_n^{sch}$	Vector of scheduled power consumption of the *n*th house;
$\mathbf{P}_n^{ca}$	Power consumption matrix of the controllable appliances of the *n*th house;
	Status of node m at time n of Susceptible;
	Status of node m at time n of *α*-Infected;
	Status of node m at time n of *β*-Infected;
	Status of node m at time n of Both-Infected;
	Specific strategy to implement antivirus program α;
$D(k_1^F)$	Total corresponding damage;
V1	Each node caused economic loss per unit time when only Virus *α* infected;
V2	Each node caused economic loss per unit time when only Virus *β* infected;
M1	Man-days effort by implementing antivirus strategy *α*;

M2	Man-days effort by implementing antivirus strategy β;
Tα	Completed time of implementing antivirus strategy α for Virus α;
Tβ	Completed time of implementing antivirus strategy β for Virus β;
m_n	The number of local data center
k	Total fix program available
M_{ij}	Communication performance between node i and j
SPT_{ij}	Possibility of communication delay among node i and node j.
SPI_{ij}	Possibility of communication outage among node i and node j.
SPP_{ij}	Possibility of transmission error among node i and node j.

CHAPTER 1

Introduction

1.1 Problem Statement

Energy grids (physical systems) are highly integrated with advanced communication infrastructures and information technology (cyber-layer) resulting in a sophisticated Cyber-Physical System (CPS). The large-scale intermittent distributed access of new energy sources, the application of energy storage technology, and the wide participation of flexible and controllable loads, bring a series of new challenges to the operation, planning, and control of the modern grid system. The increased implementation of information techniques is expected to facilitate the robustness, reliability and efficiency of the CPS energy system through the installation of complicated monitoring and controlling management, such as a modern demand energy management system. Moreover, the advanced communication and information facilities of the CPS have evolved from traditional isolated construction into a more networked and open version of the energy grid, where the system has become more vulnerable to cyber-invasion, which leads to physical system shutdown. As such, power system robustness continues to attract increasing attentions to determine the operation and resilience of the system.

In the 21st Century, the concept “Smart Grid” was introduced and then the International Council on Large Electric Systems (ICLES) further proposed the concept of an active distribution network [1] in 2008. The large-scale deployment of Advanced Metering Infrastructure (AMI) and two-way communication facilities, which enable the multi-source data (state data of energy equipment, environmental meteorological data, various kinds of information of end users, topology and operation data of distribution network, etc.) to be monitored and collected in real time on the demand side, and makes the grid system evolved into a strong interaction and highly coupled Cyber- Physical System (CPS), where extracting data from multi-source big data effectively and making decisions driven by the data [2]. In the CPS environment, the connections of intelligent terminal equipment and the developed power communication technologies as well as the advanced measurement architecture make observation and control of the demand side easy. The power CPS not only provides the technical supports of multi-communication transmission and multi-information interaction for the demand management, but also offers the possibility of active response control for the demand side [3].

The integrated CPS system realizes the interactions of users to users, users to energy and information communication between systems. As a comprehensive energy participant, demand side plays an important role in the integrated CPS energy system, which affects energy production, transportation, distribution, storage, distribution, trading and many other links. In the CPS power system, the pattern of energy supply and demand has undergone profound changes, where the flexibility and adaptability of energy supply and balance is enhanced, and the energy efficiency is improved through demand management.

The existence of Phasor Measurement Unit (PMU) and a large number of sensing devices in CPS demand side also means that there is a need for more information transfer and processing than that of traditional power systems. Consequently, a CPS grid tends to be more dependent on the computing systems and communication networks, and the increasing number of external connections introduces more risks to system instability. They also present an increased dependency on cyber resources which could be vulnerable to attacks. Additionally, the extensive deployment of intelligent electronic devices (IEDs) to monitor and control a power system from a remote-control center based on information and communications technology (ICT) further introduced risks for potential cyber intrusions. The vulnerability of such system also become a serious concern. The CPS system is more at risk from cyberattacks than the traditional grid, therefore, the robustness of the power system is essential for whole system operation. For instance, there were three large power crises caused by extreme weather conditions/storms in Texas, the USA. More than 4.5 million homes and businesses suffered the power outages, and more than 150 people were killed in these events. Fig.1.1 shows the major power blackouts and their primary causes in USA between 2000 and 2016.

Clearly, the robustness of CPS demand-side systems plays an essential role, and a comprehensive strategy is needed to enhance the reliability of physical equipment and cyber security. Based on [4], when the physical equipment is subjected to external factors such as natural environment, various operating conditions, and human factors, the whole CPS reliability maybe decreased. In addition, the CPS system may also be affected by network attacks. Compared with a physical attack of the power system, network attack has the characteristics of low cost, high concealment and large scope. Once successful, the consequences can be serious [5]. For example, at the end of 2015, Ukraine's power grid suffered from malicious network attacks, and the implantation of computer viruses made the control servers lose the ability to perceive and control the physical equipment of the power grid. This caused a large-scale black out [6], which serves thereafter as a typical example of cyber security for a power system today.

Given the growing challenges and risks associated with CPS cyber security, this thesis aims to research enhancement to the cyber-physical robustness of demand-side energy systems from the perspective of outage energy management (i.e., community-level scheduling and appliance-level energy management), the communications infrastructure development and the cyber security strategies for when virus attacks are encountered. All these aspects facilitate the demand-side system’s self-serve capability and operational robustness under extreme conditions and dangerous scenarios.

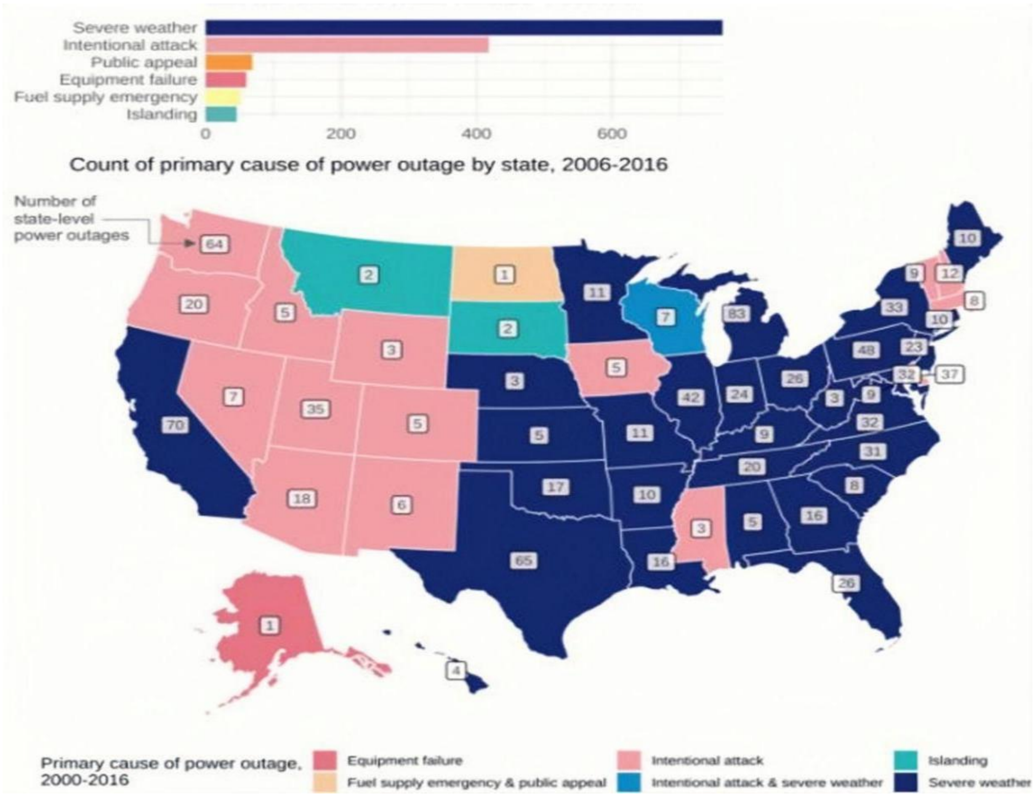


Figure 1.1 Summary of major energy blackout events of the USA in 2000-2016 [7].

1.2 Research Contributions

The research contributes of the thesis are grouped around the robustness of CPS demand-side energy system. The contributions can be summarized in the following aspects:

(i) Literature review on the state-of-the-art of Cyber-Physical System (CPS) of demand-side management is given in the thesis, together with special hybrid control system analysis as well as CPS system reliability and security assessment for system robustness enhancement.

(ii) Because there is little study on systematic robustness strategy about CPS scheme on demand side, this research has made an initial attempt to build a general scheme to enhance the robustness of CPS demand management among outage situation, communication network layout and virus attacks. Under system outage, there are two layers for maximizing the self-power supply duration in the extreme conditions. The study first proposed a resilient energy management system for residential communities, by scheduling coordinately the battery energy storage system and energy consumption of houses/units. A hierarchical resilient energy management system (EMS) by fully considering the appliance-level local scheduling. The method also considers the customer satisfaction and lifestyle preferences in order to form the optimal outcome;

(iii) A complex multi-hop wireless remote metering network model for communication layout in a CPS demand side was proposed, which decreased the number and locations of data centers in demand side and reduce the security risk of communication and the infrastructure cost of the smart grid for residential energy management. A novel evolutionary aggregation algorithm (EAA) was proposed to obtain the minimum number and locations of the local data centers for fulfilling the connectivity of the smart meters.

(iv) Finally, the system facing virus attacks has been studied as well. A novel risk management approach to confront viruses in the system with numerous network nodes is proposed. It is a trade-off scheme for double-virus problem, which enable to determine the allocation of antivirus programs to avoid system crashes and achieve the minimum potential damages. A DOWNHILL-TRADE OFF algorithm is proposed to address a appropriate allocation strategy under the time evolution of the expected state of the network. Simulations are conducted using the data from the Smart Grid, Smart City, [SGSC reference?] national demonstration project trials.

1.3 Thesis Outline

In Chapter 1, the problem statement is illustrated, together with the research contributions and the structures of this thesis.

Chapter 2 analyzes the state-of-the-art of Cyber- Physical strategies for demand-side energy systems, and emphases the significance for the survival of the system under abnormal and dangerous conditions. The comprehensive literature reviews on cyber-physical system (CPS) and demand-side management are given as well. The review covered fundamental concepts, and associated technologies in the literature. Modelling of CPS demand-side with the integrating of hybrid-system and the relevant verification approaches are introduced. Based on this, the existing control methods and potential challenges for demand side integrating information physical system are also discussed. They conjunct determine the entire demand side robustness in cyber- physical system.

Chapter 3 proposes a resilient energy manage scheme in the residential community under grid outage conditions. The system equipped with Battery Energy Storage System (BESS) and the community-scale renewable resources to improve the self-supply ability in the community-scale system in demand side. Case studies and comprehensive comparisons are given using "Smart Grid. Smart City" database to verify the effectiveness of the developed methods.

Chapter 4 designs a hierarchical demand-side-energy management scheme in order to minimum the effect of power blackout for entire system and it facilities energy sharing ability among multiple households. The model enhances the robustness of cyber-physical demand side from community-level to appliance-level in the extreme blackout conditions. The model schedules multiple houses' residential energy appliances with a bi-level structure, where individual home energy management system (HEMS) interacts iteratively with community energy management system (CEMS). It is executed consecutively from community-layer to house-layer as its constraints. First, after receiving the outage information from the grid, the community-level scheme is able to make decisions about the discharging/charging of community battery energy storage system (BESS) and the load shifting decisions of multiple houses. Second, the housed-level model autonomously preforms the appliance-level scheduling on the home energy resources followed by the load shifting instruction from the community-level. Consumer satisfactions are also considered, and individual HEMSs' autonomous scheduling result are sent back to the CEMS to determine the latter. The results are continuously updated until the convergence criteria is met. Extensive case studies are given to demonstrate the efficiency and feasibility of the proposed model. With the implementation of home HEMS and CEMS, the information security can be protected in this system and the risk of data exposure can be avoided.

Chapter 5 proposes a complex muti-hop wireless remote metering network in order to fulfill the connectivity requirement with the minimum locations and number of the

powerful nodes in demand-side communication. A new evolutionary aggregation algorithm (EAA) is introduced and implemented to solve the optimization problem in the 2-hop network with 2 novel adaptive operations (the shuffle operation and the switch operation). The model can be solved with a more generic EAA algorithm (n-hop) to achieve n-hop (n>2) smart meters' optimization results. Comprehensive simulation studies and statistical analysis are given to validate the effectiveness and efficiency of the developed scheme and algorithm. The infrastructure performance is evaluated from the perspective of robustness, reliable scalability, and operational efficiency for energy management.

Chapter 6 analyzes existing security risks in a CPS demand side, then proposes a novel cyber security strategy to confront viruses in the system with a large number of network nodes. Current research takes double-virus intrusion as an example to form a trade-off scheme which determines the allocation of antivirus programs to avoid system crashing with the minimum potential loss. A DOWNHILL-TRADE OFF algorithm is proposed to find an appropriate allocation strategy under the time evolution of the expected state of the network. Case studies and comparisons with other algorithms are given to verify the efficiency and effectiveness of the proposed method. In addition, three representatives of network models are considered for model verification that validate the feasibility and applicability of the proposed algorithm.

Finally, conclusions and the potential future work are given in Chapter 7. Multiple more sophisticated viruses and propagating models such as the time-varying propagating model, the stochastic propagating and the impulsive model are identified as worthy of further studies. The double-antivirus model can also be extended to a multiple-antivirus scheme, and new algorithms, such as intelligent NAA algorithm, are needed to solve the problem. In addition, a secure multi-party computation-based demand-side data communication module is also needed for future work. This model is able to protect the private information of users.

CHAPTER 2

State-of-the-Art of Power Demand Side System in A Cyber-Physical Grid

2.1 Introduction

Modern power grids are heavily stressed due to more frequent extreme weather and ever-increasing power demands. As a result, optimizing the efficiency of resource utilization, maximizing the robustness of power operation, and making energy management resilient have become essential research topics around the world. In 2001, the U.S. Department of Energy proposed a plan to develop an integrated energy system to promote the popularization and application of distributed energy and combined heat and power (CHP) technology, in order to increase the proportion of clean energy utilization, and further improve the reliability and economy of the social energy supply system [8]. Germany launched the E-Energy project in 2008, aiming to promote the efficient operation of the energy system and large-scale utilization of renewable energy through advanced information and communication technology and market mechanism [9].

The integration of multiple distributed energy appliances, two-way communications equipment, and the implementation of advanced metering infrastructure has meant numerous multi-source information (i.e., the data on energy operating status, environmental monitoring data, end-user information, topology and operation data in distributed network) can be monitored and collected continuously, which makes it possible to control the energy on the demand-side and optimize power utilization [10]. The deep integration of power and information makes the grid system develop a Cyber-physical System (CPS). Consequently, as the scale of the network and the number of sensors increases, the external information directly or indirectly affects control of the energy system and the interaction mechanism between the energy space and information space becomes more and more complex. Energy space is the energy network which comprises power generation, transmission, and distribution. Information space can process and store the data received from physical devices over communication networks. As with traditional power systems, robust and reliable capacity is one of the basic requirements of CPS demand-management development. Some works discuss the reliability of CPS. In [12], the EU grid demonstration project "eco grid EU", a safe and reliable information and communication system is used to send real-time control commands so that demand side resources can effectively participate in the system dispatching operation. [13] proposes an information on the physical fusion mechanism of wind energy conversion system and pointed out that the close coupling between the physical components and communication network increased its vulnerability. [14] analyzes the impact of information attacks on the toughness of oil and gas physical information system. With society's increasingly high requirements for reliability in the energy system, it is very important to carry out corresponding reliability analysis and research for a system that contains electricity, heat, gas and other multi-energy under the deep integration of Information Physics [16]. However, there is less research on the robust analysis of CPS, which is also important to ensure system operation and optimize the ability to self-supply in extreme conditions. Moreover, little research has been conducted on the robustness of CPS demand management, which makes it possible for residents to manage energy actively and improve power efficiency.

This chapter analyzes the state-of-the-art of Cyber-Physical Systems for demand-side energy systems first, and then emphasizes the importance of the survival of the system under abnormal and dangerous conditions. The comprehensive literature review on cyber-physical system (CPS) and demand-side management are introduced respectively, including publications on their basic concepts, and the supporting technologies in a power grid. Based on this, the modeling for demand-side integration of physics and cyber system is presented. The corresponding conjunction of verification and control methods that determine the entire demand side robustness in the cyber-physical environment, is also discussed.

2.2 State-Of-The-Art

2.2.1 State-of-The-Art of Cyber-Physical System

The term cyber-physical systems (CPS) were first proposed by NASA in 1992 [17]. Helen Gill, a scientist at the National Science Foundation (NSF), described the concept in detail at an international symposium on cyber-physical systems in 2006. However, the sources of the terminology of Information Physics systems can be traced back to earlier time. In 1948, Norbert Weiner created the word cybernetics in Greek. In 1954 [18], Qian Xuesen published Engineering Cybernetics, and it was the first time this concept was used in engineering design and experimentation [19].

Since then, "cyber" has often been used as a prefix to describe things related to automatic control, computers, information technology and the Internet. Therefore, a cyber-physical system is essentially a research topic that originated from computer science. A traditional embedded system is the simple primary stage of CPS [17-18], which means that the embedded software running on a small computer/processor can only realize the controls and optimization processing functions under limited resources and performance [20]. With continuous expansion to industrial scale, the degree of automation and intelligence constantly improved, and the information utilization and degree of integration also increased. Following the rapid development and promotion of new-generation information technology, such as cloud computing, new sensing, communication and intelligent control, the information physical system based on the expansion and extension of control systems and embedded systems that has been formed [19] [21]. For example, Home Energy Management System (HEMS), an energy controlling system, which can embed various software and intelligent devices for different specific functions. Therefore, the system performance and ability are able to realize advanced control and solve complex problems. Based on a great number of distributed senser monitoring equipment resources, as well as the high-speed and reliable communication network, CPS realizes the integration of the physical data and external information, and then controls the physical process more accurately and effectively [22] [23]. As Fig.2.1 demonstrated, the Grid CPS divides into three layers, physical layer, information-physical integration layer and the cyber layer.

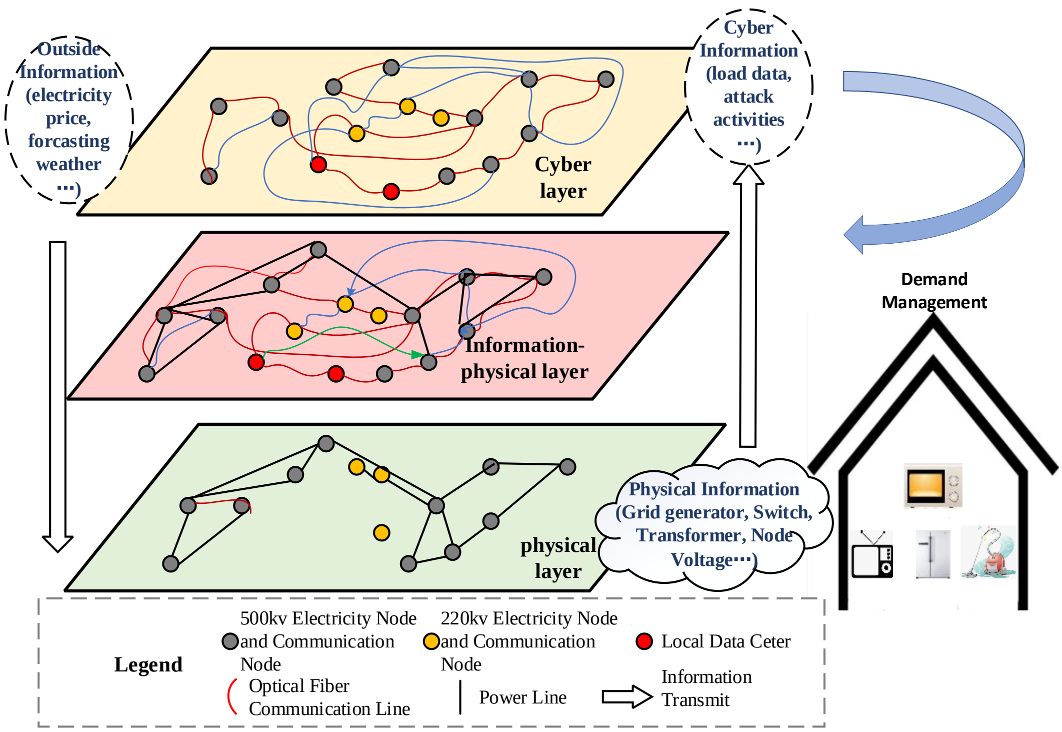


Figure 2.1 Virtual reality mapping of a cyber-physical system [23]

The physical layer mainly refers to primary power equipment, including generators, transformers, lines, switches, and loads. The internal components of the physical layer are tightly coupled through the electrical connection on the grid side, and the physical entity layer and the information-physical integrated layer are tightly coupled through the process of information collection and instruction execution. The information-physical integrated layer includes the communication network and secondary device layer network. Among them, the power CPS communication network is mainly composed of communication equipment (such as SDH equipment, switch, router, etc.) and communication protocol (the function of communication protocol includes unified data format, sequence and rate, link management, flow regulation and error control, etc.) It is to realize the transmission of information in the cyber system. Its impact on power CPS is mainly manifested in the delay, error code and interruption in the process of information transmission. The secondary layer network is a network entity based on the communication network, which mainly refers to the power system intelligent control network (i.e., the HEMS based network is a secondary equipment layer network in Fig.2.3).

Its performance is not only related to the performance of the secondary equipment layer network itself, but also affected by the performance of the communication network. On the one hand, the function of the secondary device layer is to realize the information collection / command distribution and transmission, on the other hand, it also includes the real-time analysis and processing of the corresponding data. Its impact on power CPS is mainly manifested in the effect of information processing (such as the accuracy of fault identification and signal acquisition) and the delay and error in processing information. The cyber system layer is a virtual network that abstracts the functions of different power control applications, such as state estimation, voltage control, security, and stability control. The function unit of the information system's control application takes the information processing result of the secondary equipment layer as the information input and generates relevant instructions accordingly. Through this process, the cyber layer and the information-physical integrated layer are closely coupled. The close and deep combination of physical equipment, information computing processing and communication transmission network gives the physical equipment and system new functions and makes it operate effectively. The basic concept is shown in Figure 2.2.

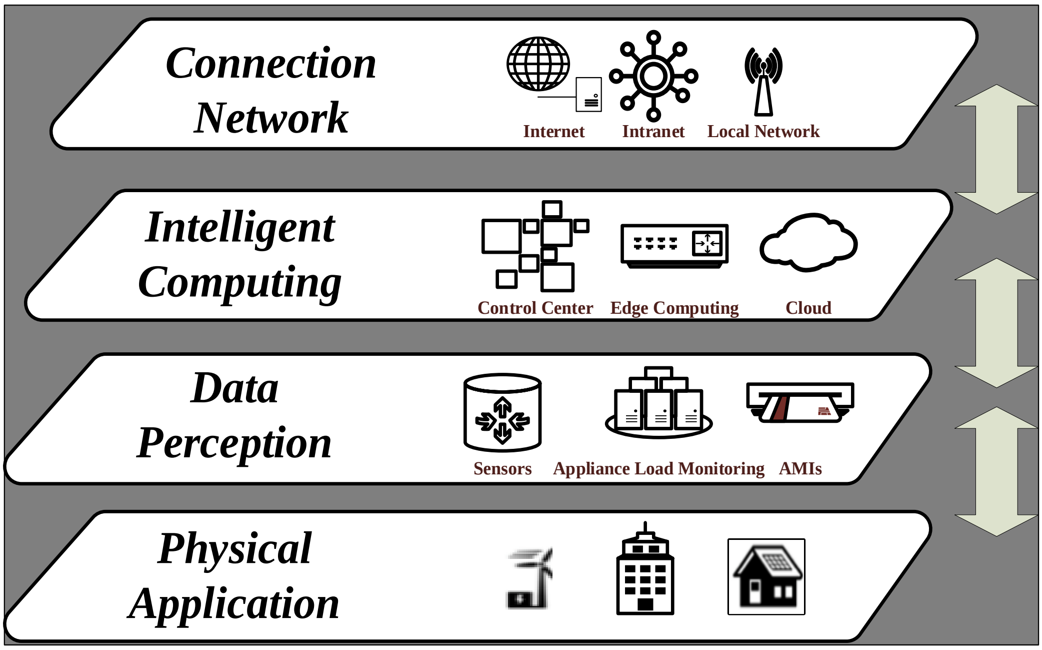


Figure 2.2 Basic Concept of CPS grids

The power system is a non-linear network with energy production, transmission, distribution, and conversion consumption, in which the components are highly complex, and its operation and schedules depend on a great number of control equipment [24]. According to the above overview of the concept of CPS, the smart grid is a typical cyber-physical system, where massive information is exchanged between secondary equipment and the main network in a power grid, and a great number of concurrent energy and information flows exist interactively in the operation analysis, optimization, and decision-making control of the whole power grid.

The proposal and development of a cyber-physical system (CPS) provides a new way to promote the deep integration of power primary systems and energy cyber systems, and ultimately achieve the objectives of power grid intelligence. CPS is a new system that combines computing resources with physical systems.

Compared with traditional control systems or embedded systems, a CPS has the following main characteristics:

The physical entities in CPS are embedded with sensing devices to achieve the information collection and behavior perception of the large-scale system;

(b) CPS connects embedded information devices and all physical entities in the system through the communication network to realize the flow and sharing of information in the system;

(c) CPS uses embedded control devices and large-scale distributed computing technology to control all system components, and then controls the overall behavior of the system;

(d) In CPS, physical devices and information devices interact with each other to determine the function and behavior characteristics of the whole system;

(e) CPS can realize dynamic reorganization of system components and online software updates. The above characteristics will make CPS more adaptable, flexible, safe, and reliable than the existing industrial system.

The power system is one of the important fields in the application of CPS. Based on the static model generated by physical entity facilities, through real-time data acquisition, data integration and monitoring, the operating status and progress of physical entities (such as collecting measurement results, tracing information, etc.) are dynamically tracked, and the entities in the physical space are reconstructed in the cyberspace to form an information space with the functions of perception, analysis, and decision-making. At the same time, with the ability to perform data comprehensive analysis and processing in the information space, effective decision-making is developed around complex changes in the external environment, and the physical power grid entities are affected by the way of virtual and real control. In this process, the interaction between physical entities and virtual information entities, virtual and real mapping, means they can work together to optimize the allocation of resources. Moreover, the CPS of the power grid can process and analyze the information in cyberspace according to perceived environmental change, and develop a knowledge base, model base, and resource base so that the system can continuously self-evolve. This enhances the ability to evolve with complex environmental changes and make an adaptive and effective response to external changes.

2.2.2 State-Of-The-Art of Demand -Side Management

With the evolution of intelligent network and two-way communication technology, residents can actually participate in production, rather than simply consumption. in a power grid. This makes it possible to manage the energy on the demand side instead of switch controlling. The intelligent interactive system provides the convenience of real-time bidirectional AC power between a power grid and users, providing multiple interactive services for users and building a high-speed communication network between users and a power grid.

A home energy management system (HEMS) is an application of a smart grid on the demand side, which is able to control and manage the energy network by integrating all the power generation, power consumption, and energy storage equipment in the home. HEMS encourages users to actively participate in power management to improve power security and energy utilization. There have been some studies on HEMS. [24-26] models a variety of household equipment (i.e., photovoltaic power generation equipment, energy storage equipment, etc.), and establishes a nonlinear day-ahead optimal scheduling model of household energy, which is solved by intelligent algorithms such as a particle swarm optimization algorithm and a genetic algorithm. In order to deal with the impact of external factors, [25] uses the model predictive control (MPC) method to reduce the impact of uncertain factors on the results, which is more robust and flexible than the previous method of optimization. The demand response mechanism can be divided into price demand response and incentive demand response [27]. A Demand response event (DRE) is defined as a period in which users are requested to reduce their electricity demand to relieve the pressure of peak load [28], which is generally manifested as the limitation of power purchase. Compared with direct load control, which hands control to the network, DRE gives the users agency. Customers are able to make a decision to reduce/increase their usage with different initiatives. In reference [29], an intelligent home device control strategy based on dynamic priority is proposed; In reference [30], the control strategy of smart home devices based on DRE operation priority is further studied based on TOU price; [31] studies the home equipment scheduling problem under the real-time electricity price, considering the risk factors of inaccurate prediction. References [29-31] are all real-time controls, so it is not easy to grasp the global information, and the control effect is not suitable to achieve global optimization. [32] proposed an event-driven smart home control strategy, constructed a linear 0-1 programming model considering automatic demand response, adopted the repetitive optimization method to deal with the addition of power consumption events, and realized long time-scale optimization with one-day as the optimization time, but the load was relatively single. None of the above studies considered the demand energy optimization strategy at large scale or researched the demand-side robustness in the cyber-physical system.

2.2.3 Technical Background and Applications

This chapter presents the representative technologies to support the cyber-physical system in demand side.

Advanced Metering Infrastructure

The advanced metering infrastructure is the essential technology to collect, store and transmit information about the home energy system and consists of the following five sections.

Meter Data Management System (MDMS): The measurement data management system is the brain of AMI. It confirms and analyzes the information collected and then transmits the processed data to the required system to ensure the data flow transmitted to the power outage management system and dispatching management system is accurate, in case of emergency. With the popularity of smart grids, meter data management systems play an essential role for data processing and data storage in the cyber-physical demand side.

Smart Meter: Compared with traditional meters, smart meters have a number of additional functions, including two-way communication, energy monitoring, data storage, and two-way calculating. In addition to the traditional meter's ability, smart meters can record and transmit the generated energy and sales amount by distributed energy users, and accept the real-time price issued by power suppliers. From the perspective of improving safety, smart meters can monitor electricity consumption, analyze power failures in time and eliminate the phenomenon of stealing electricity. A smart meter is the core equipment of demand energy management, which provides technical support for home energy scheduling and user demand-side response.

Two-way Communication Technology: Advanced communication technology is one of the important preconditions needed to realize a smart grid, which is the link between power suppliers and home users. Power line communication (PLC) is usually used in short distance communication. This technology uses current as a carrier to transmit the signal and uses a modem to separate the signal at the receiving end, before transmitting it to the computer terminal for processing. The installation is simple, and the cost is low. There also are other communication developments, such as Radio frequency (RF) which is used for short-range wireless, general packet radio service (GPRS) and multi carrier wireless information local loop (McWill etc. [33].

Home Area Network (HAN): HAN is the bridge of smart meter, home load, intelligent interactive terminal and other internal links, which makes the whole family energy system into an entity. Because of the complexity of home load types, a wireless network is suitable for HAN. The commonly used home HAN technologies mainly include Bluetooth, wireless fidelity (WiFi), and LTE, which is widely used because of its low power consumption and low cost. This research aims to improve the robustness of cyber-physical system for use on the demand side, therefore, multiple houses will be built into the model and other communication protocols will be implemented, such as Neighborhood Area Network and Wide Area Network.

Table 2.1 Comparison of wireless communication technologies [30][33][34]

Technology	Transmission Range	Speed	Frequency
3G	10 m	384 Kbps- 2 Mbps	1.92-1.98 GHz 2.11-2.17 Ghz
LTE	100-300m	10Mbps-100Mbps	2.3-2.4GHz
Bluetooth	1-100m	721 Kbps	2.4 GHz
Zigbee	30-50 m	250 Kbps	2.4 GHz 868-915 MHz
WIFI	50-100 m	54 Mbps	2.4/5.0 GHz

Terminal Load Monitoring: The purpose of terminal load monitoring is to monitor the energy consumption curve of various electrical equipment (household appliances or circuit interface) in the building through certain technical means. Through the load monitoring technology, the energy consumption of buildings can be monitored in a in fine detail, and the power consumption patterns of end users can be identified, which lays a foundation for the development and formulation of a demand-side management scheme.

The terminal load monitoring can be divided into intrusive and non-intrusive monitoring. Intrusive monitoring technology can physically monitor the energy consumption of electrical equipment through the installation of sub-meters. The advantage of this technology is that it can accurately collect the energy consumption data of electrical equipment in real time, but the disadvantage is that it requires the installation of sensors in the field, which costs money. Non-invasive appliance load monitoring (NILM) was first proposed by Hart in 1992 [34]. It aims to decompose and identify the energy consumption of each household appliance by analyzing the real-time aggregate energy consumption data collected at the main electrical intersection, based on the prior knowledge of household appliances' energy consumption, which is called a "power signature". For example, [34] uses active and reactive power as the power signature and identifies on / off events of different household appliances based on this. In references

[35] and [36], harmonic and voltage current signals are used as power signatures respectively to identify the on / off events of electrical appliances. The non-event based NILM technology does not require customization of the hardware interface, but only takes the aggregated building energy consumption time series (sampling frequency ranging from 1 second to 1 hour) as the input to decode the energy consumption of various electrical appliances. For example, in reference [36], sparse coding technology is applied to aggregate power sequences with sampling frequency up to 1 hour to estimate the energy consumption sequence of a single household appliance; Reference [37] used machine-learning technology to train and perform NILM identification on an aggregate power series with sampling frequency of 10 minutes. In previous work [37, 38], the author used a hidden Markov model (HMM) to model the operation cycle of electrical appliances, and combined it with a hybrid programming technology to identify NILM.

A. Big-data and Cloud Computing Platform

The data in an active distribution network has typical big data "4V" characteristics: large volume, variety, fast growth or speed, and great value. The network has a large scale and complex structure. It not only contains high permeability distributed power generation, electric vehicles and smart home, but also connects large-scale smart meters, integrated measurement units, synchronous measurement units and other monitoring elements. In October 2007, IBM and Google announced a cooperation in cloud computing, which has rapidly become a research hotspot in industry and academia. The application requirements and characteristics of big data in a CPS grid are very consistent with the service mode and technical mode of cloud computing. The adoption of cloud computing technology in the power industry can not only realize big data collection and sharing, and provide business intelligence and decision analysis through data mining, but it can also improve the value of power marketing services by transforming data into services. The establishment of a big data cloud computing platform to integrate multi-source heterogeneous data information resources can greatly improve the real-time control and advanced analysis ability of an active distribution network, and provide effective support for the development of CPS grid technology.

2.2.4 System Development Prospect

This section investigates the integration of cyber information for a demand-side energy management system (see Fig.2.3). The system aims to enhance the robustness for CPS demand-side.

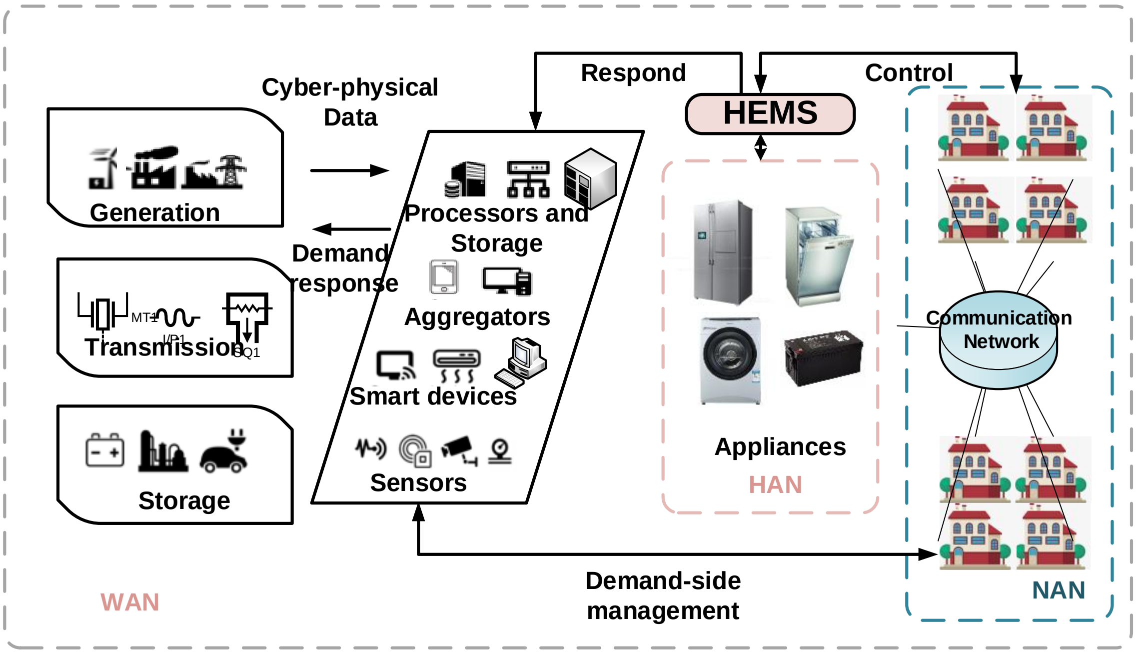


Figure 2.3 Development of cyber- physical system in demand-side

The Fig.2.3 presents the demand-side system integrated into CPS system. Multiple communication protocols can be applied to the power system: Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN). HAN is implemented to provide communication between household appliances and HEMS; NAN is used to communicate among different houses/units; WAN provides the connection between grid information and demand-side management. Advanced technologies discussed in the previous section support the CPS demand-side operation and any node failure in the power system will have adverse effects on the safe and stable operation of power on the CPS demand side.

These advanced techniques facilitate the energy efficiency and communication of the grid, but the risk of grid operation is also increased.

2.3 Modeling for Demand-Side System under the Cyber-Physical System Context

As CPS is the integration of a physical continuous dynamic process and a computing communication system, it usually contains both continuous and discrete dynamic process. The Information system monitors, calculates, and instructs physical process based on discrete digital data, and physical process is described by continuous dynamic differential model evolving with time. Usually, information and physics coordinate to achieve the same optimization control objectives, but they are configured separately with different time scales. Because the information system in the process of data collection, processing and analysis is carried out according to a certain time sequence logic, there must be a time difference with the physical process, so complete real-time synchronization between the two systems cannot be strictly and accurately guaranteed. Considering its cornerstone importance and the above objective difficulties, the modeling of a CPS system is one of the current focuses of research.

This chapter discusses the main directions of grid cyber-physical system modeling: the hybrid-system model between the physical power grid and the information network; and the risk evolution and robustness evaluation model of a power grid across information physical space. In a grid CPS system, the essential feature is the interaction fusion of the power information network and the grid physical system. Therefore, modeling the integration of the cyber layer and physical layer is the basic problem of grid CPS research. The interaction mechanism based on cyber and physical fusion requires the establishment of a risk and robustness model to realize the dynamic assessment of risk propagation and fault evolution. In addition, the modeling of CPS demand management is also presented in this section, which introduces the classification of demand-side models and a robust modeling framework for the demand side.

2.3.1 Modeling of Hybrid-System

The Hybrid-system model is one of the most successful methods for power grid cyber-physical fusion modeling [39]. Edward Lee first proposed this method formally in reference [40]. He proposes that hybrid-system modeling is the combination of a continuous equation that describes physical process, and a finite state machine model to refine and abstract state. A case of hybrid-system modeling for some practical engineering systems is given. In [41] [42], the hybrid-system modeling method is adopted to make the physical system reflect the event state and coexist continuously and discretely. The organic combination with embedded software is able to solve the problem that the concurrency of physical system and the seriality of software cannot be unified. However, most of the existing research around hybrid-system modeling is aimed at solving the synchronization and concurrency problems in embedded software development, and there are few examples and applications in power system modeling. In [43], the basic steps of modeling a hybrid system are described in detail, and the control effect of establishing a reasonable model is demonstrated by an example. In [44], a power system component library of a hybrid system is constructed, and the influence of discrete events on continuous dynamics is studied by using the trajectory sensitivity method. In [45], a hybrid-system model of power system with distributed generation is established, and a hierarchical control system that includes sliding mode control and predictive control is proposed.

Research [46] and [47] discuss the modeling method of a CPS system based on a hybrid system, in which the interaction between discrete computing process and continuous physical process is realized. The hybrid-system modeling method is applied to a distribution network of wind turbines, photovoltaics, energy storage and distributed generation. The hybrid system models are analyzed and established, and the interaction between the calculation process and physical process of each system is realized by using a state machine and a mathematical physical equation.

[48] and [49] put forward the CPS modeling method based on hybrid system and its implementation scheme for power grid control and studied the hybrid-system model and control taking flexible load and coordinated control of source, network and load as an example. Two hybrid system models, finite state machine (FSM) and mixed logic dynamic (MLD), are used as the CPS fusion model. Firstly, the FSM model is established according to the hybrid model framework and all the states of the modeling object, and then it is transformed into the MLD model. The MLD based control model is transformed into mixed integer quadratic programming to solve the problem. The control sequence of T steps in the future can be obtained at the current time and returned to the controlled research object side for control. This method can describe the continuous physical change law and the discrete state transition law, put the continuous and discrete in the same frame for reflecting the combination of the primary system and the information system, and can be applied or studied in the two systems respectively. This method is first introduced in detail and applied hybrid system model method to grid CPS system. The rationality and

effectiveness of this method are verified by simulation, and the fusion modeling effect of combining power grid physics and an information system and reflecting that the interaction between them is achieved. Therefore, the hybrid system model method should be further used in physical system analysis and control process expression, and its future research and application progress in CPS Fusion Modeling in a power grid is worth looking forward to.

A modeling example of a hybrid-system based on matrix method [50] is demonstrated in Fig. 2.4. As the previous figure introduced, the CPS can be divided into physical layer, information-physical layer and cyber layer. The CPS modeling procedure is to build the information-physical layer first and then connect the physical entity layer, the information-physical layer and the cyber layer through the correlation characteristic matrix to establish an integrated power CPS model.

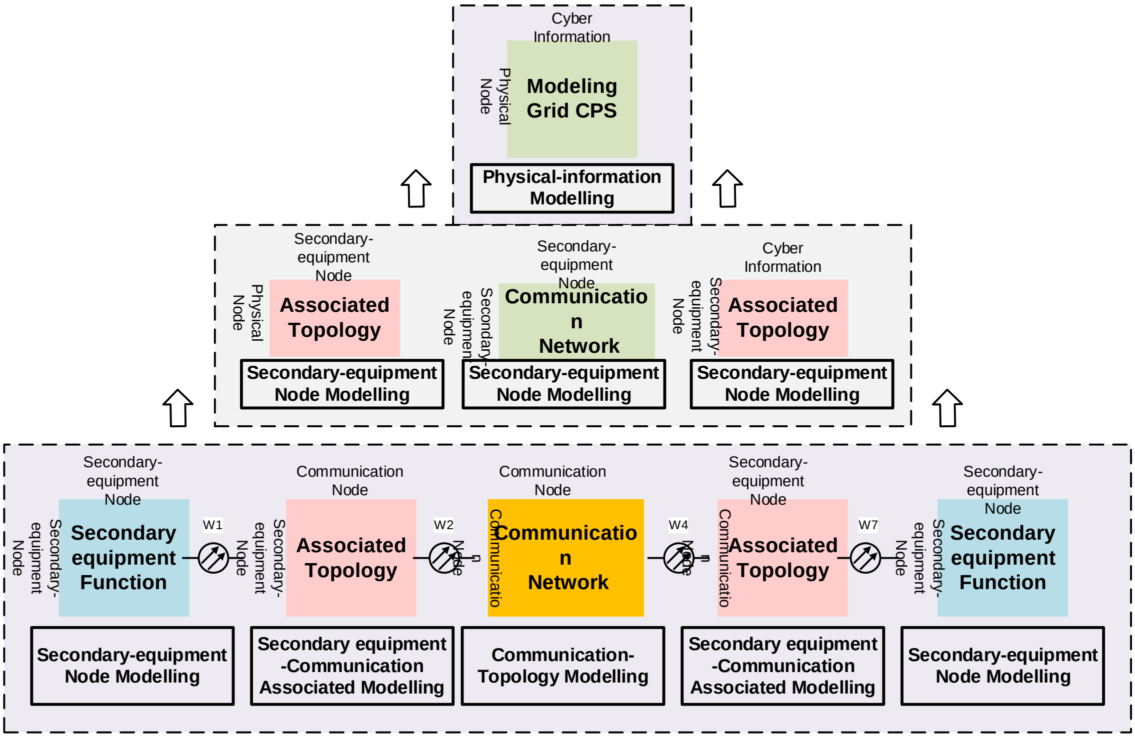


Figure 2.4 Modeling example of hybrid-system based on matrix method [50][51]

The information-physical layer consists of the communication network and secondary equipment network that is a entity network based on communication network. Therefore, the modeling of the information-physical layer requires the communication network to be established first, and then modeling the secondary-equipment network by combining the communication layout.

Communication Network Modeling: The direct impact of the communication network on a power grid information physical system is mainly reflected by signal transmission delay, signal loss and signal transmission error [51]. The model should be able to describe the communication performance of the communication network, which is mainly determined by the performance of communication node, branch and topology. This model uses a multivariate group to describe the different communication performance of the communication node and branches, and it uses an adjacency matrix to describe the topological characteristics of the communication network.

Assuming there are m physical nodes, n number of communication nodes, k is the number of secondary-equipment and cyber information in the proposed CPS. Equation (2.1) represents the operating performance of communication node.

$$N_{ij} = (T_{ij}, I_{ij}, P_{ij} \ldots) \tag{2.1}$$

where $T_{ij}, I_{ij}, P_{ij} \ldots$ are respectively the possibility of communication delay, communication outage and transmission error among node i and node j. Different communication performance has different forms due to different analysis requirements of power CPS. For example, when analyzing the impact of communication interruption on the real-time operation of power CPS, communication interruption can be indicated by "0-1" state. However, when analyzing the impact of communication interruption on the reliability of power CPS, communication interruption should be described as communication interruption probability or communication reliability. Therefore, in this model, the communication performance of communication nodes and communication branches is described by multi group, and the elements in that multi group can be expanded according to the application requirements of power CPS.

Based on the node modelling of a communication network, the topology of communication network is developed based on the communication network adjacency matrix as follows.

$$\mathbf{M}=\begin{matrix} & \begin{matrix} 1 & \cdots & j & \cdots & n \end{matrix} \\ \begin{matrix} 1 \\ \vdots \\ i \\ \vdots \\ n \end{matrix} & \begin{bmatrix} \mathrm{M}_{11} & \ldots & \mathrm{M}_{1j} & \ldots & \mathrm{M}_{1n} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ \mathrm{M}_{j1} & \ldots & \mathrm{M}_{ij} & \ldots & \mathrm{M}_{jn} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ \mathrm{M}_{n1} & \cdots & \mathrm{M}_{nj} & \cdots & \mathrm{M}_{nn} \end{bmatrix} \end{matrix} \tag{2.2}$$

$$\mathrm{M}_{ij} = (T_{ij}, I_{ij}, P_{ij} \ldots) \tag{2.3}$$

where M is a $n \times n$ matrix equation which demonstrates the matrix data transmitted in CPS communication network. If there is the connection between node i and node j, the

refers to the communication performance; if there is no connection between node i and j, $\mathrm{M}_{ij} = (0,0,0)$.

Secondary-Equipment Modeling: The secondary equipment network is a physical network based on a power-communication network, which serves the measurement, control, analysis and calculation of a power grid. The characteristics of the secondary equipment network are not only determined by its topology, but are also related to the corresponding communication network performance. Therefore, the secondary device layer network modeling mainly includes the secondary device node and network topology modeling, and also includes the modeling of the relationship with the corresponding communication network.

$$\mathrm{S}_{ij} = (F_{jj}(Input) T_{jj}(F_{jj}), P_{jj}(F_{jj}) \ldots) \tag{2.4}$$

where $F_{jj}(Input)$ is an information processing algorithm could consist of multiple sections with different logics. The transmission delay and possibility of error caused by information processing are determined by the algorithm embedded in the secondary equipment. Modeling of every piece of secondary equipment can develop a matrix as in Equation (2.5).

$$\mathbf{S}= \begin{array}{c} \\ 1 \\ \vdots \\ j \\ \vdots \\ k \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & \cdots & j & \cdots & k \end{array} \\ \begin{bmatrix} S_{11} & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ 0 & \dots & S_{jj} & \dots & 0 \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & S_{kk} \end{bmatrix} \end{array} \tag{2.5}$$

For The relationship between the secondary device layer network and the communication network mainly includes two aspects: one is the physical association generated by the direct connection of the physical link; the other is the logical association generated by the communication path of the secondary device layer network in the communication network. In the actual power CPS, the logical association depends on the communication path configuration adopted by the specific business, such as static configuration or routing search, and this association may change at any time. Therefore, it is difficult to express the logical relationship by using the static correlation characteristic matrix and the connection from the physical link. For the number of k secondary-equipment nodes and n communication nodes in grid CPS, the matrix DC is the processing of data collection and CD is the processing of data output. Their models are established similarly. We use DC as an example.

$$
\mathbf{DC}=\begin{array}{c} \\ 1 \\ \vdots \\ i \\ \vdots \\ k \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} 1 & \cdots & j & \cdots & n \end{array} \\ \begin{bmatrix} \mathrm{DC}_{11} & \dots & \mathrm{DC}_{1j} & \dots & \mathrm{DC}_{1n} \\ \vdots & \ddots & \vdots & ⋰ & \vdots \\ \mathrm{DC}_{i1} & \dots & \mathrm{DC}_{ij} & \dots & \mathrm{DC}_{in} \\ \vdots & ⋰ & \vdots & \ddots & \vdots \\ \mathrm{DC}_{k1} & \cdots & \mathrm{DC}_{kj} & \cdots & \mathrm{DC}_{kn} \end{bmatrix} \end{array} \tag{2.6}
$$

The associated network between the communication nodes and secondary-equipment nodes can demonstrate as $DC_{ij}=(DCT_{ij},DCI_{ij},DCP_{ij}...)$, where $DCT_{ij},DCI_{ij},DCP_{ij}$ are the possibility of communication delay, communication outage and transmission error among node i and node j.

$$
S_{net}=\begin{array}{c} \\ 1 \\ \vdots \\ i \\ \vdots \\ k \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} 1 & \cdots & j & \cdots & n \end{array} \\ \begin{bmatrix} S_{11} & \dots & \mathrm{S}_{1j} & \dots & \mathrm{S}_{1n} \\ \vdots & \ddots & \vdots & ⋰ & \vdots \\ \mathrm{S}_{i1} & \dots & \mathrm{S}_{ij} & \dots & \mathrm{S}_{in} \\ \vdots & ⋰ & \vdots & \ddots & \vdots \\ \mathrm{S}_{k1} & \cdots & \mathrm{S}_{kj} & \cdots & \mathrm{S}_{kn} \end{bmatrix} \end{array} \tag{2.7}
$$

$$
\mathrm{S}_{ij}=(F_{jj}(Input)T_{jj},P_{jj}...) \tag{2.8}
$$

Equation (2.7) shows the modeling of secondary-equipment network, where S_{ij} is the performance of secondary-equipment communication, if there is no connection of secondary-equipment i and j, $\mathrm{S}_{ij}=(0,0,0)$.

Grid CPS Modeling: Based on the modeling of the communication network and secondary-equipment network, the CPS integration model can be established. The matrix (**PS-SP**) is physics-secondary equipment integrated modelling, and (**SC-CS**) is the cyber-secondary equipment integrated modelling. Because the modeling of these associated networks is similar, the **SC** is used as an example as follows.

$$
\mathbf{SC}=\begin{array}{c} \\ 1 \\ \vdots \\ i \\ \vdots \\ k \end{array}\begin{array}{c} \begin{array}{ccccc} 1 & \cdots & j & \cdots & n \end{array} \\ \begin{bmatrix} SC_{11} & \ldots & \mathrm{SC}_{1j} & \ldots & \mathrm{SC}_{1n} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ \mathrm{SC}_{i1} & \ldots & \mathrm{SC}_{ij} & \ldots & \mathrm{SC}_{in} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ \mathrm{SC}_{k1} & \cdots & \mathrm{SC}_{kj} & \cdots & \mathrm{SC}_{kn} \end{bmatrix} \end{array} \tag{2.9}
$$

The associated network between the nodes of cyber layer and secondary-equipment nodes can demonstrate as $SP_{ij} = (SPT_{ij}, SPI_{ij}, SPP_{ij}\ldots)$, where $SPT_{ij}, SPI_{ij}, SPP_{ij}\ldots$ are the possibility of communication delay, communication outage and transmission error among node i and node j.

2.3.2 Modeling of Risk Evaluation and Robustness

Based on the hybrid-system model, the risk and robust assessment model of power grid CPS focuses on the transmission of cross-space risk and description of the cascading failure evolution. On this basis, considering the characteristics of information system and physical system, a cross-space robustness evaluation system is constructed.

Cross-space risk refers to the risk factors of the propagation and evolution in the process of power grid information physical interaction integration. According to its basic framework and the theory of cellular automation, a risk propagation model of CPS information physical security in a power grid can be established [52]. Based on Markov theory, the three-state reliability model of circuit breaker components and information system reliability model that evaluates connectivity evaluation can be established [53-54]. Monte Carlo proposes a CPS robust algorithm for an isolated microgrid. However, this model focuses on the probabilistic analysis of information layer reliability, does not involve the system fusion dynamics, and does not pay enough attention to the comprehensive evaluation of information physical interaction and cross-space reliability.

For the demand-side information physical system combined with hybrid communication network, the robust model of information system can be established by considering routing transfer and complex fault factors [55]. By considering the influence of information system monitoring and control function failure and application layer software failure on the system, the robust evaluation model can be established [56-57]. The dependence and matching degree of information physical components can provide ideas for establishing the robust model of CPS demand side considering the influence of information failure [58].

To sum up, in the aspect of risk propagation and robust assessment modeling, the existing research mostly focuses on the analysis of subsystems such as component, function or partial application layer, and there is a lack of a unified framework for risk description and robust consideration of the global system.

2.3.3 Modeling of CPS Demand Management

The cyber-physical energy system realizes the energy interaction and information communication between users and energy system. As the main participants of the integrated energy system, users who affect many links such as energy production, transportation, distribution, storage, regulation, trading of grid operation play an important role in the CPS. In the process of robust analysis and risk control of an integrated energy system, it is necessary to fully consider user factors and promote the interaction between users and the energy system [59]. Under the background of grid CPS, the pattern of energy supply and demand has undergone profound changes, and the user centered multi energy network [60] enhances the flexibility and adaptability of users to participate in energy supply and balance adjustment through energy demand-side management, which improve the energy utilization efficiency [61]. The modeling of CPS demand-side management can be divided into user physical characteristics modeling [62] and data-driven user energy consumption modeling [63].

User physical characteristics modeling: The modeling method based on the physical characteristics of load can analyze different kinds of load in detail and better understand its physical mechanism, such as the thermodynamic model of air conditioning users, the charging and discharging model of electric vehicles [62]. [63] considers the influence of different control variables, the time-varying load models of electricity price load and establishes the direct control load and interrupt load. In reference [64], the influence of an electric hot water load model on the energy supply reliability of a distributed integrated energy system was analyzed. Based on the thermodynamic model, the single air-conditioning load and aggregate air-conditioning load are modeled [65]. Under the influence of demand side user preference and user satisfaction, the potential for the air-conditioning load to provide reserve capacity to the system is quantitatively evaluated [64], so as to improve the operational reliability and economy of the power network. In [66], considering the charging and discharging characteristics of battery and user behavior habits, the load modeling of an electric vehicle is carried out. In reference [67], by analyzing the driving characteristics of a demand side electric vehicle and comparing it to a standby power supply, the mapping relationship between charging and discharging randomness and system reliability is established. [68] takes electric vehicles as the connection point between the urban road network and the distribution network, and proposes a system reliability evaluation method. In the aspect of data-driven load modeling method, [69] decomposes and reconstructs historical load data, and constructs load modeling data based on wavelet packet theory. In reference [70], equivalent relation clustering and fuzzy clustering are used to explore the comprehensive load characteristics of various industries.

Data-driven user energy consumption modeling: The data-driven load modeling method can make full use of the measurement data of intelligent meters in the integrated energy system, and make a better unified load modeling. Therefore, it is very important for the robustness analysis of the whole energy system to analyze the energy use and supply situation of the demand side users in the integrated energy system, including user classification, energy type, energy price, energy type and energy price. By studying different types of individual users' demand and consuming activities, a Self-learning Model of different types of users is established based on massive energy data, and the Self-Learning Model Based on artificial intelligence algorithm, such as a neural network, is used to realize the user energy load forecasting method [71]. Compared with the traditional energy consumption prediction method [72], the Self-learning Model Based on artificial intelligence algorithm makes use of mathematics, information processing and other methods to carry out abstract simulation on human brain neurons and establish the model. Its advantages lie in its strong self-learning, self-organization, adaptive ability, and strong nonlinear fitting ability.

In addition, according to the sensitivity of different types of users' energy consumption to energy prices, this section explores users' energy consumption psychology, and models the individual/group energy load, in order to quantify the impact of energy market price changes on different energy consumption behaviors, and puts forward the energy consumption/supply behaviors and interaction models of different types of customers in the energy market environment; Finally, according to the influence of randomness and uncertainty of users' energy consumption behaviors on the robust modelling of cyber-physical system, the demand side risk and robust model of CPS is established (see Fig.2.5).

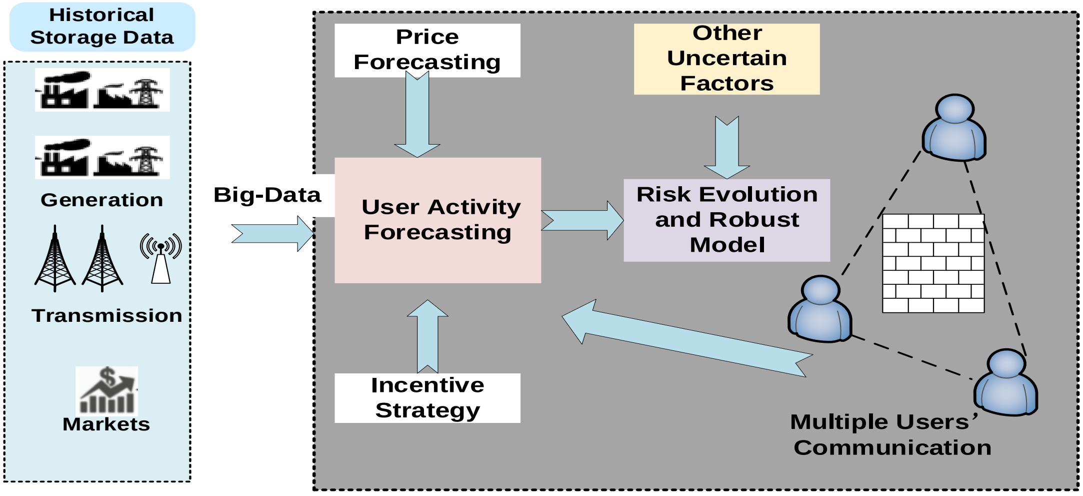


Figure 2.5 Framework of the risk and robustness evaluation model

2.4 A Formal Verification Method

Building a complete formal verification system is an indispensable section in the modeling process of a power cyber-physical system. Through the Formal Specification and Formal Verification, it provides the support to completely cover the possible state of the system, and fundamentally ensure the correctness and reliability of the model's logic.

Formal specification includes formal representation based on various logic, standard language and theorem reasoning tools that is an abstract process to describe the static characteristics of a system and its behavior. It has a strict mathematical definition of syntax and restriction. The described system characteristics include behavior characteristics, time characteristics, performance characteristics and internal structure. Based on propositional logic and predicate logic, the formal description language derives many kinds of logic, such as Linear Time Logic (LTL) and Computation Tree Logic (CTL), which can be used to express the inference conditions of system state judgment and state transition.

Formal verification based on formal specification, including various verification rules and tools, can infer and verify the model and logic. Formal verification uses strict logical reasoning method to verify whether the model or behavior logic of the system conforms to all or part of its formal description and rule definition. Formal verification is based on formal specification. On the contrary, formal verification can be used to verify whether the formal description meets the characteristics and requirements of the system. There are two main methods of formal verification: model simulation and theorem proving, both of which use validate the performance of a system.

2.4.1 Verification of Model Simulation

Model simulation is a verification that uses the specified formal description language to construct the behavior model of the system, and the transition path and mode of the key parameter state of the model are traversed through the established constraints and computing technologies to confirm if it meets the requirements of the system. In terms of the system with finite parameters and states, model simulation can always search the changed paths and validate the states; in addition to the infinite system, after a considerable scale of operation depth, the verification objectives can be achieved by mathematical induction. There are numerical studies to validate the model by setting up the simulations. In [73], by introducing the SOS method into the hybrid system theory, the formal modeling of a CPS system can be combined with the simulation's interoperability technology and applied to Devs Bus for verification. [74] pointed out that, because the instantaneous and highly uncertain verification process of CPS system must be fast and accurate, the time limited behavior of the system in the short term needs to be focused. But this means the research focuses on the instantaneous behavior of the system and does not analyze the continuous process in a long-time interval. By integrating the model checking technology into the CPS design process, [75] makes a formal analysis on the time attribute and security characteristics of a CPS system, and uses the UPPAAL tool to test timed automation.

2.4.2 Verification of Theorem Proving

Theorem proving is a proof process of its expected characteristics is gradually deduced from the original state, which utilizes the logical operators and qualifiers of propositional logic and predicate logic, on the basis of drawing up the inference rules of the system or model behavior, relying on its derived definition and intermediate inference, to validate the model. Compared with model simulation, theorem proving tends to deal directly with infinite state space. Theorem proving has not yet been developed into an automatic reasoning tool, and therefore it can only be done manually. This leads to the slow development of too abstract and difficult theorem proving that is not easily accepted by the application field.

For the power system, the theorem verification is mainly to verify the rationality and feasibility of the system from the perspective of logic analysis, and then to test the security and stability of the real-time system. [76] proposes the formal modeling of an intelligent distribution network information model based on the common information model standard, and carries out formal verification of ontology semantics, finds out the logical connection of each element in the model, and checks whether it meets the physical characteristics and application requirements of an intelligent distribution network. Through logical reasoning rules, the problems of model version updating, model synchronization and heterogeneous model transformation are solved. In [77], a formal method with strict mathematical definition is used to standardize the core logic of three typical topology analysis applications of a distribution network, namely, the determination of unobservable area, branch line contraction and electric island division, and the formal verification is carried out by theorem proving or model checking. This method: ensures the strictness of the logic applied during the distribution network topology analysis; meets the requirements of the completeness and accuracy of the distribution network system analysis; and is suitable for the online topology analysis needs of the distribution network with the change of topology structure, complex network structure and various types of equipment. For the purposes of practicability and reliability standard, reference [78] established a core model and algorithm of distributed self-healing of a distribution network based on IEC 61850 standard, introduced a formal method to describe the algorithm, and verified the algorithm by theorem proving and model checking. This proved the correctness and robustness of the self-healing algorithm. A complete reliability evaluation and verification system of distribution network self-healing system is formed together with reliable and robust evaluation.

2.5 A Hybrid Power Control Method

2.5.1 Basic Control Logic

The information physical system of a power grid integrates operational information, equipment information and environmental information. By using an information network and control terminal, the optimal control strategy is realized through the control method based on the cyber-physical fusion model. Considering the characteristics of high integration of CPS information system and physical system in power grid, the hybrid control mode combining network control with local control should be considered in power grid control in CPS demand side [79]. The control of CPS demand system has the following characteristics,

A. The control method can accurately monitor the changes to the model and power grid operation environment in real time.

B. The hybrid model is used as the basis of control mode, and the coordinated interconnection control of physical system and information system is considered.

C. The hierarchical and partitioned control structure is adopted to realize the unified and coordinated control between the upper system and the lower equipment. For the hybrid system model widely used in power grid CPS, its control logic can be divided into two categories:

   1) Events determine the evolution path of a CPS demand-side system, develop the control instruction and send it to physical system for control [80].

   2) The application of a hybrid model in the control loop is deepened and the hybrid logic of continuous dynamic and discrete state is considered. Continuous variable evolution and discrete state switching are applied to control loop at the same time for coordinated controlling at a system level.

2.5.2 The Hybrid Control Methods

The CPS demand management relies on the communication network to transmit information and control signals between dispatching agencies, smart loads, distributed generation, electric vehicles and intelligent devices. Therefore, the CPS demand side will be a typical networked control system. On the other hand, considering the possibility of temporary failure due to fault or network attack in the actual operation of the communication network, it is possible to reduce the operation reliability and robustness of the system by completely relying on network control. Therefore, in the smart grid environment, the ideal control mode should be the combination of network control and local control.

A networked control system (NCS) is a kind of control system where sensors, controllers and actuators are distributed on different network nodes and exchange information through communication networks. At present, most of the research on CPS demand-side controls concentrates on the following aspect: based on the hybrid modelling of flexible load and the hybrid system, the optimizing model and control strategy are constructed under the background of active demand-side network. [81] build a CPS based modeling and simulation verification platform for modeling hybrid logic dynamic and predicatively control optimizing calculation. Aiming at the collaborative control strategy of power grid CPS and its multi-level and distributed characteristics, a distributed entity control architecture including measurement, communication, calculation and physical objects is established to realize the collaborative control of power grid CPS, and a vulnerability assessment method of power grid CPS under the distributed collaborative control mode of dynamic attack and defense game is proposed [81-82].

2.5.3 Current Limitations

The control method and control system are restricted by the performance of the power information system. On the one hand, the performance of the computing system determines the maximum time complexity of a control algorithm. If the control algorithm is too complex, the calculation system may not be able to complete the control instruction calculation in time. On the other hand, the performance of the communication network determines the maximum amount of information that a control method can use. Generally speaking, the more system information is used, the better control strategy is likely to be obtained. However, the performance of the communication network determines the limitation of the amount of information that can flow from sensor devices to dispatching center or substation. From the perspective of cost reduction, the communication of a CPS system, especially from grid generator to distributed end users, will probably be realized by using the existing general communication network (such as Internet). In this context, a high performance for the flexibility of control method and control system is required. From this point of view, the power CPS demand control should be able to flexibly switch between a variety of control methods. If the performance of information system permits, the overall optimal control method should be selected, such as the global optimizing control by the dispatching center. Once the performance of the information system is reduced due to faults or external attacks, the system will automatically select the sub-optimal control method (such as hierarchical and partitioned control) based on the methods which will be developed in following sections. In serious cases, such as communication network failure or loss of the main server in a dispatching center, all kinds of equipment will implement local controlling according to local information. The hybrid control strategy combined with the above control methods can improve the system's robustness and reliability.

2.6 Potential Challenges

Robustness is the primary premise of reliable and stable operation of power grid. Due to the deep integration of information physical process, the communication and operation performance in information space suffers the risk of virus intrusion and malicious code. Therefore, the security risk problem of CPS demand side is more complex and difficult compared to the traditional grid, and considering the robustness is significance important to research.

2.6.1 Vulnerability of CPS Demand-Side

The demand system of CPS usually uses "security zoning, network dedicated, horizontal isolation, vertical authentication" and other ways to improve its network security [83]. However, these measures cannot fully guarantee the absolute security, and the network threats such as impersonation, eavesdropping and replay still exist. Moreover, even in a private network isolated from the outside, the power information system may still be infected with viruses. For example, some technicians intentionally or unintentionally implant malicious code into the system when repairing or debugging the system, thus damaging the normal operation of the power system [84].

In addition, with the continuous development of distributed device and energy storage technology, the structure of the power system is gradually changing. In future CPS, more and more intelligent electronic devices with communication and information processing capabilities will be deployed in all aspects of the demand-side system; The types and scope of information to be collected in power CPS will gradually increase, and the private network and general network (such as Internet) will be used in combination, and an open communication protocol (such as IEC 61850 standard) will be adopted. The application of these intelligent devices and open communication protocols brings more potential security threats to the power information system, and the traditional network protection measures may not be effective. There is numerical research on the vulnerability of CPS.

[85] comprehensively summarizes and discusses the sources of risk factors in a power secondary system and discusses the action forms of risk factors and their influence on primary system. [86] establishes a two-element relative fuzzy evaluation method and a set of risk assessments to improve the robustness of the power system to deal with information space security attacks. [87] - [88] are all aimed at the security situation of the power information network, which is evaluated and predicted based on triangular fuzzy number, support vector machine (SVM), particle swarm optimization (PSO), severity and sensitivity vector method, etc. In [89] - [90], the quantitative security risk assessment

caused by software failure is considered for substation communication security. The model of intrusion detection and prevention system is established, and its security is evaluated. The experimental environment is developed to study the influence of interaction between the information system and the power grid physical system on Power Grid performance and reliability.

In addition, [91] ~ [95] also study the vulnerability of key information network nodes and the important links of a power grid information physical system, such as the impact of communication system failure on abnormal operation of the power grid, the vulnerability of mutual confrontation between threat intrusion and power grid self-defense, that is, the vulnerability under an attack defense game, etc. [91] proposes a composite system incidence matrix which can reflect the power communication topological structure correlation, and establishes a composite system static vulnerability matrix, which can evaluate the vulnerability degree of a certain time section power communication composite system, and update the vulnerability value of the composite system in real time based on the changes of electrical and communication state. A dynamic vulnerability matrix is formed to evaluate the real-time vulnerability of power communication composite system. In [93], the propagation mechanism of interactive cascading failure is explained from a macro perspective by using the theory of interdependent networks. The modeling and vulnerability assessment method of power information physical dependent network is given. The factors that influence its structural vulnerability and the edge protection strategy are studied.

2.6.2 Risk of Propagation

In CPS demand-side, there is a wide range of interaction between information network and power network. As shown in Figure 2.6, in these two network, various monitoring and control terminals (i.e., smart meter, relay protection device, remote terminal unit (RTU), feeder terminal unit (FTU) etc.) are able to connect and interface between information network and power network. On the one hand, these terminal devices are able to collect the power consumption information and equipment status data of different power users for the control center to analyze the power system operation status and formulate the appropriate control scheme. On the other hand, they receive control commands from the control center, and perform control actions on the primary power equipment, such as decreasing or increasing the output of the generator, adjusting the tap changer of the transformer, etc. As far as the security risk of information space is concerned, these terminal devices are the only way to spread to the power space. Network attacks against information systems will affect the ability of terminal devices to perform monitoring functions, and then affect the normal operation of devices in power space. This is the basic communication form of information physical security risk in CPS demand-side. [96] describes the basic form of cross space propagation of power CPS security risk and establishes the propagation model of information physical security risk according to the characteristics of cellular automation-theory. Through the simulation, the influence of risk cross space transfer probability and failure cell cure probability on risk propagation is analyzed. Based on the improved percolation theory, a power system cascading failure model with information physical integration is developed. In [97], the dynamic development of cascading failures is described as a multi-stage process of fault propagation and expansion alternately in the information layer and physical layer. The physical layer power flow, topological integrity in the vulnerability index, and fault propagation are considered comprehensively. The information layer's delay increment is used to simulate cascading failure cases.

To sum up, the current research on the theory and method of risk assessment and robust analysis of CPS demand-side management still requires stronger mathematical modeling, calculations, and holistic robust simulation. Through the expected results, the factors and variables that affect the system security and change dynamically are fused and analyzed, which provides an effective method for real-time mastering and evaluating the robustness of CPS demand-side in the complex operation environment of multi factor interweaving.

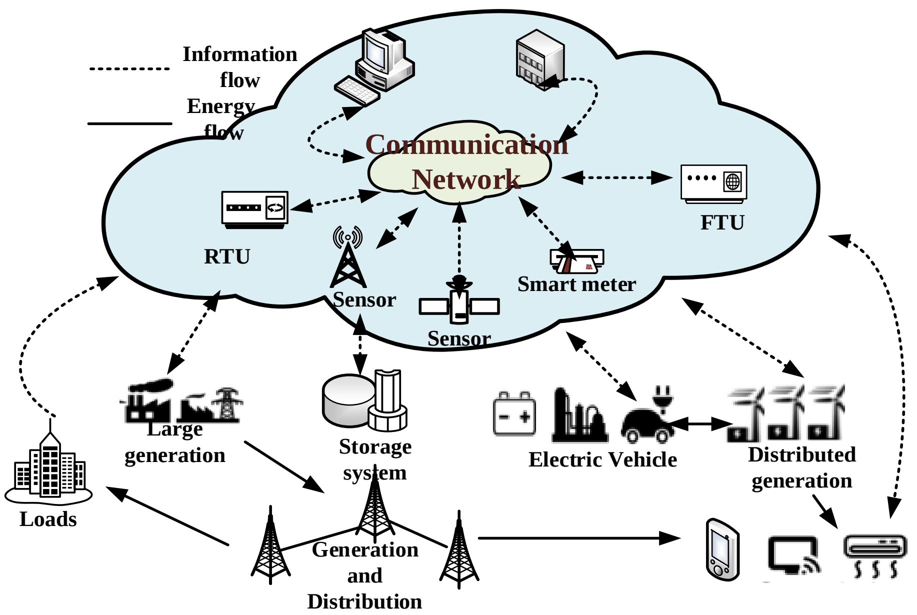


Figure 2.6 Interaction between the cyberspace and the physical space

2.7 Chapter Summary

This chapter introduces the state-of-the-art of cyber-physical energy management for demand-side. The comprehensive literature review on cyber-physical system (CPS) and demand side management are demonstrated respectively. It includes publications on their basic concepts, and the supporting technologies in a power grid. As CPS is the integration of physical continuous dynamic process and computing communication system, it usually contains both continuous and discrete dynamic processes. Modelling of CPS demand-side and the verification approaches are significant to study. Based on this, the existing control method and potential challenges for demand side integration of am information physical system are also discussed to determine the necessity for enhanced robustness of the entire demand side system in cyber-physical network.

CHAPTER 3

Resilient Energy Management for Residential Communities under Grid Outage

3.1 Introduction

As Chapter 2 discussed, the large-scale intermittent distributed access of new energy sources, the application of energy storage technology, the wide participation of flexible and controllable loads, bring a series of new challenges to the operation of demand-side system. The increased implementation of information technique make system vulnerable to get attacked. For instance, at the end of 2015, Ukraine's power grid suffered from malicious network attacks, and the implantation of computer viruses made the control server lose the ability to perceive and control the physical equipment of the power grid, which led to a large-scale blackout. In addition to the more frequent extreme weather and ever-increasing demand, both of them make the grid outage happening are more frequent than before. There are the five-year annual average of outages across the U.S.A doubled every five years in 21st century [97]. Moreover, the recent technologies including building automation systems, energy storage systems, and distributed renewable energy generation in CPS also provide support to sustain the grid outage duration and enhance self-power supply for buildings.

Grid blackout events are generally categorized into two classes: unplanned blackouts and planned blackouts. Unplanned outage refers to unexpected outage (e.g. caused by a sudden grid fault) with unknown duration, while planned outage is the outage event that users would be informed in advance and offered with sufficient outage information including the begin time, duration of the blackout and range of influence. Planned outage is not unusual in modern grids. Due to the equipment maintenance, there are roughly 1,700 planned powers cut off across Australia between 2015 and 2016, while more than 500 customers were affected in every outage event [98]. Modern technologies provide the opportunity to design the strategy of energy management in advance to sustain the outage duration and facilitate the self-power supply of buildings.

Building energy management is often based on various building-side distributed energy resources, including Plug-in Electric Vehicle (PEV), Photovoltaic (PV) solar/wind energy source, Battery Energy Storage System (BESS), controllable household appliances and distributed diesel generator. In recent years, there have emerged some researches about grid outage energy management of building side [99-101], which general utilize PEVs as backup generators to maintain the building demand (acts as the “Vehicle-to-Home, V2H” technology). In [100], the capabilities of PEVs in the V2H scenario are analyzed, where the PEV refers to as a backup generator under power blackout. The work in [99] utilizes the capability of PEV’s power discharging/charging to accommodate the rooftop-solar-power source, then designs a V2H enabled off-grid operation proposal for smart homes. The study in [101] coordinated control air conditioner system and PEV. The approach enhances the resilience of home energy by using the PEV to offer energy while serving a minimum thermal comfort’s level under the blackout.

The concept of “Smart Community” is introduced extending from the single building, which constitutes multiple buildings in a small area, and integrates various energy resources, Information, advanced energy management and control techniques and Communication Technologies (ICTs). There are some studies on energy management of smart communities. For instance, in [6], a mixed-integer linear programming (MILP) is proposed to schedule the devices with solar power optimally in a community. [102] develops an inexact community-scale energy model (ICS-EM) by sufficiently considering the uncertainty of renewable appliances. [103] proposes a interval two-stage programming technique based on superiority-inferiority for renewable energy management of community-scale. [104] developed a community energy management system(CEMS) which considers the limits excess reverse power flows to the grid and aiming to minimum the peak demand of community consumption during peak loading. In the research of [105], a game-theoretic distributed energy management technique is developed which make it possible reach a Nash equilibrium on the scheduling of the customers' appliances in a community. In [106-108], the peer-to-peer energy trading problems are discussed for the same community's residential houses. Through literature review, the current community energy management research is limited on the grid-connected scheme and the energy management problems under grid outages are little addressed. As for the grid outage duration problem of single building level, existing resilient energy management researches only mainly emphasize the PEVs' energy storage capability, but ignores the load shifting 's flexibility of end users. In the grid outage event, consumers would like to obtain more energy consumption being served with shifting their power loads to a certain degree.

This chapter designs a resilient energy management scheme on community-side, aiming to maximize the total amount of served load for a group of residents under the outage events. The developed strategy schedules energy resources of the community coordinately, including: (1) charging/discharging power of a community-scale BESS; and (2)the load shifting of each house in the community. An heuristic optimization algorithm, Natural Aggregation Algorithm (NAA), is applied to optimize the proposed model in this research.

Rest of the chapter is organized as follows: Section 3.2 discusses the workflow and communication protocols of community system; In Section 3.3, the model to coordinately manage community resilient energy is proposed; Section 3.4 introduces the solving approach of NAA algorithm; Section 3.5 presents the simulation research and comparison result. Finally, the Section 3.7 concludes this chapter.

3.2 System Model

This section gives detailed introduction of proposed workflow and supporting communication protocols of the system.

3.2.1 System Workflow

In this chapter, the building community model involves a community Battery Energy Storage System(BESS), a community PV solar source and multiple residential houses. The community is equipped with a Community Energy Management System (CEMS), which performs energy management to obtain a certain social welfare objective for the community; The BESS and PV panel are shared by all units of the community; in the proposed community; There is a Home Energy Management System (HEMS) installed on the house, which can communicate with the CEMS and control the individual energy appliances of house. The schematics of the system as shown in Fig. 3.1.

3.2.2 Communication Protocols

In practice, there are multiple communication protocols applied to constitute this community EMS: Home Area Network (HAN), Neighbor- hood Area Network (NAN) and Wide Area Network (WAN). HAN provides support for the communication between Home Energy Management and controllable devices. Several wireless standards, such as ZigBee (IEEE 802.15.4 standard), Bluetooth (IEEE 802.15.1 standard) and WiFi (IEEE 802.11 standard). NAN is applied in buildings and homes to enhance the communication between CEMS and HEMSs. NAN utilizes multiple protocols in design, such as 4G/5G, IEEE 802.22， 4G and WiFi, are able to be implemented in NAN. A Wide Area Network (WAN) is able to provide the information exchange between the utility and the CEMS (e.g. the outage information from the grid utility).

3.3 Meter Resilient Community Energy Management Model

The proposed energy management model of residential community in order to facilitate self-supply capability as well as minimize the total unserved load of the community during the outage period.

$$\min F = \sum_{t=1}^{T} (L_t^{us} \cdot \Delta t) \tag{3.1}$$

where T is the number of time intervals; Δt is the duration of one time interval (hour); L_t^{us} is unserved load of the community at time t (kW), calculated as:

$$L_t^{us} = \max\left[\left(\sum_{n=1}^{N} L_{n,t} + P_t^{bess} - P_t^{pv}\right), 0\right] \qquad t = 1:T \tag{3.2}$$

where N is the number of houses in the community; $L_{n,t}$ is the actual power consumption (after load shifting) of nth house at time t (kW); P_t^{bess} represents the charging/discharging power of the BESS at time t (kW), positive: charging; negative: discharging); P_t^{pv} is the power output of the community PV source at time t (kW).

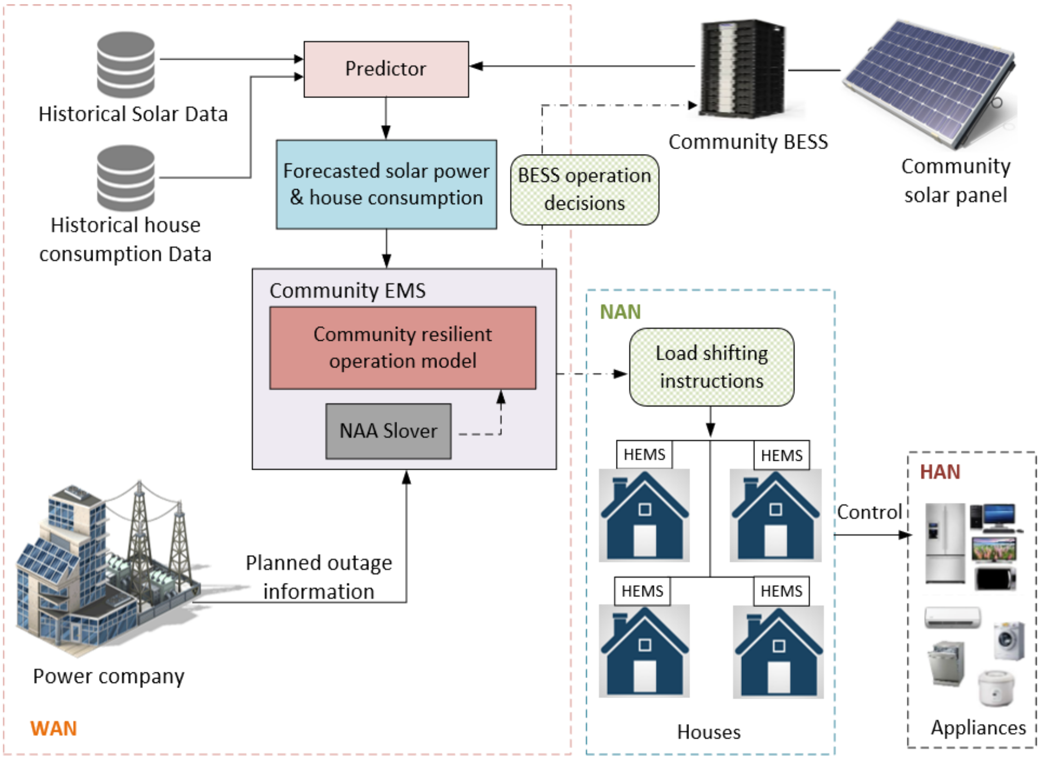


Figure 3. 1 Schematic of the proposed community resilient energy management

Model (3.1) is subjected to following constraints:

BESS operational constraints:

$$E_{t+1}^{bess} = \begin{cases} E_t^{bess} + \Delta t \eta^c P_t^{bess} - E_t^{bess} \eta^l \Delta t & P_t^{bess} > 0 \\ E_t^{bess} - | P_t^{bess} | \eta^d \Delta t - E_t^{bess} \eta^l \Delta t & P_t^{bess} \le 0 \end{cases} \tag{3.3}$$

$$SOC_t^{bess} = E_t^{bess} / E^{bess,rate} \qquad t = 1:T \tag{3.4}$$

$$\left| P_t^{bess} \right| \le P^{bess,rate} \qquad t = 1:T \tag{3.5}$$

$$SOC^{\min} \le SOC_t^{bess} \le SOC^{\max} \qquad t=1:T \tag{3.6}$$

where E_t^{bess} denotes the energy stored in the BESS at time t (kWh); η^c and η^d are charging and discharging efficiency of the BESS (%); SOC_t^{bess} is the State-of-Charge (SOC) of the BESS; $P^{bess,rate}$ and $E^{bess,rate}$ are power capacity (kW) and energy capacity (kWh) of the BESS; $SOC^{\min}$ and $SOC^{\max}$ are minimum and maximum allowable

SOC limits. In particular, Eq. (3.3) models the variation of energy stored in the BESS; Eq. (3.4) specifies calculation of the SOC of the BESS; Eq. (3.5) constraints the maximum charging/discharging power of the BESS must below its rated electricity; Eq. (3.6) ensures the SOC of the BESS is maintained within an allowable range, to protect the lifetime of the battery.

Power balance constraint:

$$P_t^{bess} \le \max\left[\left(P_t^{pv} - \sum_{n=1}^{N} L_{n,t}\right), 0\right] \qquad t = 1:T \tag{3.7}$$

Constraint (3.7) restricts that when the BESS is charged ($P_t^{bess} > 0$), its charging power should be less or equal to the surplus solar power of the community. Note that if the BESS is discharged ($P_t^{bess} < 0$), then constraint (3.7) naturally holds.

Load shifting constraint:

$$\sum_{t=1}^{T} L_{n,t} = \sum_{t=1}^{T} \tilde{L}_{n,t} \qquad n = 1:N \tag{3.8}$$

$$\sum_{t=1}^{T} \left(\left| L_{n,t} - \tilde{L}_{n,t} \right| \cdot \Delta t \right) \le \lambda_n \qquad n = 1:N \tag{3.9}$$

where $\tilde{L}_{n,t}$ is the originally intended power consumption of house n at time t (kW); λ_n is load shifting tolerance factor for house n (kWh). Constraint (3.8) ensures that the total power consumption over the outage horizon before and after load shifting must be the same; constraint (3.9) ensures that for each house, the total shifted energy amount cannot exceed a pre-specified tolerance threshold.

3.4 Solving Approach

This study uses a heuristic algorithm, Natural Aggregation Algorithm, to solve the proposed model. As a biological intelligence inspired optimization algorithm, NAA is able to simulate the group-living animals' self-aggregation intelligence, and make use of heuristic rules to seek for the near-global/global optimal solution in the certain problem space. Several optimization problems of power system have been solved by NAA algorithm successfully, such as [111-113]. More details about NAA refer to [109][110].

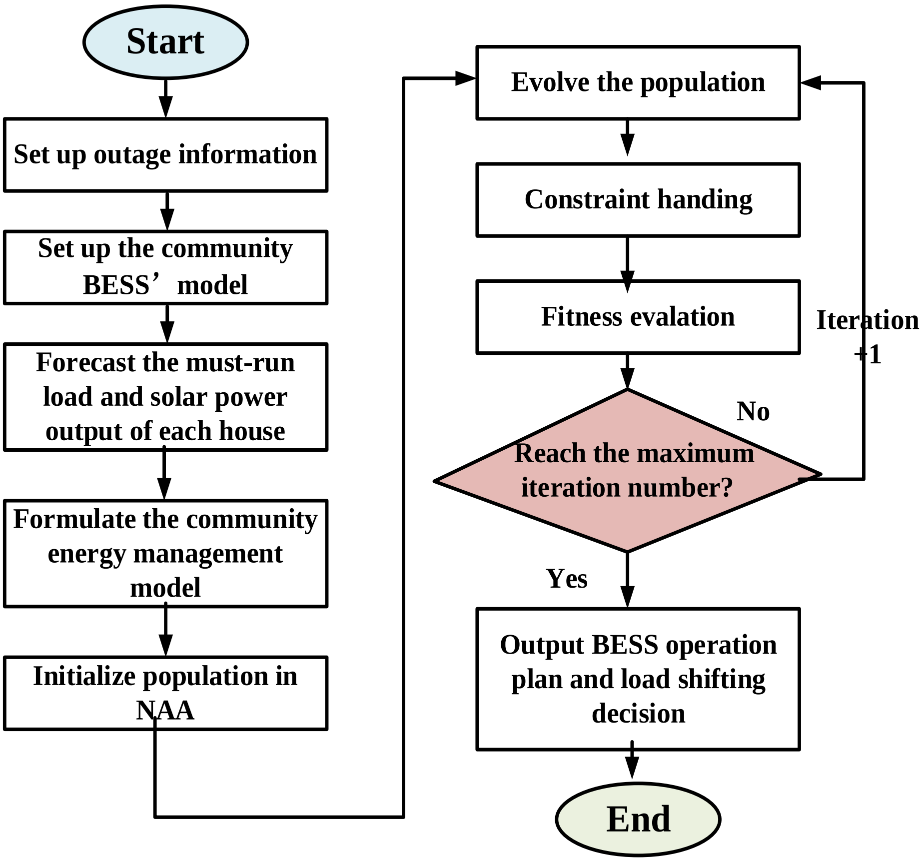


Figure 3. 2 NAA-based solving approach for community resilient energy management

Individuals represents a potential resilient energy management solution in NAA, encoded as a $(N+1)\times T$ dimensional vector. The first $N\times T$ dimensions represent the load shifting decision of the N houses, where every sequentially T dimensions represents the shifted load of one house. The last T dimensions represents the BESS's discharging/charging power profile. Fig.3.2 shows the overall of solving procedures. After receiving the outage information, CEMS is able to set up a BESS model and residential community energy management based on the forecasting load consumption and solar power, then the NAA algorithm will be used to develop this optimization (see section 3.5).

3.5 Numerical Study

3.5.1 Simulation Setup

In this section, numerical simulation studies are researched to validate the effectiveness and reasonability of the proposed method. Matlab are implemented for executing all numerical programs on a Microsoft Surface laptop. The results and simulation details are reported as follows.

We simulate a 24-hour planned outage event, starting from 0 am of a normal day consisting with a four houses residential community. The intending consumption profile of 24-hour power the four houses are gained from the Australian "Smart Grid, Smart City" project [114]. The energy consumption of four houses over 24 hours are totally 59.54kWh. the community side is assumed to install a solar panel with 4 kW capacity. Fig. 3.3 illustrates the 24-hour forecasted PV solar power output. The key parameters set as Table 3.1 is simulated the community BESS. Table 3.2 shows the four houses' the energy shifting tolerance threshold. The control parameter of NAA are set as bellows: maximum generation time =1,000, population size =1,000, Cr_{global} =0.1; α =1.5; δ =1; Cr_{local} =0.9; Cp^S =16; N^S =12.

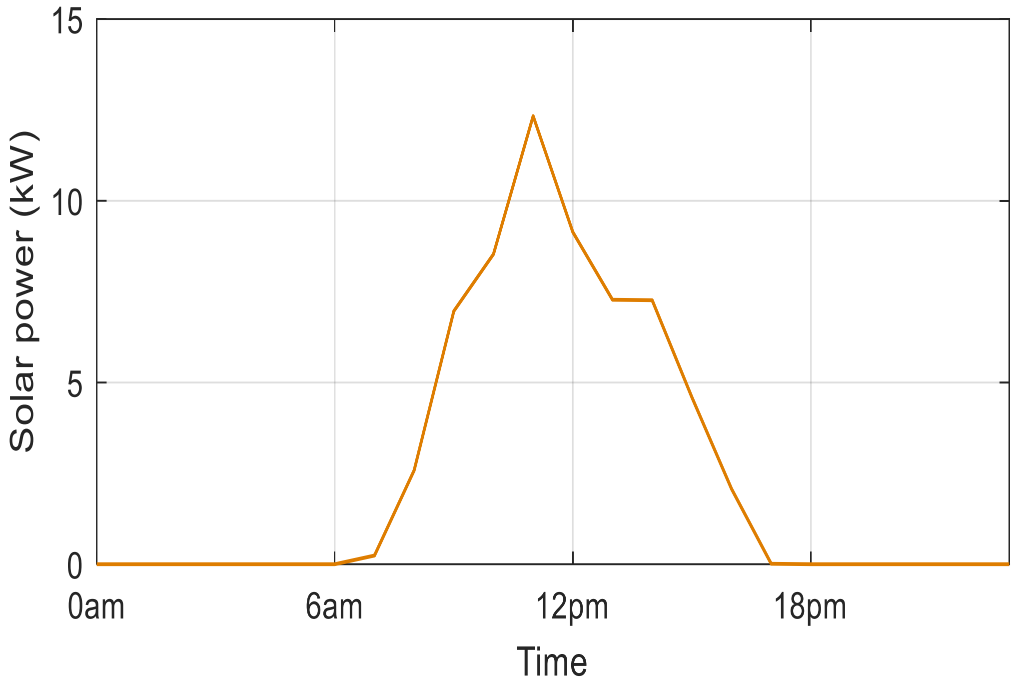


Figure 3. 3 Forecasted solar power profile

Table 3.1 BESS Model

Rated power	Energy capacity	Initial SOC
4kW	16kWh	50%
Charging/discharging efficiency		
0.9	0	100

Table 3.2 Energy Shifting Tolerance Threshold

	House 1	House 2	House 3	House 4
λ_n	1.2kWh	2.4kWh	4.8kWh	2.4kWh

3.5.2 Energy Management Results

After optimizing the proposed model, 45.19 kWh out of the 59.54kWh demand is satisfied by the community solar panel and BESS. The community BESS operation and house load shifting are determined as Figure 3.4 and Figure 3.5, respectively. Fig.3.4 shows that the original demands of houses are properly shifted, so as to maximize the self-supply duration of the entire community. The shifted degree is determined by the tolerance threshold of individual house. For example, the House 3 in Figure 3.4 shifted the load largest since its tolerant value is highest (4.8kWh), therefore, there are more consumption can be changed in order to enhance the community-scale self-serve ability. Figure 3.5 represents the BESS operation solutions with the allowable range of SOC [10%,90%]. The battery is able to charge to supply the power when there is no solar or little PV (i.e., evening); while the BESS is discharged when there is sufficient solar energy (i.e., noon). The efficiency of resilient power controlling is shown as Fig. 3.6, all appliance is accommodatingly managed to maximize the self-supply duration for whole community.

3.5.3 Comparison Study

To further illustrate the efficiency of the proposed resilient energy management model, we compare the proposed model on following three benchmark cases: SOC^{min} SOC^{min}

Case 1– With load shifting, no community BESS;

Case 2– With community BESS, no load shifting allowed;

Case 3– No load shifting allowed; no community BESS.

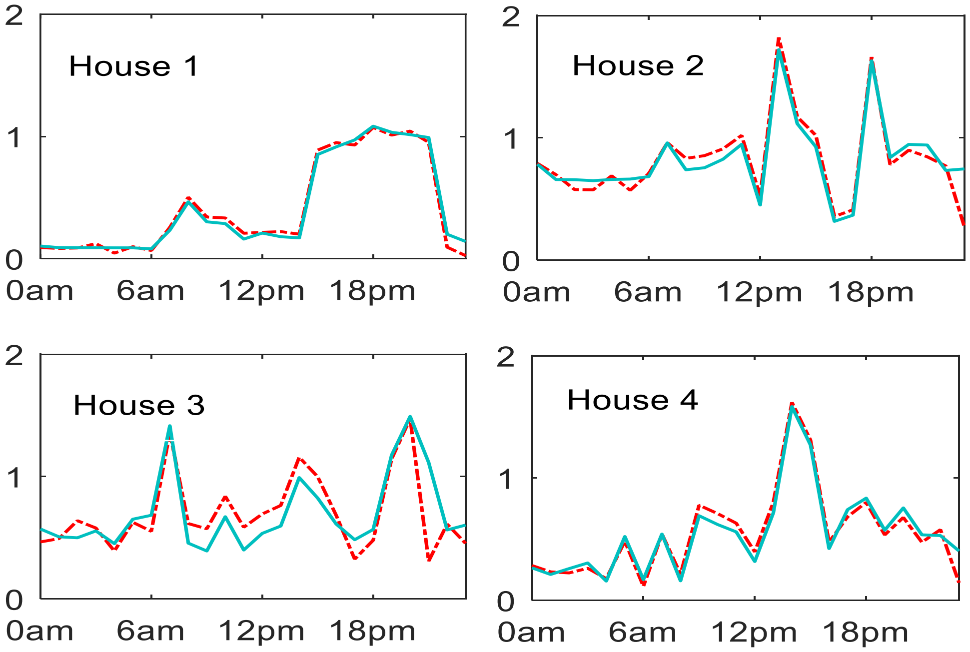


Figure 3. 4 Original (blue line) and shifted (red, dotted line) power consumption of houses

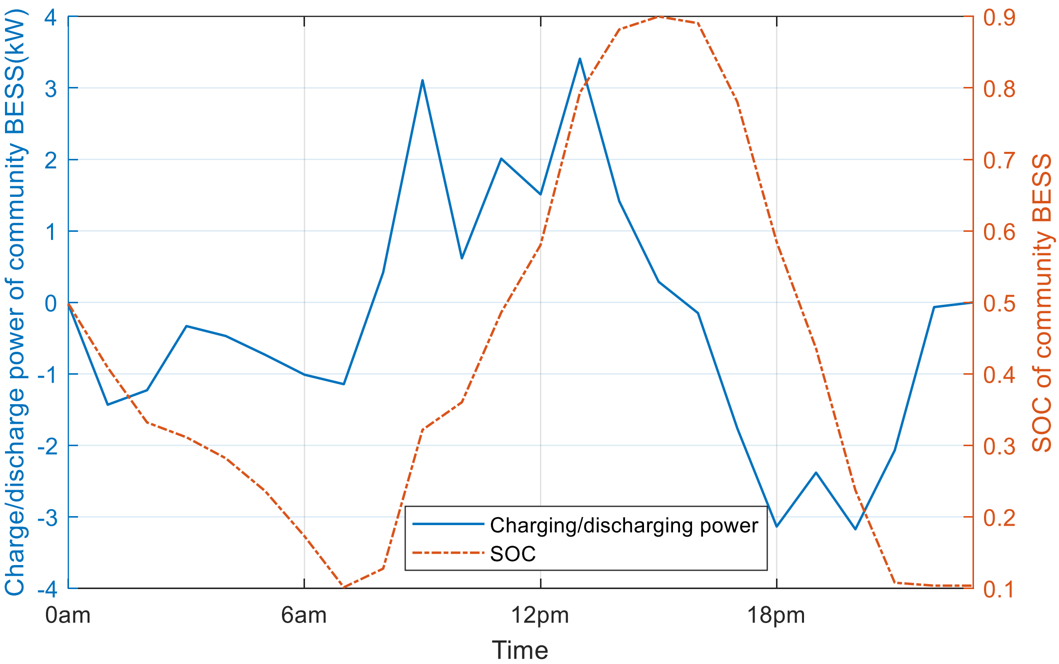


Figure 3. 5 SOC variation of the community BESS and discharging/ charging power profile;

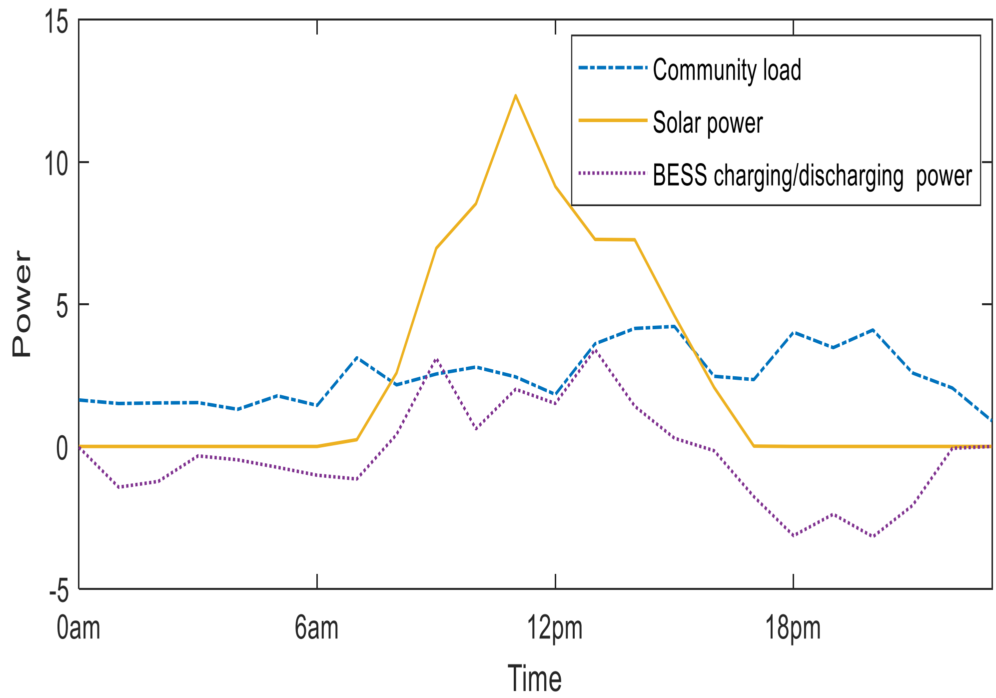


Figure 3. 6 Profiles of community load, solar power, and BESS operation under optimal solution

Table 3.3 Comparison study results

Community Summary Information		
24h community load		**24h solar power**
59.54kWh		61.01kWh
Comparison Results		
	Served community load	**Utilized solar power**
Proposed method	45.19kWh (75.9%)	38.85kWh (63.7%)
Case 1	25.82kWh (43.37)	26.82kWh (44.0%)
Case 2	42.41kWh (71.23%)	36.99kWh (60.6%)
Case 3	23.22kWh (39.0%)	23.22kWh (38.07%)

In Table 3.3, the numerical comparison results are presented. As to the results, comparing with other 3 cases, it can be seen that the best resilient energy management efficiency is able to be obtained by properly shifting the house load and coordinated scheduling the community BESS. 63.7% solar power is utilized and 75.9% community load is served in total. When no load shifting (Base Case 2) but only the BESS is implemented, 60.6% solar power is utilized and the majority of the community load (71.23%) enable still be well served, but still slightly less than the proposed method of the chapter. When there is only solar power is used (Base Case 3), and neither no BESS nor load shifting, the energy management efficiency is worst, which satisfy only 39% community load, and only use 38.07% solar power. In brief, proposed method is validate the effectiveness in comparison.

3.6 Chapter Summary

A resilient energy management of residential communities under the grid outage event is studied in this chapter, which optimally manages the energy consumption of houses, community BESS and the solar panel to optimize the self-supply capability of the whole community. Simulation results show that by properly shifting the power consumption of houses and coordinately scheduling the BESS, the renewable power can be better utilized, and the community can better maximize the outage period.

In this chapter, the community-level energy management under the power outage is discussed, which facilitates the whole community energy self-power supply, while the latter appliance-level optimization system will be presented in Chapter 4, where the Home Energy Management will be installed in house and performs the instructions among controller appliances to sustain the outage duration.

CHAPTER 4.

Hierarchical Energy Management Scheme under Blackout Events

4.1 Introduction

In chapter 3, a community-level energy management for demand -side system is proposed, and this chapter would develop a hierarchical scheme which considering the appliance-level under the blackout events for residential communities. This will further enhance the robustness for CPS demand side and facility the entire system self-supply capability under blackout situation.

Power blackout events are becoming more frequent owe to the extreme weather days caused by the global climate change and ever-increasing energy demand recently [118]. For instance, in the USA, statistical data indicates that the average number of outage events doubles every five years [119]. Grid outage events can be generally classified into two categories: unplanned outages and planned outages. Unplanned outages is defined as unexpected accidents which usually incurred in sudden, such as the extreme weather caused the transmission line faults. Planned outages are usually because of some pre-determined reasons such as system maintenance and load shedding, which are refer to temporary scheduled blackouts by the grid. Blackout are not uncommon in modern grids. For instance, there have been roughly 1,700 planned power outages across Australia due to equipment maintenance between 2015 and 2016, affected at least 500 customers of every accident [120].

Modern buildings have been transforming to energy “prosumers (producers and consumers)" from being pure energy consumers, with the operating at the edge of the grid [121]. Penetration of building-side building automation facilities, smart sensors and actuators and distributed renewable energy sources offers essential support to serve self-supply energy for residents under the power outage. In practice, energy management strategies can be proposed to support houses to optimize their energy usage over the planned outage horizon while minimizing the life disturbance to the user.

Existing works study on building energy managements (e.g. [122-125]), but limited literature has focused on grid outage event of the building energy management problems [126-129]. Most research utilizes "Vehicle-to-Home (V2H)" technology that harnessed the Plug-in Electric Vehicle (PEV) to provide energy for demand use in outage events. a rule-based V2H control strategy is studied in [9]: before the maximum State-of-Charge (SOC) level reached, the PEV's battery is able to charge while there is surplus PV solar power. In all other cases, the power of the PEV's battery is implemented to supply the house energy. The application of V2H under planned outages are discussed in [127] and [128] study. In [129] a V2H system to power home is developed, which operates in two modes: (1) risk-adverse mode, where the customers prefer to optimize the self-energy serve period of the home. In this mode, the TCAs' comfort level is given to low, and low priorities of the NTCAs are turned-off. The author of [128] designs an optimization model which coordinately manage both battery of a Plug-in Hybrid Electric Vehicle (PHEV) and the gasoline engine to provide energy under planned outages. In industry, the Nissan Motor Company Ltd illustrates an off-grid self-sufficient smart home in 2011, referred to as the "Leaf-to-Home" [129]. (2) risk-prone mode, where the consumer prefers to ensure the comfort level on the appliance usage. In this mode, the Thermostatically Con-trolled Appliances (TCAs) 's comfort degree is designed to be high, and all Non-Thermostatically Controlled Appliances (NTCAs) are preferred to operate. In this demonstration, the house is completely powered by a Nissan Leaf and electric vehicle solar panel.

There are several researches extensively studied on the single residential house/unit's energy management under planned outages. It would be opportunities to share power with each other for individual residential units/houses and maximize the power shutdown duration, equipped with distributed renewable energy sources (e.g. wind turbine or rooftop photovoltaic (PV) solar panel). However, the community-level energy management problem is little discussed during grid blackouts. The only reported work is found in [131], where a "Vehicle-to-Homes (V2Hs)" scenario is extended by author. In that scenario, multiple units installed with PHEVs controlled centrally to serve the community to serve the blackout period. However, the work in [11] is limited in two aspects: (1) the proposed V2Hs system is a centralized structure, which would make the power control computationally difficult when considering a large number of units/houses. This would be limited by the technology's application scale; and (2) the proposed model does not consider other types of controllable building energy resources but electric vehicles. For instance, the time shifting flexibilities and reduction of home load are not exploited and these would contribute to decrease the impact of grid outage (illustrated as Fig.4.1).

In this chapter, a hierarchical energy management for a residential community on outage problem is discussed. As an innovative contribution to this less-investigated area, an Energy Management System (EMS) is proposed to optimize a social warfare objective – minimize the totally un-served consumption of over blackout duration. In order to tackle the large dimension complexity induced by the large number of Residential Energy Resources (RERs) present in the multiple houses, the proposed EMS consider the workflow of energy management into two layers. In the upper layer, when the Community

Energy Management System (CEMS) receives the outage information, and then it solves a social warfare maximization model to determine the discharging/charging of the load-reshaping decision of each unit/house and the community Battery Energy Storage System (BESS). In the lower layer, the controllable appliances' operation would be performed by the Home Energy Management System (HEMS) of in the house on appliance-level, followed by the load-reshaping instructions received from the CEMS. After that, the individual HEMSs are sent autonomous scheduling result back to the CEMS, which would be scheduled by the latter updates upper-layer decisions. This process continues until the convergence criteria is achieve.

Compared to the current research [126-129], the innovations of the proposed EMS are as follows:

1. The proposed EMS provides support to enhance the robustness of system and cooperation of multiple houses and facilitate the whole community's self-energy supply ability;
2. The proposed system incorporates the load re-shaping capability of controllable appliances and the BESS's energy storage capability into a comprehensive framework, which would offer more flexibilities of energy management for the occupant during blackout;
3. The proposal adopts a decomposed structure, enabling the model to be more practical and scalable for utilizing with varying numbers of units/houses without incurring significant computational burdens; and
4. The decomposed structure also secures the sensitive information of users (i.e., appliance-level data) is control autonomously by the local HEMS, rather than being exposed to other third-party data center.

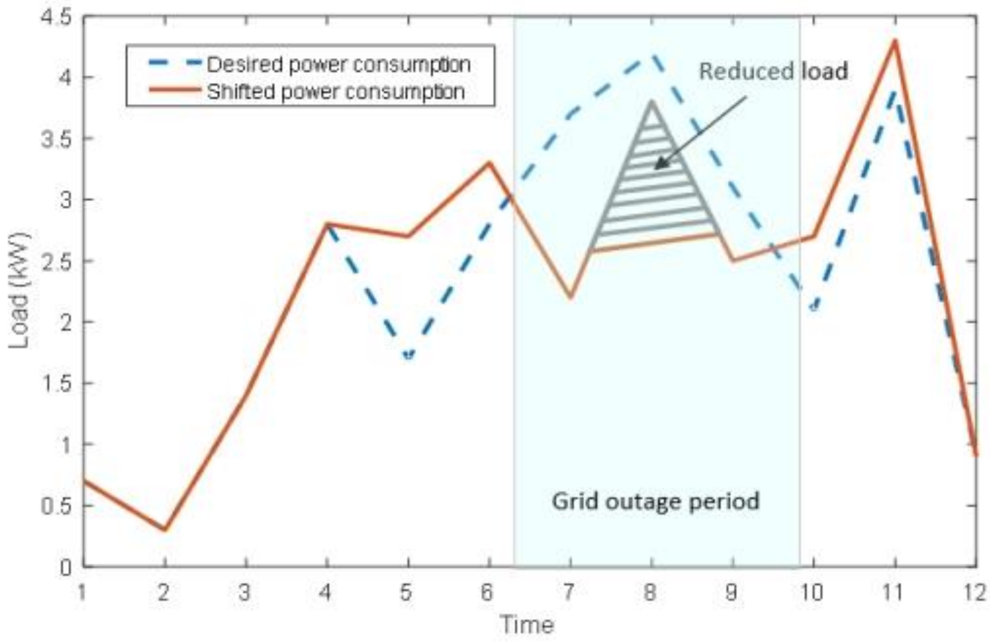


Figure 4. 1 Illustration of home load's shifting and reduction flexibility in grid outage event

4.2 System Overview

In this section, an overview of system schematic and several relevant implemented technologies are presented.

4.2.1 Schematic of the System

Fig. 4.2 indicates the schematic of the system is shown. There are N houses consisted in community; each house is equipped with a HEMS and rooftop photovoltaic (PV) solar panel. A set of controllable appliances are managed by the HEMS autonomously in the house. There are a shared BESS and CEMS implemented in the community side. In the community, the BESS can absorb surplus power generated by the rooftop PV solar panels, and then discharge energy to supply the residential community. The CEMS can communicate with the houses' HEMSs and manage the community BESS. low-voltage distribution market, it plays the role of both service retailer and power generator. That illustrates eliminating the intermediaries in trading processes.

After received the outage information from the utility firstly (i.e., the date, starting time and duration of the period), the CEMS send instructions to HEMSs. Furthermore, HEMSs perform solar power output forecasting and home load forecasting, which can be completed utilizing the embedded programs implemented in the HEMS or third-party Web services. When the outage happens, the physical connection between the community is disabled and the distribution system; the community then operates as an island micro-grid, where multiple HEMSs and the CEMS control and manage the energy appliances in the community (i.e. the solar panel and the controllable appliances and community BESS in each house).

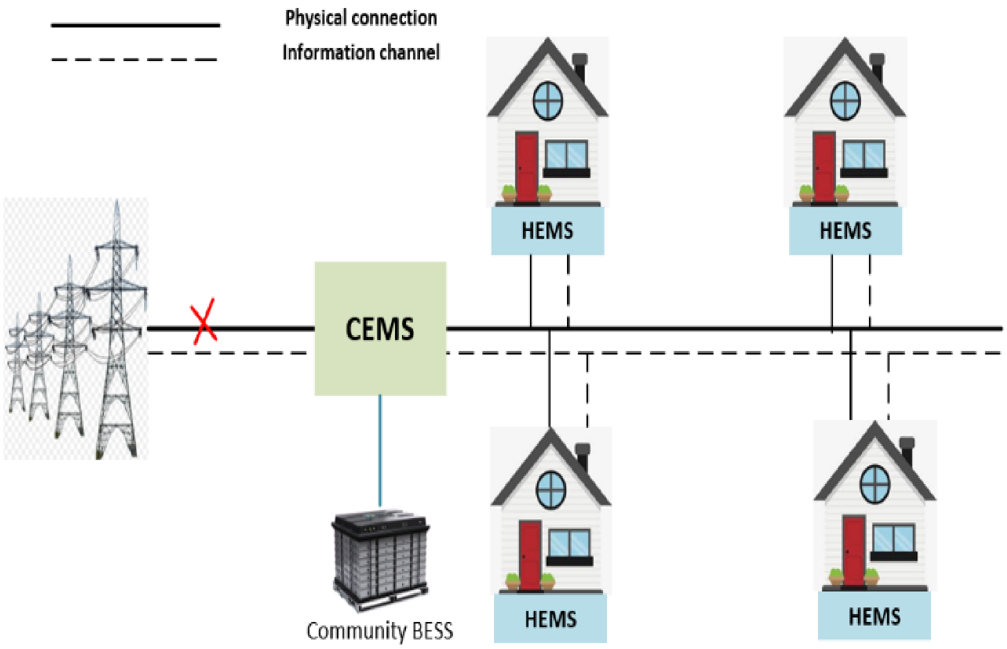


Figure 4. 2 Schematic of the community energy management under grid outages.

Based on the solar power and foretasted home load, the CEMS interacts with the HEMSs to collaboratively determine the community BESS's discharging/charging energy as well as the individual operations of controllable resources, so as optimizing the community' social warfare and enhance the robustness of whole system, i.e., the totally community served load under the blackout duration.

4.2.2 Implementation Technologies

In power blackout events, the wireless communication facilities are only approach to provide operation when the physical connection between the external grid and the community is interrupted. Multiple domains of communication protocols can be served.

In order to maintain the machine-to-machine communication between the HEMS and on-site household appliance, some short-range Home Area Network (HAN) protocols that install IEEE standards can be used, such as ZigBee (IEEE 802.15.4 standard), Bluetooth (IEEE 802.15.1 standard), and WiFi (IEEE 802.11 standard). With the objectives to support communication between CEMS and HEMs, the Neighbourhood Area Network (NAN) protocols can be implemented, i.e., Cellular technologies such as 4G/5G and WiMax (IEEE 802.16 standard). In terms of the larger scale, Wide-Area Network (WAN) protocols such as TCP/IP can be used to serve communications between the external entities and CEMS/HEMS, such as the third-party Web services and utility.

Data of the community, such as the houses' meter data and the historical solar power data is able to reserve in the individual local data storage or reserved in third-party clouds and accessed through Web service and interfaces TCP/IP, [13].

4.3 Hierarchical Energy Management for Residents

4.3.1 Modeling of Controllable Household Appliances

We assume that for each house (indexed by n), its HEMS manages following three controllable appliances' types.

(1) Ω_n^{CA1} : Set of controllable appliances that operate have a prescribed energy consumption at the nominal power and which must be completed between a specific time range. Their operations cannot be interrupted. For example, toasters, rice cookers and coffee machines;

(2) Ω_n^{CA2}: Set of controllable appliances that have a prescribed energy consumption at the nominal power operation which must be completed between a specific time range. Operation of these type resources enable to be interrupted and resumed later. Typical appliances in this class include dish washers and washing machines;

(3) Ω_n^{CA3} : Set of controllable appliances without a total energy consumption requirement but operating power in the range of $[P_{a,n}^{\lim}, P_{a,n}^{dsr}], a \in \Omega_n^{CA3}$. Instead, a certain disutility metric can be applied to measure the dissatisfaction of the user for deviating from a nominal operating point. Appliances that fall under this category involve lights, heaters, air conditioners, etc.

4.3.2 Workflow of Community Energy Management under Outage

The developed scheme is based on a previously proposed bi-level programming technique (Chapter 3) which is a kind of distributed optimization solver. In this model, a hierarchical two-layer structure is proposed and refers as a leader-follower. The leader's decision can effect the follower's strategy, and the follower's response would be fed back to the leader and also influence the leaders' decision.

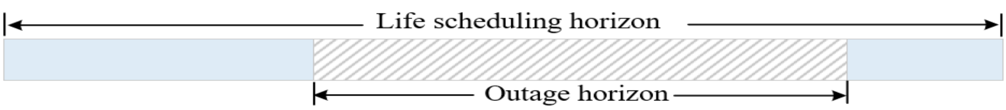


Figure 4. 3 Illustration of life scheduling horizon and grid outage horizon

In addition to the application, the CEMS is the leader and the HEMSs referred as the followers. Two horizons are deigned (Fig. 4.3): one is the "Outage Horizon (OH)", and another is the "Life Scheduling Horizon (LSH)". The LSH is often performed on daily basis and the period in which the user wants to accomplish their daily lifestyle tasks (e.g., clothes washing and cooking); The OH usually represents a duration covered by the power blackout period. The OH is a sub-segment of LSH. In this chapter, to enhance the robustness of the system and satisfy the community users' lifestyle tasks during the LSH as much as possible. In Table 4.1, the overall workflow of energy management system is illustrated.

Table 4.1 Algorithm of Energy Management for a Community under Planned Outages

Start	
1	Forecast the must-run home load and solar power profiles for each house; set up the controllable appliance models for each house; set up the BESS model;
2	Receive outage starting time and duration from the utility;
3	The CEMS solves an upper-level social warfare maximization model (model (1)-(9) in Section III-C);
4	**Repeat**
5	The CEMS sends load shifting and reduction instructions to each HEMS;
6	Each HEMS solves a lower-level home energy resource scheduling model to follow the load shifting instruction (Section III-D);
7	Each HEMS sends the scheduling result to the CEMS;
8	The CEMS solves the community-scale social warfare model to update load shifting instructions, based on the HEMSs' scheduling results;
9	**Until** the CEMS announces no new schedules;
10	Output the results.
End	

Line 1 shows the outage information is received by CEMS from the utility; then, the CEMS and HEMSs collaboratively manage the community operation to maximize the social warfare (Lines 3-9). The CEMS optimize an upper-level community self-supply capability to decide: (a) re-shaping decisions of the load for each house (Line 3); and (b) the BESS's discharging/charging energy decision. After that, the CEMS sends the instructions of load shifting and reduction to individual HEMS (Line 4). When the instructions of reduction and load shifting received, a lower-level autonomous scheduling model would be optimized by the HEMS, to determine the operational scheduling for controllable appliances of the household, with the objectives of minimizing the deviation between the instructed power consumption sent by the CEMS and the scheduled power consumption of houses (Lines 5 and 6). The lines 7 and 8 present that the HEMS's solving result is sent back to the CEMS, and based on it the latter updates the upper-level decisions. Such process continues until the CEMS announces no new plans for two consequent optimizations.

4.3.3 Upper-Level: Community-Scale Social Warfare Maximization Model

In this study, the social warfare objective is defined to minimize the amount of unserved load of the whole community over the planned outage horizon. The upper-level energy management model is defined as

$$\min F_1 = \sum_{t=1}^{T^{oh}} (\tilde{L}_t^{lost} \Delta t) + \alpha \sum_{n=1}^{N} F_2(\mathbf{L}_n^{sch},\ \mathbf{P}_n^{ca}) \tag{4.1}$$

where $\mathbf{L}_n^{sch} = [L_1^{sch},...,L_{T^{lsh}}^{sch}]$, denoting the power consumption vector of the nth house over Model (4.1) includes two items: (i) the first one is the total unserved load of the community; and (ii) the second one is the scheduling deviation between the upper- and low-level energy management models, which is integrated into model (4.1) through a penalty coefficient. Model (4.1) is subjected to the following constraints:

a) Operational constraints of the community BESS:

$$E_{t+1}^{bess} = \begin{cases} E_t^{bess} + \Delta t \eta^c P_t^{bess} - E_t^{bess} \eta^l \Delta t & P_t^{bess} > 0 \\ E_t^{bess} - | P_t^{bess} | \eta^d \Delta t - E_t^{bess} \eta^l \Delta t & P_t^{bess} \le 0 \end{cases} \tag{4.3}$$

$$SOC_t^{bess} = E_t^{bess} \big/ E^{bess,rate} \qquad t = 1:T^{oh} \tag{4.4}$$

$$\left| P_t^{bess} \right| \le P^{bess,rate} \qquad t = 1:T^{oh} \tag{4.5}$$

$$\left| P_t^{bess} \right| \le \sum_{n=1}^{N} P_{n,t}^{pv} - \sum_{n=1}^{N} L_{n,t}^{sch} \qquad P_t^{bess} > 0,\ \ t = 1:T^{oh} \tag{4.6}$$

$$SOC^{\min} \le SOC_t^{bess} \le SOC^{\max} \qquad t = 1:T^{oh} \tag{4.7}$$

Eq. (4.3) models the variation of energy stored in the BESS; Eq. (4) calculates the SOC of the BESS; Eq. (4.5) restricts the maximum charging/discharging power of the BESS must below its rated power; Eq. (4.6) ensures that when the BESS is charging, its charging power cannot exceed the surplus solar power of the community; Eq. (4.7) ensures the SOC of the BESS is maintained within an allowable range, so as to protect the lifetime of the battery.

b) Total energy consumption constraint for the house, which is expressed by the condition that the total amount of the re-scheduled energy consumption of each house cannot exceed the house's originally desired consumption amount:

$$\sum_{t=1}^{T^{lsh}} L_{n,t}^{sch} \Delta t \le \sum_{t=1}^{T^{lsh}} L_{n,t}^{dsr} \Delta t \tag{4.8}$$

c) House load reduction constraint. The CEMS needs to ensure that for each house, its reduced total power consumption cannot be larger than a threshold pre-specified by the user:

$$\sum_{t=1}^{T^{lsh}} L_{n,t}^{dsr} \Delta t - \sum_{t=1}^{T^{lsh}} L_{n,t}^{sch} \Delta t \le \lambda^{lr} \tag{4.9}$$

The decision variables of the upper-level energy management model include P_t^{bess} and $L_{n,t}^{sch}$.

4.3.4 Lower-Level: Autonomous Home Energy Management Model

After solving model (4.1) - (4.9), the CEMS determines $\mathbf{L}_n^{sch}$ for each house, and sends it to the HEMS of each house. By receiving the home load re-shaping instruction, each HEMS schedules its managed HERs to comply, as much as it can, with the specified instructions.

$$\min F_2 = \sqrt{\sum_{t=1}^{T^{lsh}} \left(L_{n,t}^{hems} - L_{n,t}^{sch} \right)^2} \qquad n = 1:N \tag{4.10}$$

where $L_{n,t}^{hems}$ is the total power consumption of the nth house at time slot t, scheduled by the HEMS (kW). It is calculated by the sum of the power consumed by the controllable appliances and must-run, uncontrollable appliances:

$$L_{n,t}^{hems} = \sum_{a \in \Omega_n^{CA}} P_{a,n,t}^{ca} + L_{n,t}^{mr} \qquad n = 1:N \tag{4.11}$$

where Ω_n^{CA} is the set of all controllable appliances of the *n*th house, i.e., $\Omega_n^{CA} = \Omega_n^{CA1} \cup \Omega_n^{CA2} \cup \Omega_n^{CA3}$. To minimize model (4.10), the HEMS of the house needs to determine the power consumption profile of each controllable appliance. This can be expressed as following matrix, which represents the decision variables of model (4.10).

$$\mathbf{P}_n^{ca} = \begin{bmatrix} P_{1,n,1}^{ca} & P_{1,n,2}^{ca} & \cdots & P_{1,n,T^{lsh}}^{ca} \\ P_{1,n,2}^{ca} & P_{2,n,2}^{ca} & \cdots & P_{2,n,T^{lsh}}^{ca} \\ \cdots & \cdots & \cdots & \cdots \\ P_{A_n,n,2}^{ca} & P_{A_n,n,2}^{ca} & \cdots & P_{A_n,n,T^{lsh}}^{ca} \end{bmatrix} \tag{4.12}$$

where A_n denotes the total number of controllable appliances of the nth house, i.e., $A_n = \left|\Omega_n^{CA}\right|$. Model (4.10) is subjected to following constraints:

a) Operation time range constraint of the controllable appliances:

$$P_{a,n,t} = 0 \quad t < \delta_{a,n}^{1} \ and \ t > \delta_{a,n}^{2} \quad \forall a \in \Omega_n^{CA1} \cup \Omega_n^{CA2} \cup \Omega_n^{CA3} \tag{4.13}$$

b) Task completion constraint of appliances in Ω_n^{CA1} and Ω_n^{CA2} :

$$\sum_{t=1}^{T} P_{a,n,t} \Delta t = E_{a,n}^{req} \quad \forall a \in \Omega_n^{CA1} \cup \Omega_n^{CA2} \tag{4.14}$$

c) Non-interruptible constraint of HERs in :

$$\sum_{t=t_{a,n}^{*}}^{t_{a,n}^{*}+E_{a,n}^{req}/(P_{a,n}^{rate}\Delta t)} P_{a,n,t} = P_{a,n}^{rate} \quad \forall a \in \Omega_n^{CA1} \tag{4.15}$$

where $t_{a,n}^{*}$ represents the time interval when the appliance a of the nth house is first time to be turned on;

d) Minimum online/offline constraints of appliances in Ω_n^{CA2}. Due to the user's lifestyle requirements or in order to protect the appliance's mechanical devices, operations of the appliances in Ω_n^{CA2} need to satisfy the following constraint.

$$\begin{cases} \tau_{a,t}^{on} \geq \tau_{\min,a}^{on} & s_a(t) == 0 \\ \tau_{a,t}^{off} \geq \tau_{\min,a}^{off} & s_a(t) == 1 \end{cases} \quad \forall a \in \Omega_n^{CA2}, \ t = 1 : T^{lsh} \tag{4.16}$$

e) Power consumption constraint of appliances Ω_n^{CA3}. For the appliances in Ω_n^{CA3}, their power consumption must be controlled within the allowable range:

$$P_{a,n}^{\lim} \leq P_{a,n,t} \leq P_{a,n}^{dsr} \quad \forall a \in \Omega_n^{CA3}, \ \delta_{a,n}^{1} \leq t \leq \delta_{a,n}^{2} \tag{4.17}$$

4.4 Problem Solving Approach

In Section 4.3 There are two optimization models. The community-level (i.e. upper-level) model is a linear programming model with linear constraints, linear objective function, and continuous variables, and it could be solved by the state-of-the-art linear programming solvers. In this study, we use the Mosek optimization toolbox for Matlab [132] for this solving. The appliance-level (i.e., lower-level) model is a mix-integer, both non-linear and linear constraints, nonlinear optimization model with both integer variables and continuous, and linear objective function. The nonlinear constraint (4.16) makes it difficult to be solved by the mathematical programming solvers. In this model, we use Natural Aggregation Algorithm (NAA), a heuristic optimization algorithm previously introduced in chapter 3 [133] to solve the appliance-level scheme.

4.4.1 Encoding Scheme of Lower-Level Model in NAA

In NAA, each individual is encoded as a vector with $\left|\Omega_n^{CA1}\right| + \sum_{a \in \Omega_n^{CA2} \cup \Omega_n^{CA2}} (\delta_{a,n}^{end} - \delta_{a,n}^{begin} + 1)$ dimensions, representing a potential appliance operation solution for model (4.10). The encoding scheme is as follows:

(1) the first $\left|\Omega_n^{CA1}\right|$ dimensions are integer variables, representing the starting time interval of the appliances in Ω_n^{CA1}. The corresponding task completion time can be calculated based on the operation cycle of appliances and starting time;

(2) the next $\sum_{a \in \Omega_n^{CA2}} (\delta_{a,n}^{end} - \delta_{a,n}^{begin} + 1)$ dimensions are binary variables, representing the ON/OFF status of appliances in Ω_n^{CA2} ; each consequentially $\delta_{a,n}^{end} - \delta_{a,n}^{begin} + 1$ dimensions represent the ON/OFF status of the appliance a within its permitted operation

time range [$\delta_{a,n}^{begin}$, $\delta_{a,n}^{end}$];

(3) the last $\sum_{a\in\Omega_n^{CA3}}(\delta_{a,n}^{end}-\delta_{a,n}^{begin}+1)$ dimensions are binary variables, representing the energy usage of appliances in Ω_n^{CA3}; each consequentially $\delta_{a,n}^{end}-\delta_{a,n}^{begin}+1$ dimensions represent the energy usage value of the appliance a within its permitted operation time range [$\delta_{a,n}^{begin}$, $\delta_{a,n}^{end}$].

4.4.2 Optimization Procedures

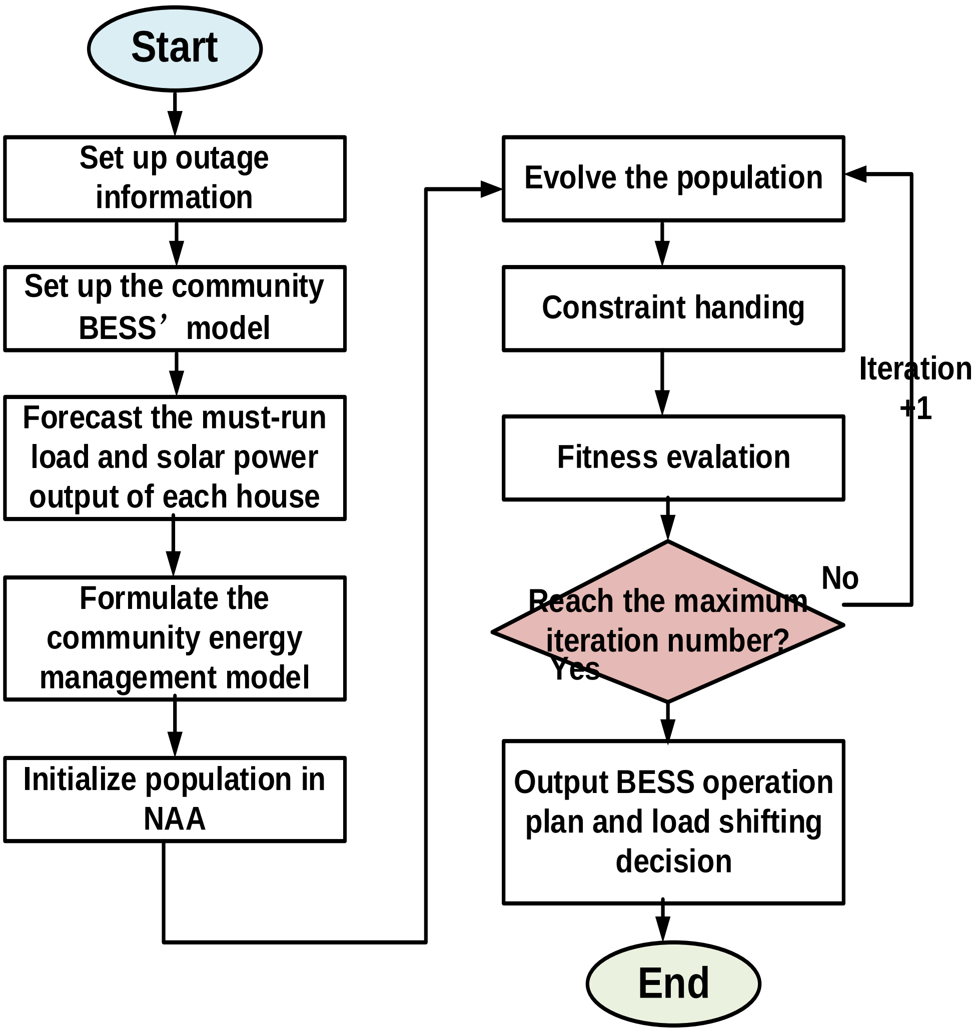


Figure 4. 4 Flowchart of the optimization procedures

The whole optimization procedures follow the algorithm in Table 4.1 that depicted visually in Fig. 4.4. At the beginning, when each house's model is built, including the community grid outage information and the model of BESS implementation, the different kinds configuration of controllable appliances, PV solar power output profile, and the must-run load profile. Furthermore, using Mosek optimization toolbox to solve model (1). The outputted decision variables of scheme (1) are preserved from data files of Matlab, and retrieved due to the NAA algorithm. With the re-shaping load instructions scheduled from the CEMS, the NAA algorithm optimizes model (4.10) for individual unit to determine $\mathbf{L}_n^{hems}$ and $\mathbf{P}_n^{ca}$, where $\mathbf{L}_n^{hems} = [L_{n,1}^{hems}, ..., L_{n,T^{lsh}}^{hems}]$. The result then is preserved into data files of Matlab and retrieved by the optimization toolbox of Mosel. The lower-level and upper-level optimization schemes are later solved iteratively until the convergence criteria is obtained. In this research, the objective function value is the convergence criteria (Eq. (4.1))'s difference of two consequential iterations is less than 0.5.

4.5 Case Study

Numerical simulations are conducted to prove the developed scheme. The programs are completed in Matlab and executed on a personal computer with two Intel Xeon processors and 4-Gigabyte memory.

4.5.1 Simulation Setup

In this study, a four-houses residential community is simulated to propose the resilient energy management. Those are indexed as House 1, House 2, House 3and House 4. Table 4.2 describes the community BESS's configuration.The rooftop solar panels are assumed to be implemented with all the four houses, with the capacity of 3kW, 3kW, 3.5kW, 4kW, 4kW respectively. The House 1's forecasted 24- hour profile of solar power output is shown in Fig. 4.5.

Table 4.2 Configuration of Community BESS

Rated power	**Energy capacity**	**Initial SOC**
10 kW	20 kWh	80%
Charging/discharging efficiency		SOC^{max}
1.0	10%	90%

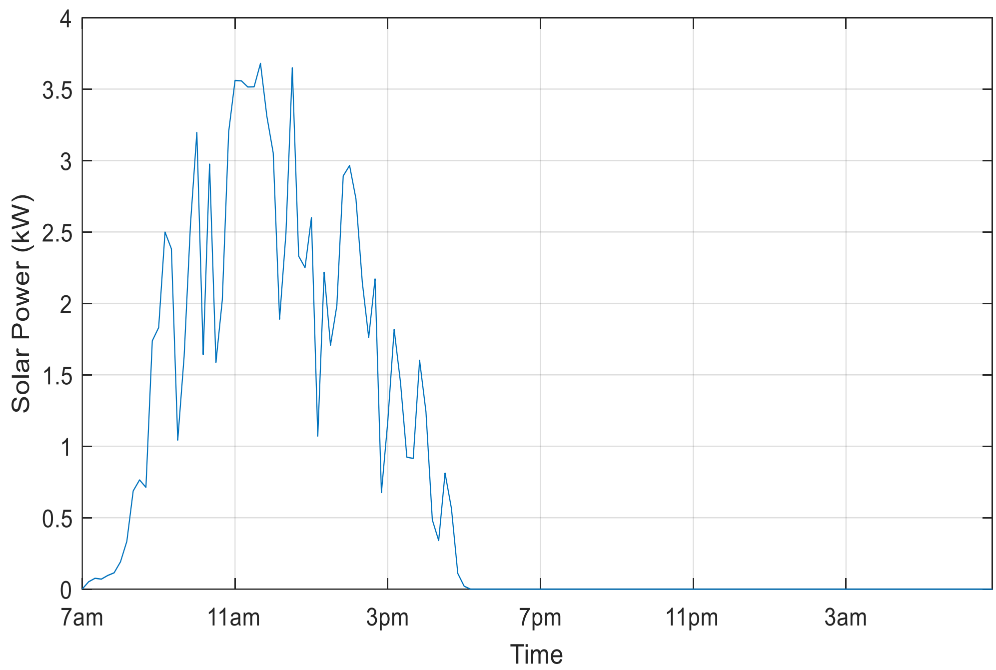


Figure 4. 5 House 1's 24-h solar energy profile

Table 4.3 Houses 1's configuration of controllable appliances

	Name	Power (kW)	AOTR	DOT	TC
Ω_n^{CA1}	Rice Cooker	0.7	[4pm, 8pm]	5pm	30mins
	Oven	1.6	[2pm, 7pm]	3:10pm	60mins
	Dish Washer	1.4	[9pm, 7am]	11pm	80mins
Ω_n^{CA2}	Pool Pump	1.3	[11am,6pm]	1pm	150mins
	Washing Machine	1.0	[12pm,4pm]	2pm	60mins
	Clothes Dryer	1.7	[9am,12pm]	9:20am	70mins
	Vacuum Cleaner	0.5	[2pm, 7pm]	4:30pm	50mins
Ω_n^{CA3}	Air Conditioner	[1, 1.5]	[1pm, 9pm]	N/A	N/A
	Light 1	[0.4, 0.8]	[4pm,10pm]	N/A	N/A
	Light 2	[0.3, 0.6]	[5pm,10pm]	N/A	N/A

It is assumed that the four houses obtained the similar solar radiations because they are located in the same geographical location. Thus, based on their solar panel capacities, we are able to simply scale the PV power profiles according in Fig. 4.5 and assign it to other three houses' solar power output. A set of controllable appliances of individuals is assumed to be controlled by the HEMS program. As a illustration, Table 4.3 presents the House 1's controllable appliances, in which the "desired operation time" represents the exact time when the consumer originally intends to operate the device when the house is connected to the grid. By running all appliances at the desired operation time, the individual desired power consumption profiles are able to gained, described in Fig.4.5.

4.5.2 Grid outage scenario study

Scenario A: 7-h Grid Blackout Study: A seven-hours power blackout period happening in the duration of [12pm, 7pm] is considered, as depicted by the shade band in Fig.4.6.

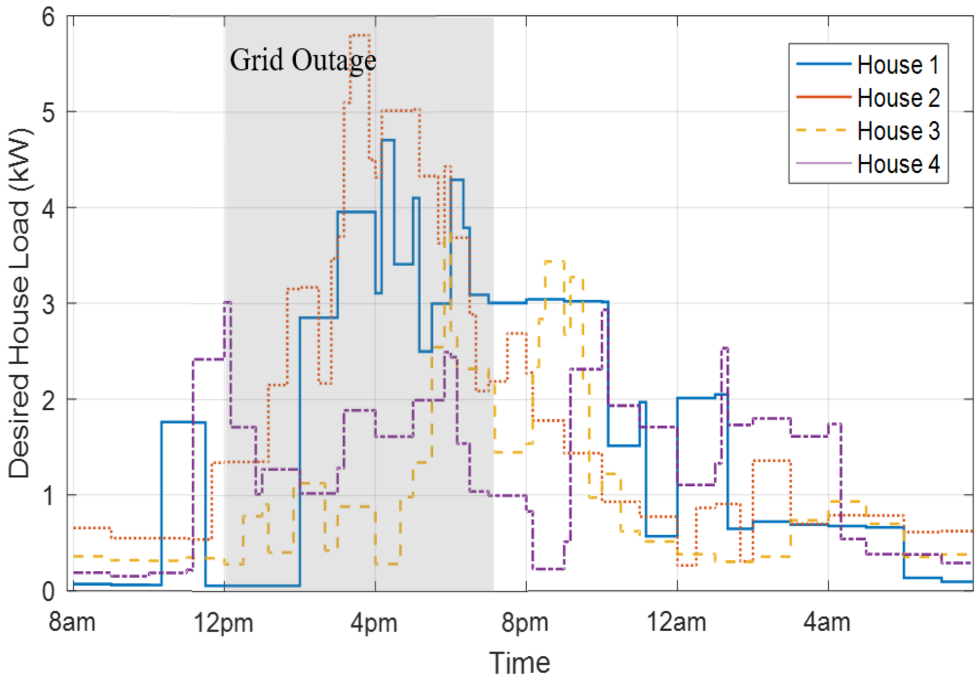


Figure 4. 6 The four-houses desired energy consumption profiles

From Figure 4.3, it can be understood that if there is no proper energy management schemes, numerous household consumption would be lost under the power outage. The proposed energy management scheme is then applied. In terms of the operational constraints of the BESS and appliances, shown in Section 4.3, are applied in the simulation. Aiming as better indicate how the BESS of community accommodate household load-reshaping and the PV solar power, we assume the BESS at the beginning of the power blackout period is almost empty (i.e., its initial SOC is 10%), which means no extra energy can be utilized over the power blackout duration. The comparison between the proposed model and other three cases are as follows:

Case 1: The proposed system installed a energy management strategy and a community BESS.

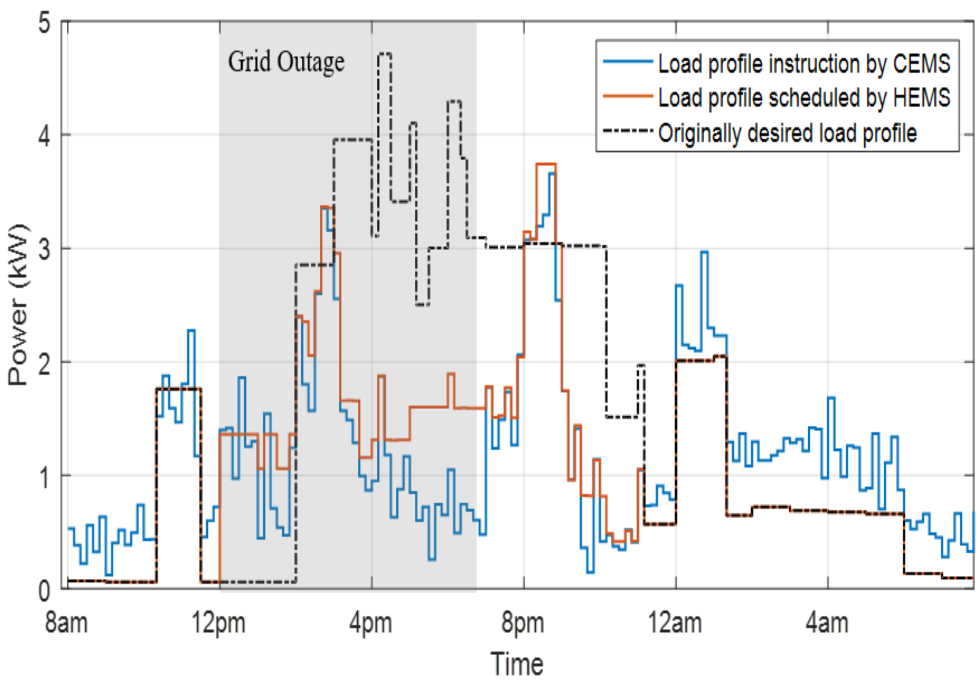
Case 2: A system has not re-shifting load optimization, but implement a community BESS. In this case, regulation-based control strategies on the BESS: the indicated community load is directly compensated by the BESS; the surplus solar power is directly charged into the BESS. Constraints (4.5) - (4.7) are also used to the BESS;

Case 3: A system neither energy management scheme nor community BESS

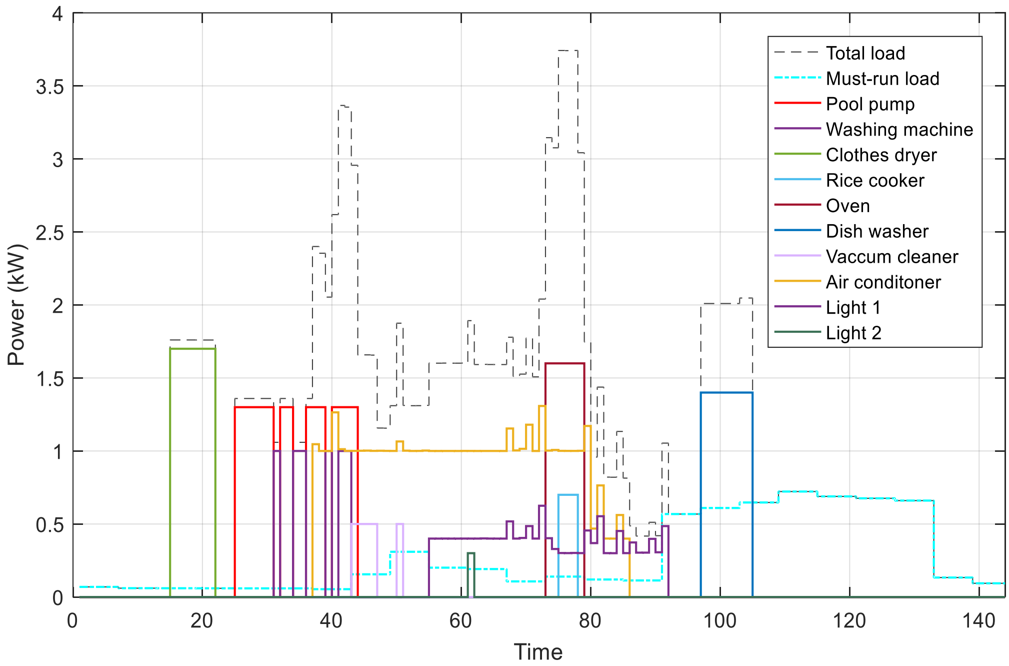
Case 4: A centralized optimization methodology, similar with the ones reported in [134]. All controllable appliances of the four houses and the community BESS are scheduled by a centralized community EMS in this case, subjected to following objective function:

$$\min F^* = \sum_{t=1}^{T^{oh}} (\tilde{L}_t^{lost} \Delta t) \tag{4.18}$$

After seven iterations, the hierarchical energy management process terminates. Fig.4.7 and Fig.4.8 illustrate the final scheduling results. The BESS operation results as well as the re-shaped and desired load of the whole community is shown in Fig. 4.8.



(a)



(b)

Figure 4. 7 Home energy management results of House 1: (a) aggregated scheduling results; (b) appliance-level scheduling results

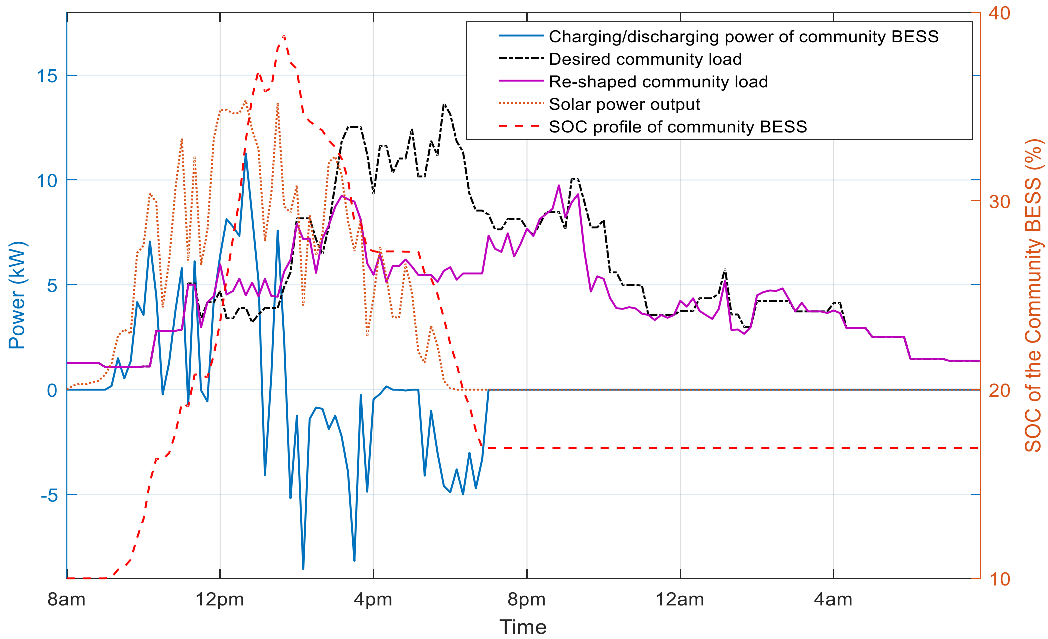


Figure 4. 8 Community scheduling result under the 7-hour outage scenario

According to the results, the community BESS is charged to over 40% energy capacity in the morning time while there is surplus solar power. In the 12-7pm (the grid outage period), the community BESS is responsible to discharged to supply the power. At the same time, to accommodate the BESS the community consumption will be significantly re-shaped when blackout. Fig. 4.7 indicates the House 1's scheduling details. followed with the similar scheduling patterns of other three houses. In Fig. 4.8 (b), the controllable appliances are described with solid line of special color listed in Table 3. It shows that with some unavoidable deviations, each house's HEMS tries to control the devices to follow the instruction of load profile sent from the CEMS.

Table 4.4 represents the numerical comparison results of other four benchmark cases and the proposed scheme. Because Cases 2 and 3 are rule-based, their computational costs are regarded to be zero. The results show that proposed system (Case 1), totally 3.32kWh load of the community is lost over the blackout duration. 30.71kWh load is lost due to the blackout when there is neither no energy management nor BESS(Case 3). There is BESS but no energy reshaped energy management process (Case 2), 14.58k is the unserved load. Case 2 is better than Case 3 but still significantly worse than the proposed model. A centralized optimization case is represented in Case 4 where the social optimal solution could be obtained. However, the resulted huge dimension of the centralized scheduling model leads, on one hand, to very high computing time (more than 18 hours) and, on the other hand, to a hard computational to find the near-globally/globally optimal result. In conclusion, these comparisons well illustrate the efficiency of proposed scheme.

Table 4.4 Comparison results: seven hours power blackout scenario

	Unserved Load (kWh)	Computing Time (minutes)
Case 1	3.32	137
Case 2	14.58	0
Case 3	30.71	0
Case 4	9.56	677

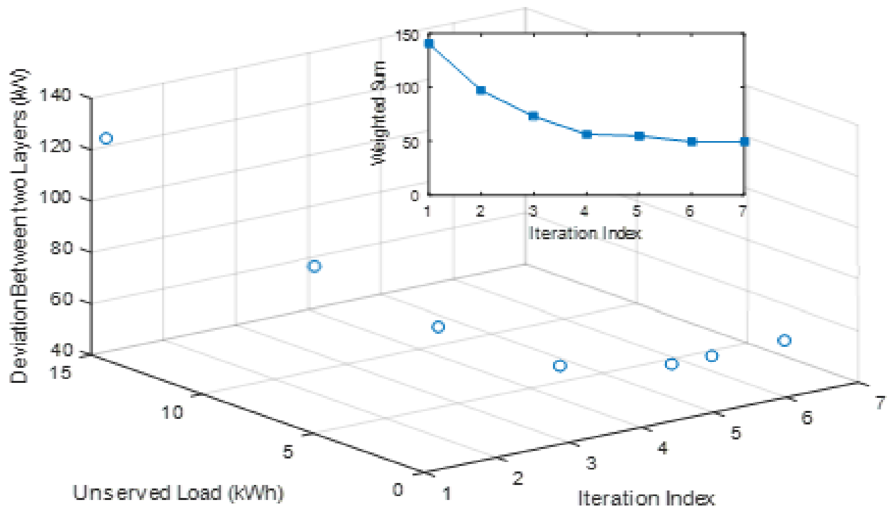


Figure 4. 9 Convergence process of the bi-level programming process.

The convergence results of the iterative NAA programming process are shown in Fig. 4.9. The significant big figure describes the two objective values' variation of model (4.1), and the small figure indicates the weighted sum of the two objective values with the setting of $\alpha = 1$. Until the 7th iteration, the weighted sum is improved iteratively, which indicates the convergence of the bi-level programming process.

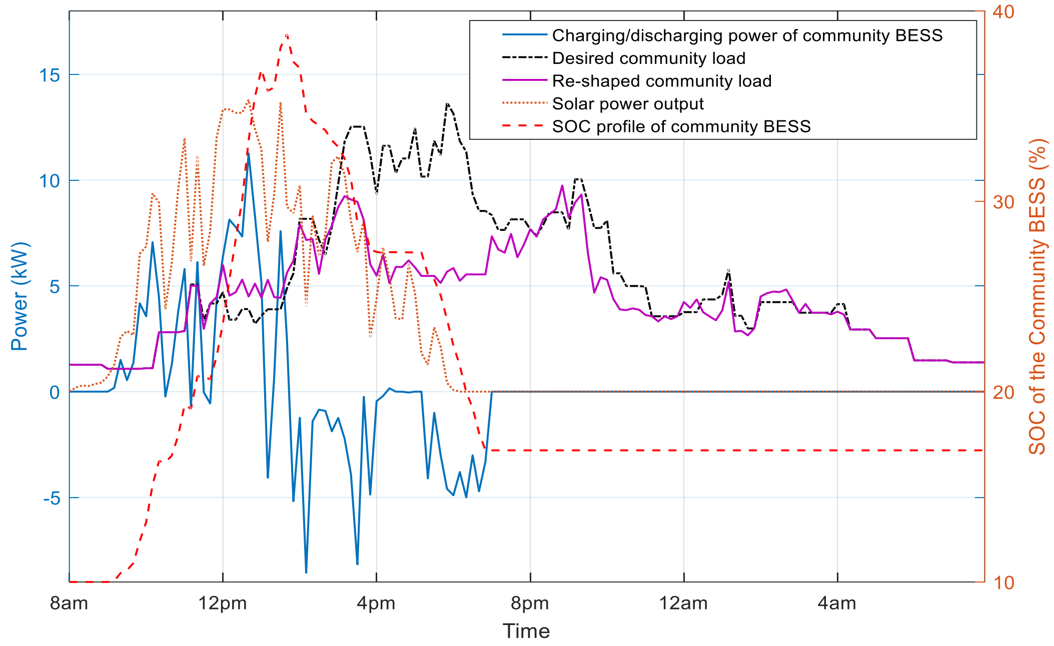


Figure 4. 10 Community scheduling result under the 24-hour outage scenario

Scenario B: 24-h Grid Blackout Study: A 24-hours power blackout event is also considered in this study for validate the system robustness and efficiency. The result of community optimization is presented in Fig.4.10 and the comparison result is shown in Table 4.5.

Table 4.5 Comparison results: 24-hour grid outage scenario

	Unserved Load (kWh)	Computing Time (minutes)
Case 1	52.49	526
Case 2	79.89	0
Case 3	101.72	0
Case 4	NA	NA

Again, the Table 5 reported the efficiency of proposed system (only lost 52.49kWh load); if there is no energy management and/or BESS (Case 2 and Case 3), the community would be influenced significant due to the power blackout. In this case, because of the huge computation dimension, the centralized optimization cannot be solved (Case 4).

Table 4.6 Comparison results of unserved load with different community sizes

	Case 1	Case 2	Case 3	Case 4
10 Houses	9.74kWh	38.89kWh	66.67kWh	NA
20 Houses	22.53kWh	72.02kWh	138.95kWh	NA
30 Houses	33.88kWh	124.18 kWh	205.54kWh	NA
100 Houses	167.50kW	324.53 kW	443.12kWh	NA
200 Houses	493.72 W	754.31 kW	987.61kWh	NA

Evaluation with Multiple Community Sizes: The larger number of houses are also discussed in order to evaluate the community size's influence. The blackout period is decided from 12pm to 7pm. We simply duplicate the four houses' implementation with some small modifications to validate other houses. Correspondingly, the power capacity of the community with the 10-, 20-, 30-, 100-, and 200-house scenarios, and BESS is installed 20kW, 40kW, 60kW, 180kW, 360kW respectively. Their unserved-load results are reported in Table 4.6. Compared to the results obtained with the other benchmark schemes, our proposed model can supply more power for the community with the increase of house number.

4.6 Chapter Summary

A hierarchical energy management system is proposed in this chapter, which validate the system is able to facilitate the self-serve energy capability of the residential community under power blackout. In order to solve the high optimization dimensions' difficulty caused by the large number of residential energy appliances in the community, the developed model decomposes the power management process into two levels. According to the simulation results, the proposed model enables to significantly increase the self-supply duration for large number of residents under blackout through iterative communications between the individual HEMSs and CEMS. Furthermore, this design is also benefit to protect the security and privacy of individual information (i.e., appliance-level scheduling data).

CHAPTER 5.

Evolutionary Aggregation Approach for Multihop Energy Metering in Cyber-Physical Grid for Residential Energy Management

5.1 Introduction

The previous chapter developed a robust system by improving the self-serve capability of CPS demand management under outage scenarios. In addition, cyber-physical grid is also an intelligent energy network with a complicated communication network incorporated into traditional physical framework. Due to the evolution of wireless technology such as NB-IOT [135] and LoRa [136], residential intelligent appliances are able to communicate and even re-control the grid generation by the local data nodes. To satisfy the operation of developed CPS grid, a robust and reliable communication network is essential to enhance the communication, monitoring and control the information. The breakdown and failure of communication network will cause significant security accident and economic loss. In addition, the implementation of smart meters [137] enable to bill electricity and collect data, which facilitates response, reliability and robustness. There are several studies on smart metering network in demand side. In [138] , the Sub 1-GHz urban path loss model is proposed to optimize the data transmission in local area; [139] demonstrates the security of physical level. In [140] a performance analysis is proposed on Sub 1-GHz wireless sensor networks in CPS grid. In [141], a priority strategy of data transmission is proposed in wireless sensor network

(WSN) based CPS grid, which minimum the delay based on the priority. In [142], a application of home energy management to evaluated the packet delay variance (PDV), delay, and delivery ratio for varying network sizes and interval times.[143] induces an scheduling optimization for home appliances and energy management to minimize the appliances power cost. An aggregation latency algorithm on data collection [144] and switching traffic scheduling algorithm [145] are discussed to facilitate the data communication network.

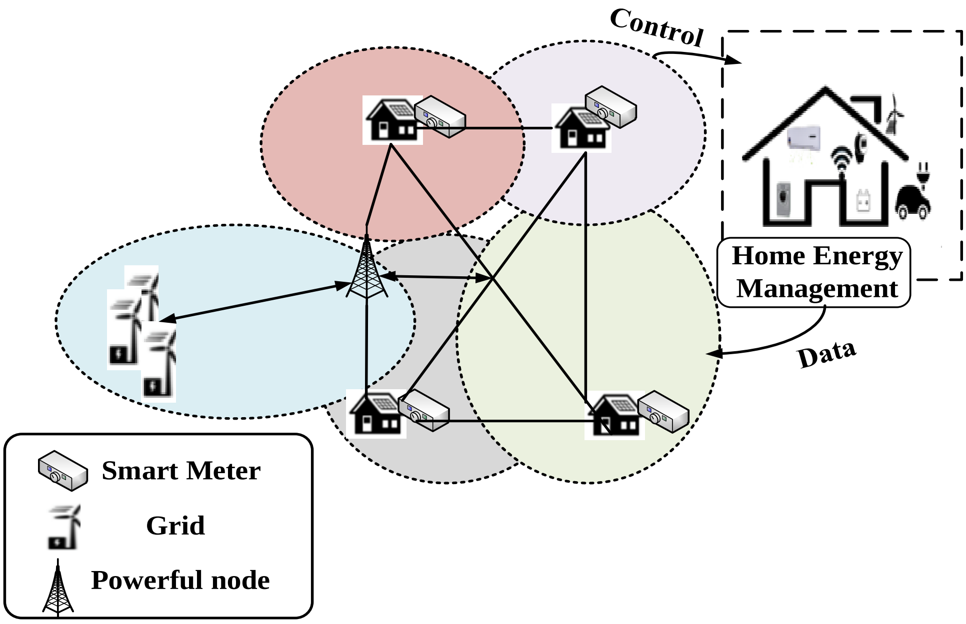


Figure 5. 1 Smart meter-based communications network

In the traditional network, each general node is required to transfer its collected data to data center for satisfying the connectivity via one data aggregation center. The risk of implementing a great number of nodes is very high. Based on the smart meters, the data aggregation center is able to collect and transfer the data in residential CPS wireless network, which enable to decrease the installed powerful nodes and enhance the robustness of communication network (see Fig. 5.1). Since a large number of sensor devices such as phasor measurement unit (PMU) and smart meter are installed in CPS demand side, therefore, the sampling frequency of sensor devices will increase significantly, and there is much more information that the system required to transmit and process compared to the current power system. This determines that the dependence of CPS demand-side on computing system and communication network will increase significantly. For the cost requirement in reality, for a large number of smart meters, smart home appliances and other terminals, a feasible way is to use public communication networks such as wired telephone network and Internet to achieve communication. However, that will make the communication delay, communication system reliability, information system security and other issues become an important factor affecting the overall performance of CPS demand side. In addition, due to the lack of information transmission and processing capacity, the current power system dispatching organization can only rely on its own controller for decentralized local control of a large number of devices in the system, (i.e., small capacity distributed generation, protection devices, etc.), which makes the system inefficient because it cannot coordinate all available resources. In order to meet the requirements of CPS demand-side energy management for self-serving, high reliability, and robustness, it is necessary to carry out novel communication network control for the above equipment. This will further enhance the robustness of CPS demand side on communication system.

There are some previous research works have been done. [146] [147] discuss the communication reliability of multiple-hop environment. The author of [148] reports the communication links' importance for wireless network. However, allocating number and locations of aggregation center is less studied.

The next section will propose a new evolution algorithm (EAA) to minimum the number and location of aggregation center in multi-hop smart meters environment. Two new adaptive operations (the shuffle and switch operation) will be designed and installed in this following sections. Numerical simulations and case studies are demonstrated to validate the efficiency of proposed n-hop mathematical model.

5.2 Mathematical Model

5.2.1 Communication Network Definition

The schematic of communication network is presented Fig. 5.1(a), denoted by N (α ; S^2 ; , N_g , S_s). There are two types of nodes in the wireless smart meter network: residential smart meters N_g installed in demand side of users' and local data center referred as powerful nodes . The number of residential nodes is defined as $N_g = \{g_{0,} g_{1,} g_{2,\ldots} g_k\}$, where g_k is the kth residential node's geometry location (i.e., in Fig.5.2(a), g_k =11). The local data center （powerful node) refers as N_m ={ m_0 , m_1 , m_2 ..., },where is the number of local data center, is the nth geometry location's data center. Each smart meter's transmission scope can be defined as S_s = { S_0 , S_1 , S_2 ..., S_n). The general node is Poissonly i.i.d. with a known density α in the square R^2 where R is length of side. The connections between general nodes and data center followed the model, in which for $g_a \in N_g$ with transmission range $s_a \in S_r$; $m_b \in N_m$, and the Euclidean distance $\| g_a - m_b \| \leq s_a$, the g_a and m_b are defined can be connected. All local data centers are assumed to be connected to the central data center. In the proposed n-hop network, the packets of other smart meters can be replayed to the local data center. The unit desk connection model is used to connect two general nodes, i.e., $g_a, g_b \in N_g$ with the transmission scopes $s_a, s_b \in S_s$, g_a, g_b can be connected if their Euclidean distance followed $\| g_a - g_b \| \leq s_a + s_b$.

5.2.2 Problem Formulation

In the designed communication network, given the information as following: (1) The distributed location of each smart meter $g_a \in N_g$ installed in the area R^2; (2) The smart meters $g_a \in \{1,2,..n\} \in N_g$; each smart meter $g_a \in N_g$ followed the transmission range $s_a \in \{1,2,..n\} \in S_s$; (3) The maximum number of wireless data packet can be relayed is *t.* In order to satisfy the full connectivity, we propose to determine the minimum quantity of the data centers $(M_{ba} = \{m_{1.}, m_2..m_k\})$ and their geometry locations that must be established in the map. In this section we introduce the *n*-hop (*n*>=2) wireless remote metering network model. A novel 2-hop EAA which could obtain the optimal result in a 2-hop network is implemented as Fig. 5.2(c).

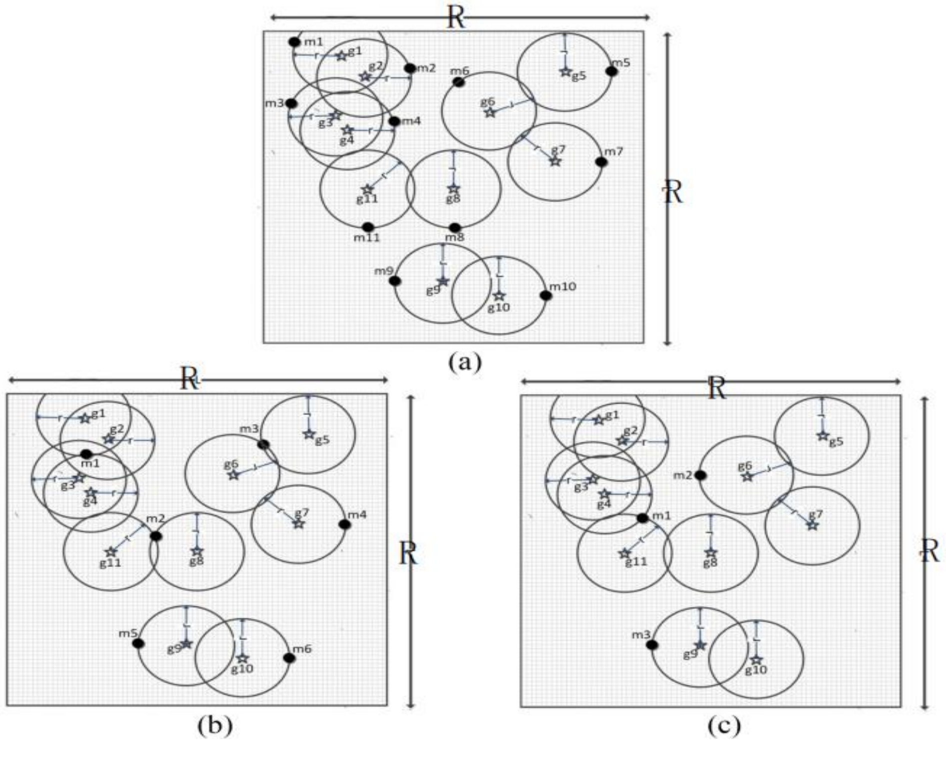


Figure 5. 2 The wireless network with smart meters

In the 2-hop EAA, we present two novel adaptive operations (Switch operation and

Shuffle operation) to improve the algorithm performance. Furthermore, the 2-hop EAA is extended to a more generic algorithm for solving the *n*-hop optimization problem in a multiple hop smart meters network is proposed.

5.3 Evolutionary Aggregation Algorithm for Two-Hop Network

Table 5.1 Algorithm of High-Level Structure of the Evolutionary Aggregation

Start
Create an Initial Population $G_x = \{Y_{1,x}, Y_{2,x} ... Y_{n,x}\}$, let $x = 1$
WHILE (y<MaxGeneration)):
Rank all $Y_{i,x}$, $i \in [1:n]$ in G_x
Select top *m(m<n)*solutions from G_x as $G_s^{'} = \{Y_{1,x}, Y_{2,x} ... Y_{m,x}\}$
WHILE *m* not equal to *n*:
Randomly generate three integer *s1, s2, s3*∈ [1:*m*] and *a* ∈ [0: 1]
IF *(a >= β)*:
Generate two new solutions $Y_{m+1,x}$, $Y_{m+2,x}$ from *Switch* $(Y_{s1,x}, Y_{s2,x})$
Add $Y_{m+1,x}$, $Y_{m+2,x}$ to $G_n^{'}$
m=m+2
ELSE:
Generate a new solution $Y_{m+1,x}$ from *Shuffle* $(Y_{s3,x})$
Add $Y_{m+1,x}$ to $G_n^{'}$
m = m +1
ENDIF
ENDWHILE
$x = x + 1$
$G_x = G_n^{'}$
ENDWHILE
Select the best $Y_{i,x}$, $i \in [1:n]$ from G_x
End

An evolutionary aggregation is used to solve the proposed problem （see Table 5.1), and we define that there are $G_x = \{Y_{1,x}, Y_{2.x}, ... Y_{s,x}\}, x = 1$ initial population. The number of populations is x and the initial solution's number is s in the generation. The termination parameter of the algorithm is represented as M*axGeneration* in the table. A feasible solution $\mathrm{Y}_{i,x}, i \in [1: n]$ in population, consisting of multiple node cluster $\{F_1, F_2, ...F_j\}$ which data can be collected and transferred through the same local data center ($\mathrm{F}_k, k \in [1: j] = \{x_{a1}, x_{a2...}x_{ak}\}$). To obtain the optimization result, Table 5.1 has three crucial procedures:(a) Obtain random results ($\mathrm{Y}_{\mathrm{i},x}, i \in [1: n]$) from step 1 of EAA algorithm; (b) Generate two novel solutions from *Switch* ($\mathrm{Y}_{s1,x}, Y_{s2,x}$) in step 8; (c) From step 11, generate a novel solution *Shuffle* $\mathrm{Y}_{s3,x}$. The approach only implements the random solution generator. The original EAA is able to obtain the optimal results but takes very long time implementing the random solution generator. Therefore, two new generators (Switch and Shuffle) of EAA provide ability to improve the performance of algorithms. To achieve the same optimal result, the processing time is reduced greatly by two novel operators. The comparison between the EAA with operators and the original EAA on the Section is shown in Chapter 5.5.3.

5.3.1 Generating Random Solutions

According to the previous work, the solution of one hop smart meter network can be obtained $\{\mathrm{Y}_i^1, \mathrm{i} \in [1: \mathrm{N}]$, and the result of two-hop network is $\{\mathrm{Y}_{\mathrm{i}}^2, i \in [1: N]$. The solving details as Algorithm 5.2. To be specific, Y_i^1 is the solution of one-hop network, constituting by p node clusters. Every cluster has multiple general nodes which are served by a local data center in one-hop network. Assume that $\mathrm{Y}_i^1 = \{F_1^1, F_2^1 ... F_p^1\}$ and

$$\mathrm{F}_1^1 = \{x_{f1,1}^1, x_{fz,2}^1, x_{f1,3}^1 ... x_{f1,t1}^1\};$$

$$\mathrm{F}_2^1 = \{x^1_{f2,1}, x^1_{f2,2}, x^1_{f2,3} \ldots x^1_{f2,t2}\};$$

...

$$\mathrm{F}_{\mathrm{j}}^1 = \{x^1_{fj,1}, x^1_{fj,2}, x^1_{fj,3} \ldots x^1_{fj,tk}\};$$

where $x^1_{fj,tk}$, $j \in [1:\mathrm{N}], k \in [1:N]$ is one of general nodes; each cluster $\mathrm{F}_n^1, n \in [1:N]$ consists of the number of general nodes $\{t1, t2 \ldots t\mathrm{k}\}$. In Table 5.2, the step 4 and step 8 represent to remove the node x or cluster $\mathrm{F}_{\mathrm{p}}^1$ from the set of cluster $\mathrm{Y}_{\mathrm{i}}^1$; the step 12 of subtract operator shows a new cluster F_p^2 is added into the $\mathrm{Y}_{\mathrm{i},1}^2$ cluster. F_p^2 is satisfied the two-hop network. Step 6 shows two nodes interact with each other within their transmission scopes.

Table 5.2 Algorithm of High-Level Structure Generating the Initial Solution for Two-Hop Network

Start
$Y_{i,1}^{2} = \{\}$
WHILE Y_i^1 still has Clusters:
Randomly pick a cluster F_p^1 from Y_i^1
$Y_i^1 = Y_i^1 - F_p^1$
FOR each general node $x \in Y_i^1$:
IF *x* intersects with any of the nodes in F_p^1:
Join *x* into the cluster F_p^1
$F_i^1 = F_i^1 - x$
ENDIF
ENDFOR
$F_p^2 = F_p^1$
$Y_{i,1}^2 = Y_{i,1}^2 + F_p^2$
Regenerate Y_i^1
ENDWHILE
$Y_{i,1}^2$ is an initial solution which satisfies the two-hop network
End

5.3.2 Switch Operation

A novel adaptive operator, Switch Operation, is introduced to enhance the performance of EAA algorithm as Table 5.3. F_{s1} and F_{s2} are the cluster sets picked randomly from the parent results $Y_{s1,,x}$ and $Y_{s2,,x}$. In step 8, two solutions （$Y_{m+1,\ x}$+ $Y_{m+2,x}$） in two-hop condition from the random results ($Y_{s1,\ x}$, $Y_{s2,\ x}$).

Table 5.3 Algorithm of Switch Operation

Start

1 Randomly pick $F_{s1} = \{x1, x2...xn\}$ from $F_{s1,x}$

2 Randomly pick $F_{s2} = \{x1, x2...xn\}$ from $F_{s2,x}$

3 *NodeSet* $Y_{s1,x}$ = {} and *NodeSet* $Y_{s2,x}$ = {}

4 **FOR** each general node $x_{s1,inx}$ in F_{s1}

5   **IF** $x_{s1,inx} \notin NodeSet\ Y_{s2,x}$

6   Find $F_{s2,inx}$ which contains $x_{s1,inx}$ in $F_{s2,x}$

7   Add all nodes of $F_{s2,\mathrm{in}x}$ into *NodeSet* $Y_{s2,x}$

8       $Y_{s2,x} = Y_{s2,x} - F_{s2,inx}$

9   **ENDIF**

10 **ENDFOR**

11 **FOR** each node $x_{s1,inx}$ in F_{s2}

12   **IF** $x_{s2,inx} \notin NodeSet\ Y_{s1,x}$

13   Find $F_{s1,\mathrm{in}x}$ which contains $x_{s1,inx}$ in $x_{s1,inx}$ in $F_{s1,x}$

14   Add all nodes of $F_{s1,\mathrm{in}x}$ into *NodeSet* $Y_{s1,x}$

15       $Y_{s1,x} = Y_{s1,x} - F_{s1,inx}$

16   **ENDIF**

17 **ENDFOR**

18 $NewSubClust_{s1} = \mathrm{Re}GenClust(NodeSet Y_{s1,x})$

19 $NewSubClust_{s2} = \mathrm{Re}GenClust(NodeSet Y_{s2,x})$

20 $F_{m+1,x} = F_{s1,x} + NewSubClust_{s1}$

21 $F_{m+2,x} = F_{s2,x} + NewSubClust_{s2}$

End

In Table 5.3, procedure 4-10 find cluster sets from $Y_{s2,x}$ ($F_{s2,inx}$) that consists the nodes in F_{s1} which picked randomly from $Y_{s1,x}$. Furthermore, the $F_{s2,\mathrm{in}x}$ clusters are removed from the $Y_{s2,x}$ solutions, which separate different nodes and added to the NodeSet. $Y_{s2,x}$ sets. Procedure 19 ReGenClust () utilizes the algorithm of Table 5.2 to generate new clusters of two-hop NewSubClusts2. Step 21 generates $F_{\mathrm{m}+2,x}$ through adding the NewSubClusters2 clusters into the $F_{s2,x}$. The same logic can be solved in

$F_{m+1,x}$.

5.3.3 Shuffle Operation

Table 5.4 Algorithm of Shuffle Operation

Start	
1	Solution $Y_{s3,x} = \{F_{s3,1}, F_{s3,2} ... F_{s3.t}\}$
2	Generate a random number $x \in [1:t]$
3	Select *p* clusters $F_{s3,sub} = \{F_{s3,t1}, F_{s3,t2} ... F_{s3,tp}\}$ from $F_{s3,x}$
4	$F_{s3,x} = F_{s3,x} - F_{s3,sub}$
5	$MuNodeSet_{r3} = \{\}$
6	**FOR** each cluster $F_{s3,inx}$ in $Y_{s3,sub}$
7	**FOR** each node x_{inx} in $F_{s3,inx}$:
8	$MunodeSet_{s3} = MuNodeSet_{s3} + x_{inx}$
9	**ENDFOR**
10	**ENDFOR**
11	$Y_{s3,newSub} = ReGenClust(MuNodeSet_{s3})$
12	$Y_{m+1,x} = Y_{s3,x} + Y_{s3,newSub}$
End	

Table 5.4 represents the Shuffle Operation details. The *p* clusters are selected from $F_{s3,x}$ solutions randomly that is consisted by *t* cluster sets in procedure. Each node picked into a set $(MuNodeSet_{s3})$ and then generate a new cluster to support the 2-hop network in procedure 5-10. The procedure 11 $ReGenClust()$ function utilize Table 5.2 to regenerate a novel 2-hop supporting cluster set ($Y_{s3,newSub}$). In procedure 12, the new result $Y_{m+1,x}$ is obtained by $Y_{s3,newSub}$ added into $Y_{s3,x}$.

5.4 Evolutionary Aggregation Algorithm for N-Hop Condition

This section the EAA solutions for n-hop network will be discussed. The structure of n-hop EAA is same as the 2-hop's structure (Table 5.1). The initial population is generated by initial method, moreover, Switch and Shuffle operations are used to spawn several children from the parent solutions. The optimal solution will be obtained after the algorithm reached the maximum generation number.

In addition, since the complexity increased with the increasing hops, new approaches are proposed for multiple-hop wireless conditions as follows.

5.4.1 Generating Random Solutions for N-Hop Network

Table 5.5 shows the generation structure of the initial result $\mathrm{F}_{i,1}^{n}$ in multiple-hop network, which is based on the solution F_{i}^{n-1} that support the multiple hop network. Similar to the Table 5.2, the procedure 4 and procedure 8 in Table 5.5 remove the node x or cluster F_{p}^{n-1} from set F_{i}^{n-1}. The new cluster F_{p}^{n} is added to the cluster $\mathrm{F}_{i,1}^{n}$ in procedure 12. F_{p}^{n} is the node set to support the multiple-hop condition, in which the node can served by one local data center in the multiple-hope network. The function $\mathrm{Y}_{\mathrm{i},1}^{n} = \mathrm{F}n(\mathrm{Y}_{\mathrm{i}}^{n-1})$ shows the entire steps of generating $\mathrm{Y}_{i,1}^{n}$ from $\mathrm{Y}_{i,1}^{n-1}$. Table 5.6 illustrates satisfying n-hop result $Y_{i,1}^{n}$ from one-hop Y_{i}^{1}.

Table 5.5 Algorithm of Generating the Initial Solution for n-hop Network

Start

$Y_{i,1}^{n} = \{\}$

WHILE Y_i^{n-1} still owns Clusters

Randomly select a cluster F_p^{n-1} from Y_i^{n-1}

$Y_i^{n-1} = Y_i^{n-1} - F_p^{n-1}$

FOR each general node $x \in Y_i^{n-1}$:

IF *x* intersects with any of the nodes in F_p^{n-1}

Join *x* into the cluster F_p^{n-1}:

$Y_i^{n-1} = Y_i^{n-1} - x$

ENDIF

ENDFOR

$F_p^{n} = F_p^{n-1}$

$Y_{i,1}^{n} = Y_{i,1}^{n} + F_p^{n}$

Regenerate Y_i^{n-1}

ENDWHILE

$Y_{i,1}^{n}$ is an initial result that satisfies the *n*-hop network

End

Table 5.6 N-Hop Algorithm of Generating the Solution from the Solution Satisfies 1-Hop

Start

$Y_i^{it} = Y_i^{1}$

FOR *k*=1 to *n*-1

$Y_i^{k+1} = Fn(Y_i^{it})$

$Y_i^{it} = Y_i^{k+1}$

ENDFOR

$Y_{i,1}^{n} = Y_i^{it}$

End

5.4.2 N-Hop Network Switch Operation

The n-hop logic structure of switch operation is similar to Table 5.3, where $F_{s1,x}$ and $F_{s2,x}$ are the cluster sets picked randomly from the parent results $Y_{s1,x}$ and $Y_{s2,x}$. From procedure 4-10, the algorithm solves clusters in $Y_{s2,x}(F_{s2,inx})$ that consists of the nodes in F_{s1} which is selected randomly from $F_{s1,x}$. Furthermore, the ($F_{s2,inx}$) clusters are removed from the result $F_{s2,x}$, which can be broken into separate nodes and then added to the $NodeSetx_{s2,x}$ set. The function $\mathrm{Re}GenClust()$ of Table 5 and Table 6 is used to generate new satisfying clusters $NewSubClust_{s2}$ for n-hop network from $NodeSetx_{s2,x}$ nodes, then, by adding the clusters $NewSubClust_{s2}$ into $F_{s2,x}$, the $F_{m+2,x}$ is obtained. The solution of $F_{m+1,x}$ also can be solved through the same logic. Because of the page limitation, the pseudocode of multiple-hop will not list.

5.4.3 N-Hop Network Shuffle Operation

The logic structure of n-hop network's shuffle operation is same as the Table 5.4 which is not drawn here due to the page limitation. We also use Table 5.4 to demonstrate its procedures. Form the solution $F_{s3,x}$, the procedure 2-3 pick x clusters to satisfy the n-hop network. Procedure 5-10 to add each node of the picked clusters into the set ($MuNodeSet_{s3}$) that can generate a new cluster set to support multiple-hop network. The function $\mathrm{Re}GenClust()$ in procedure 11 in Table 5 and Table 6 to regenerate the new cluster set ($Y_{s3,newSub}$) for n-hop. The solution $Y_{m+1,x}$ is generated by adding the $Y_{s3,newSub}$ cluster into $Y_{s3,x}$

5.5 Numerical Analysis and Case Study

All algorithms and model are conducted in Matlab and executed on a computer with 8-GB RAM 32 GHz CPU. The EAA algorithm's parameters are as Table 5.7, where *n* is the number of results in every generation; *m* is the number of elite results picked from every generation; *MaxGeneration* is the termination parameter of the algorithm that the EAA is able to terminate and exit when the *MaxGeneration* obtained. Because the total number of smart meters is known in simulation, the sufficient trails can be done to achieve the optimal *MaxGeneration* value. After that, 500 is the best setting for *MaxGeneration* in the following cases; ∂ is the factor to set the using of Shuffle and Switch operators. All parameters are defined in Table 5.7.

Table 5.7 EAA Parameters

Parameter	Value	Parameter	Value
n	100	m	60
MaxGeneration	500	∂	0.5

5.5.1 Different Smart Meter Scenario Study

We simulate a residential system with different numbers of smart meters, random locations and random transmission scopes. EAA algorithm is used to solve the optimal solution in 1-hop, 2-hop and n-hop communication networks (see Table 5.8). There are 15 cases have been done in this paper, and the performance evaluation and statistic solutions are presented in Table 5.9 and Table 5.10. In addition, since the page limitation, the graphic result of three typical studies will be posted in this section (Fig.5.3-5.5).

Scenario A: 21 Smart Meters We consider a residential system with 21 smart meters in different networks (1-hop, 2-hop, 3-hop, 4-hop). The circles represent the transmission scopes of every smart meter, whose middle located the smart meter. The local data centers are demonstrated as the highlighted dark dot which is able to serve communication to surrounding smart meters. Fig.5.3 (a) shows the optimal result by EAA Algorithm in 1-hop network. Fig.5.3 (b) shows the optimal result in 2-hop network. In the figure, we can understand that there is less local data centers required because the smart meters are able to relay the packet. Fig.5.3 (c) is the optimal result in 3-hop network. Compared to Fig.5.3 (b), the N0.17 and No.20 smart meters are not required since No.14 and No.9 smart meters enable to relay the communication to their local data center. Fig.5.3 (d) is the optimal result in 4-hop network, where the least number of local data centers are needed in these four scenarios.

Scenario B: 41 Smart Meters Fig.5.4 demonstrates a residential system with 41 smart meters communication network. The comparison results in 1-hop, 2-hop, 3-hop, 4-hop are shown Fig.5.4(a), Fig.5.4(b), Fig.5.4(c), Fig.5.4(d) respectively.

Scenario C: 61 Smart Meters Fig.5.5 illustrates 61 smart meters residential system by EAA algorithm. Fig.5.5 (a) represents the optimal result by EAA Algorithm in 1-hop communication network, where need the largest number of local data centers. Fig.5.5 (b) shows the optimal result of 61 smart meter in 2-hop network. Fig.5.5 (c) is the optimal result in 3-hop network and Fig.5.5 (d) is the optimal result in 3-hop network. From these figures, we can see that there is less local data centers required with the increased number of hops since the smart meters are able to relay the packet.

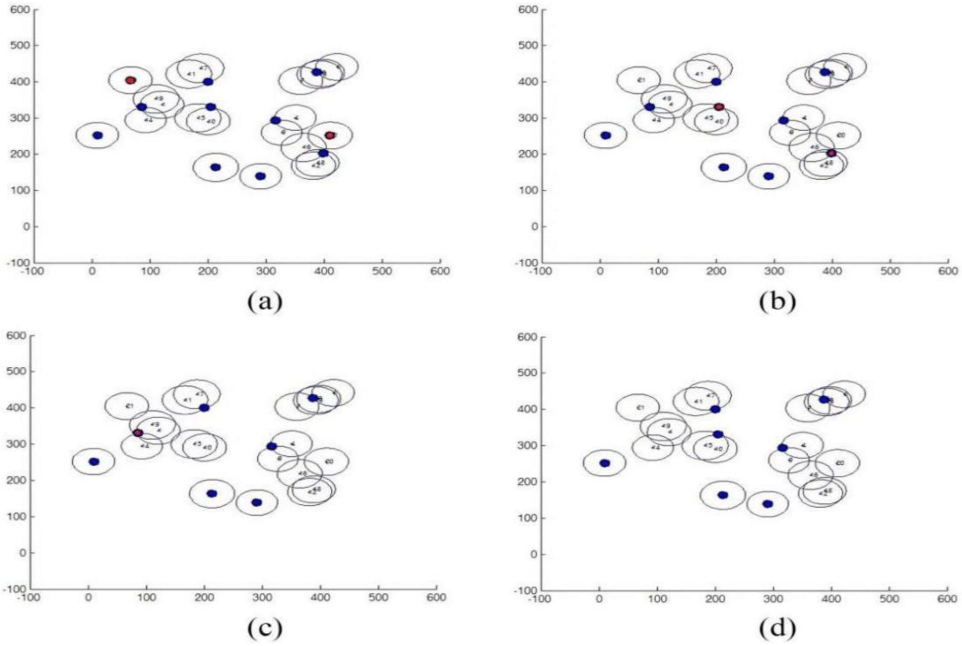


Figure 5. 3 21 Smart meters scenarios (a)1-hop; (b)2-hop; (c)3-hop; (d)4-hop

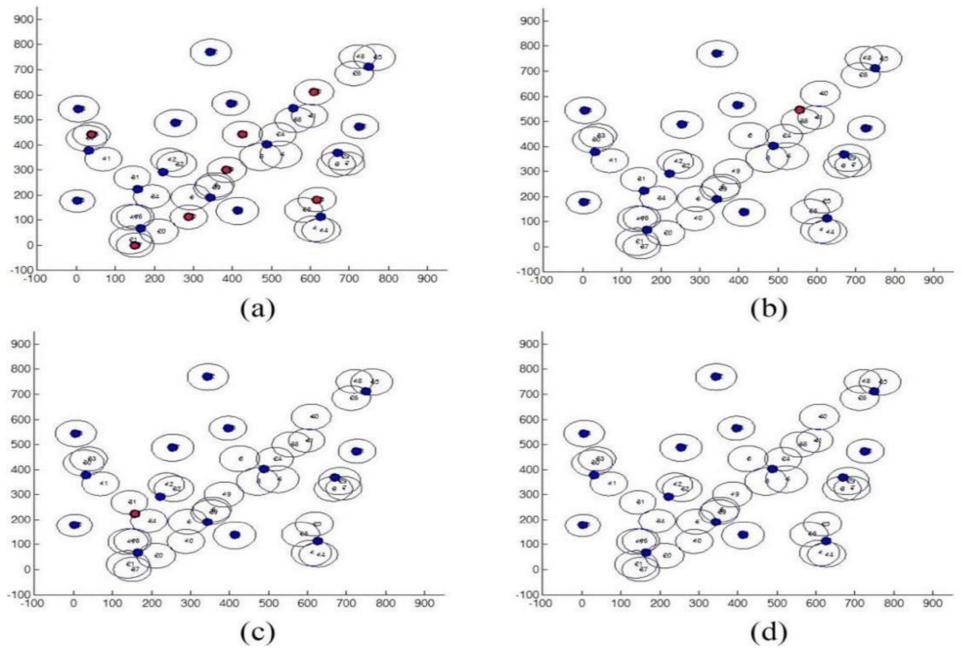


Figure 5. 4 41 Smart meters scenarios (a)1-hop; (b)2-hop; (c)3-hop; (d)4-hop

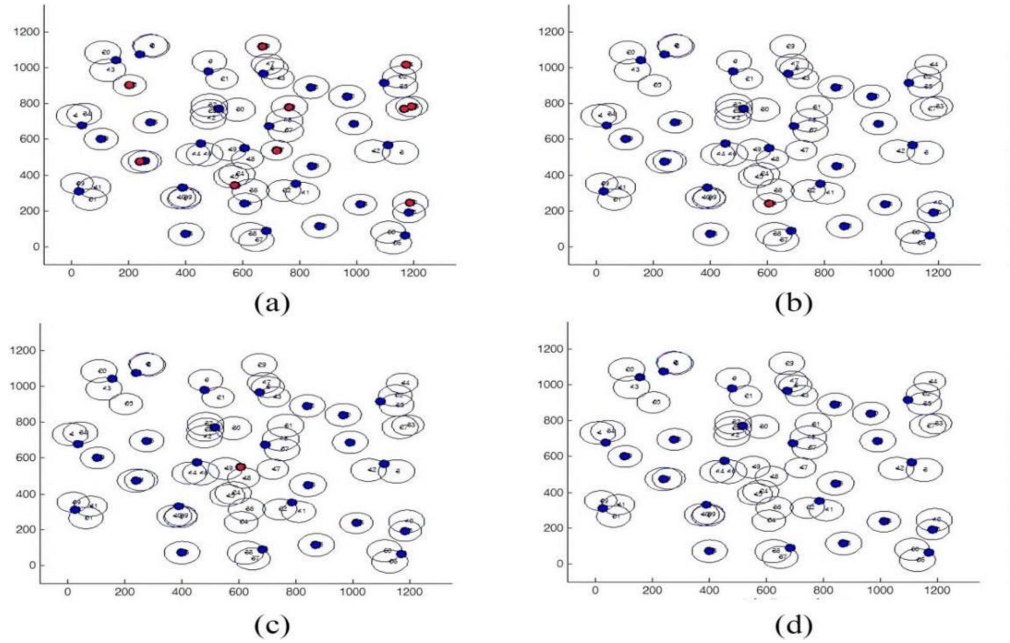


Figure 5. 5 61 Smart meters scenarios (a)1-hop; (b)2-hop; (c)3-hop; (d)4-hop

Table 5.8 Evaluation Cases

	Smart Meter Number	Map Size	Transmission Range
1	21	450	[35-40]
2	41	800	[45-55]
3	61	1200	[55-65]
4	81	1600	[75-85]
5	101	2000	[85-95]
6	121	2400	[90-100]
7	141	2800	[95-105]
8	161	3200	[100-110]
9	181	3600	[105-115]
10	201	4000	[110-120]
11	221	4400	[115-125]
12	241	4800	[120-130]
13	261	5200	[125-135]
14	281	5600	[130-140]
15	301	6000	[135-145]

Table 5.9 Number of Local Data Center of Fifteen Cases

	Smart Meter Number	One-hope Network	Two-hope Network	Three-hope Network	Four-hope Network
1	21	11	9	7	7
2	41	24	17	16	15
3	61	38	28	27	26
4	81	47	39	32	29
5	101	55	45	40	36
6	121	61	55	47	41
7	141	72	66	54	49
8	161	89	74	60	53
9	181	98	90	78	67
10	201	110	91	80	68
11	221	130	92	86	71
12	241	142	99	90	73
13	261	149	105	101	84
14	281	169	122	113	95
15	301	172	136	125	102

Table 5.10 Processing Time of Fifteen Cases (Seconds)

	Smart Meter Number	One-hope Network	Two-hope Network	Three-hope Network	Four-hope Network
1	21	0.03	8.57	369	1098
2	41	0.12	33.29	1420	4623
3	61	0.24	54.87	2140	6405
4	81	0.59	100.3	3031	8983
5	101	0.98	201.1	4985	14875
6	121	2.14	376.3	6310	19013
7	141	4.01	512.9	9001	26068
8	161	5.67	694.9	11743	33063
9	181	6.33	887.3	14689	45872
10	201	7.08	1185.9	17330	52063
11	221	7.91	1674.5	21201	62971
12	241	9.87	1949.9	26300	77459
13	261	10.79	2220.5	29045	99371
14	281	11.98	2847.8	36013	106698
15	301	13.07	3417.9	40936	124479

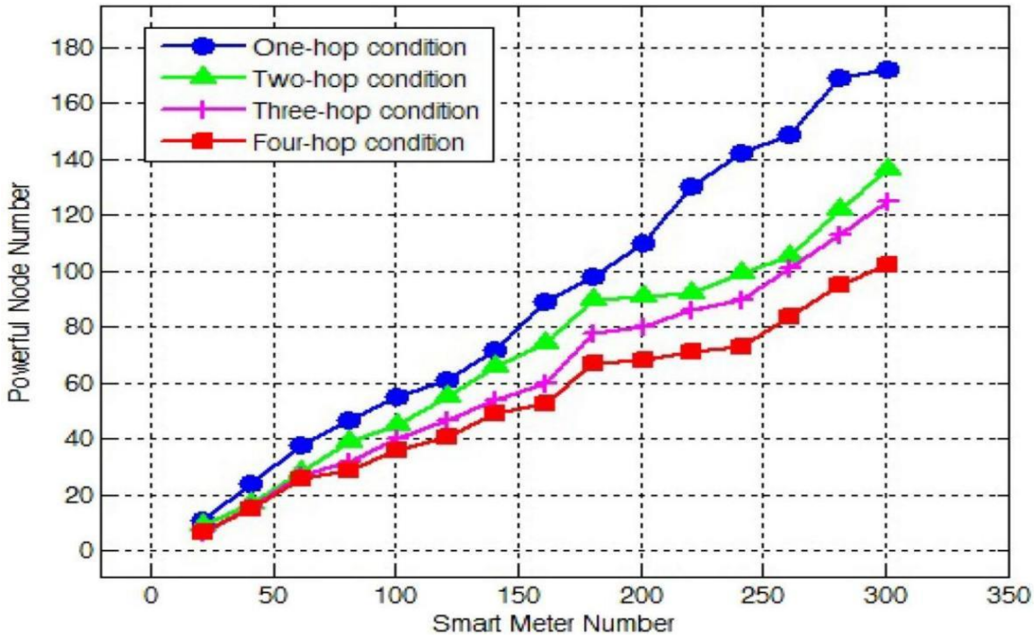


Figure 5. 6 The number of local data center for all cases in multiple network conditions.

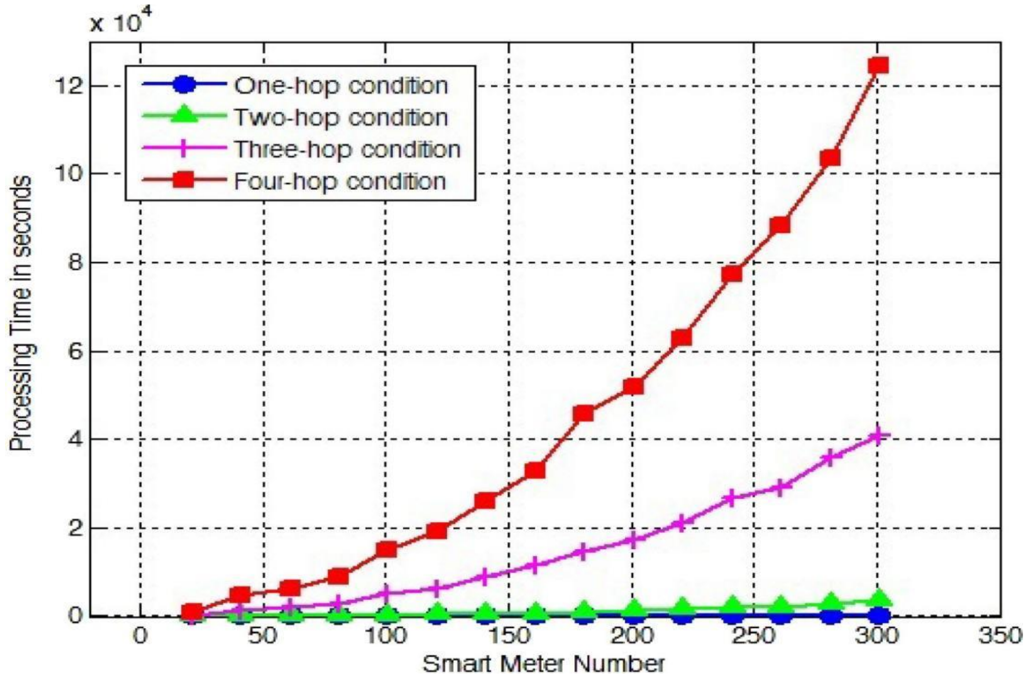


Figure 5. 7 Processing time for all cases in multiple network conditions

5.5.2 Numerical Analysis on Multi-Hop Study

Table 5.9 demonstrates the obtained the number of local data centers in multiple hops for fifteen cases. Fig.5.6 shows the trends of gained number of local data center for fifteen cases. The processing time of EAA algorithm for every communication network versus the number of smart meters. The number of local data center is decreased with the increasing of hop number. In addition, the EAA performance enhanced with the number of smart meters grows. The processing time of EAA algorithm increased exponentially as the number of smart meters growing in the 3-hop and 4-hop network, because the EAA algorithm of 3-hop and 4-hop rely on the calculation of the iterations of 2-hop EAA. In reality, because all the smart meters in demand side is known in advance, the complexity of time is acceptable. In addition, the faster programming language and more powerful computing server can be used for facilitating the processing time. Hence, the proposed model and EAA algorithm can be utilized to solve the optimization problem of local data centers and enhance the robustness of system.

5.5.3 Performance Comparison Between Traditional EAA and Improved EAA

Traditional EAA Algorithm Pseudocodes: Table 5.11 demonstrates the structure of traditional EAA algorithm [149], where the initial generation is $\mathrm{G}_x = \{\mathrm{Y}_{1,x}, \mathrm{Y}_{2,x}, ...\mathrm{Y}_{n,x}\}, x = 1$. x is the number of population and n is the initial result number of generation. *MaxGeneration* is the termination parameter in algorithm. The feasible result of population is $\mathrm{Y}_{i,x}, i \in [1:n]$ that consisted by multiple node clusters. The cluster is a community of smart meters that data can be collected through the same local data center. In Table 5.11, the procedure 6 utilizes the algorithm of Table 5.5 to solve the new result $Y_{m+1,x}$.

Table 5.11 Traditional EAA High-Level Structure

Start	
1	Create an Initial Population $G_x = \{Y_{1,x}, Y_{2,x} ... Y_{n,x}\}$, let x=1
2	**WHILE** ($x < MaxGeneration$):
3	Rank all $Y_{i,x}, i \in [1:n]$ in G_x
4	Select top *m(m<n)* solutions from G_x as $G'_n = \{Y_{1,x}, Y_{2,x} ... Y_{m,x},\}$
5	**WIHLE** (m not equal to n)
6	Generate one new solutions $Y_{m+1,x}$
7	Add $Y_{m+1,x}$ to G'_n
8	m=m+1
9	**ENDWHILE**
10	x=x+1
11	$G_x = G'_n$
12	**ENDWHILL**
	Select the best $Y_{i,x}, i \in [1:n]$ from G_x
End	

Comparison Between Traditional EAA and Proposed EAA Performance: All 15 cases have been run as Table 5.12 in different hops conditions, and Table 5.13 illustrates their processing time among all 15 cases computed by traditional EAA algorithm. different hops conditions, and Table 5.13 illustrates their processing time computed by traditional EAA algorithm. The comparison of obtained local data center processed by traditional EAA and improved EAA is represented in Fig.5.8. It is clearly demonstrating the number of local data center is decreased solution $Y_{m+1,x}$ in the iteration (procedure 6) that uses higher CPU load than proposed algorithm with Switch and Shuffle operator. Fig.5.9 shows the comparison of processing time between traditional EAA and improved EAA is represented, and the proposed EAA spends less time. In summary, the proposed EAA performs better in both powerful node number and processing time.

Table 5.12 The Number of Local Data Center For by Traditional EAA For All 15 Cases

	Smart Meter Number	One-hope Network	Two-hope Network	Three-hope Network	Four-hope Network
1	21	11	9	7	7
2	41	25	19	17	17
3	61	42	32	30	28
4	81	55	45	41	34
5	101	67	55	49	42
6	121	74	67	58	47
7	141	82	76	69	54
8	161	100	88	81	69
9	181	120	113	90	81
10	201	140	128	105	93
11	221	170	151	117	100
12	241	181	170	133	112
13	261	191	174	146	119
14	281	198	180	157	128
15	301	216	189	167	137

Table 5.13 The processing Time (Second) by Traditional EAA (Seconds) For All 15 Cases

	Smart Meter Number	One-hope Network	Two-hope Network	Three-hope Network	Four-hope Network
1	21	0.09	9.69	378	1201
2	41	0.48	38.29	1516	4846
3	61	0.98	84.87	2522	6824
4	81	1.09	140.6	3824	9743
5	101	2.48	289.4	5845	15654
6	121	5.13	424.3	7340	20203
7	141	8.32	699.5	9942	27293
8	161	5.67	694.9	11743	34121
9	181	12.98	1013.1	15631	46101
10	201	15.09	2045.4	18874	53522
11	221	17.71	3072.1	22634	64993
12	241	21.22	3555.9	29130	79886
13	261	24.99	4020.5	31113	90332
14	281	28.07	4204.8	37924	110278
15	301	35.013	4987.5	43014	131082

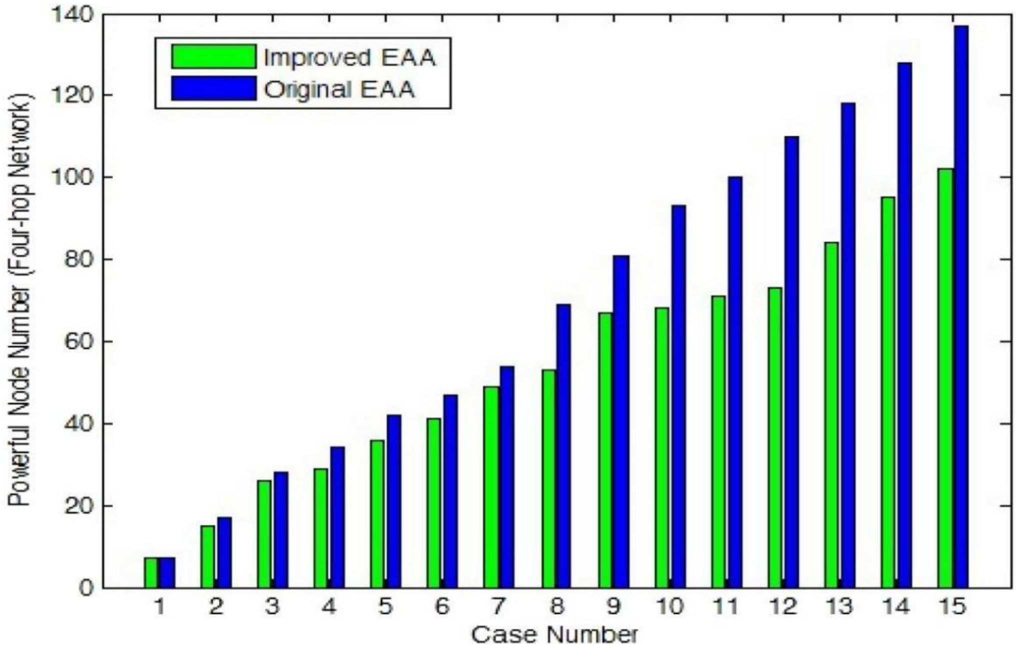


Figure 5. 8 Comparison of obtained local data center number

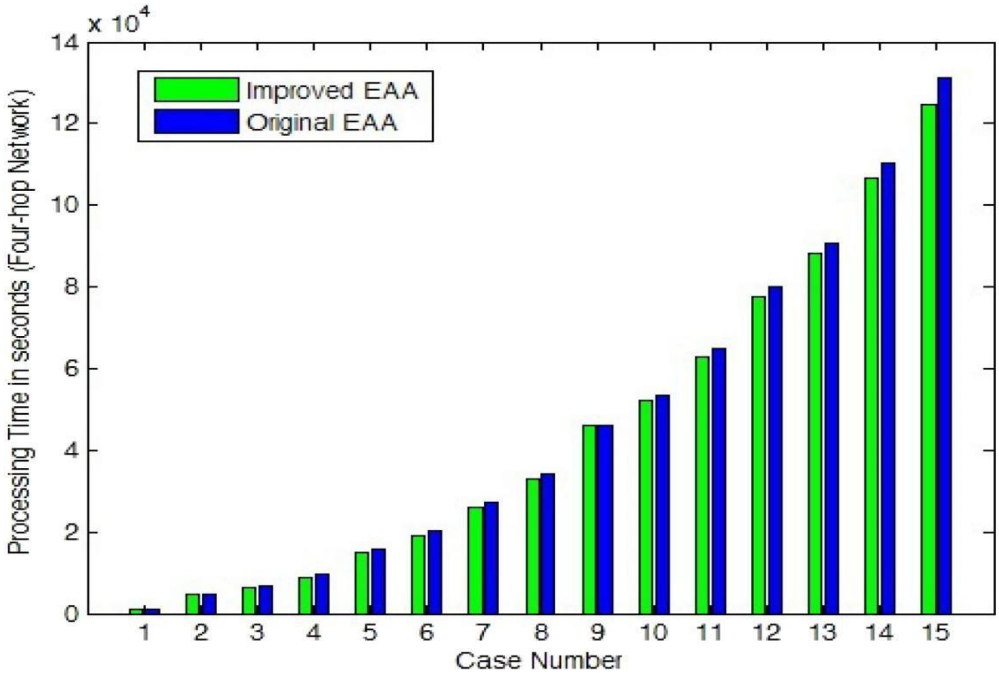


Figure 5. 9 Comparison of the processing time

5.6 Chapter Conclusion

This chapter proposed a wireless smart metering network model and a novel EAA algorithm that can optimize the least number of local data centers in multiple-hop communication network. The EAA algorithm with two new adaptive operations is first designed to solve the problem in 2-hop condition. In addition, the network is extended to multiple-hop communication network, and numerical analysis and case studies are simulated that validate the efficiency of developed EAA algorithm. The minimum number of local data centers provides more robustness to satisfy the connectivity requirement for CPS demand side management.

CHAPTER 6.

Power Security Strategy based on Two-Virus Attack Prediction

6.1 Introduction

A power cyber-physical system is a deep integration of a power physical network and an information network, coordinated by implementing physical equipment, sensor resource, information communication and IoT-based systems. In this context, it is easier to encounter network attacks on energy supply, transmission, power consumption processing and energy information physical system. Compared with the physical attack of an energy system, a network attack has the characteristics of low cost, high concealment and large scope. Once successful, the consequences are quite serious [150]. For example, at the end of 2015, Ukraine's power grid suffered from malicious network attacks, and the implantation of computer viruses made the control server lose the ability to perceive and control the physical equipment of the power grid, which led to a large-scale blackout [151]. In addition, the demand side was more susceptible to viruses because it had two-way communication capability that affected the entire system operation.

When a virus is detected, the system assigns fixing resources and proposes the corresponding antivirus programs to repair the system and secure privacy. In reality, there are multiple viruses attacking the system at the same time. With the integration of multiple sensors, smart meters, and distributed resources, the gird is increasingly at risk of being attacked by a virus, especially on the demand side. There is a great amount of privacy and user information on the demand side, which is able to connect and even control the grid's generation and operation. Once one virus invades the network, it attempts to infect other appliances of the system via cyber protocols, i.e., SMTP and TCP/IP, which would cause a greater loss. Therefore, a trade-off allocation is essential for operation and robustness of system. There are some studies on internet viruses. [151-153] introduce the virus propagation followed by homogeneous or scale-fee network, and [154] summarizes several propagation models of arbitrary condition. Recently, the epidemic of individual-level referred as a new approach to research the way the virus spreads, which is an epidemic method to qualify the evolution of network expect state by separate equations. [155][156] illustrates the Susceptible-Infected (SI) scheme that is able to capture the virus while releasing the antivirus program. In this chapter, we implement the risk management of a fix resource allocation problem when the grid system faces two-virus attacks. In addition, a double-antivirus model is developed under two different virus challenges. A new DOWNHILL- TRADEOFF algorithm is developed to solve the trade-off problem to confront the complex threats, and numerical simulation to validate system efficiency.

6.2 Robustness Consideration for Cyber Attacks

The failure of power information system will threaten the security of the power system. Therefore, it is necessary to develop an effective CPS security analysis method. As the result of information system failure is usually that the control center loses the ability to control related power equipment, the impact of information system failure on the power system should generally be regarded as a large disturbance. Therefore, in the robustness analysis of power CPS, we should focus on the impact of an information system fault on power system transient stability.

6.2.1 Procedures of Robustness Analysis

The general steps of CPS demand-side robustness analysis are as follows:

a) Establish a preconceived accident in a cyber-physical demand side;

b) For each contingency, develop a dynamic model described above (in Chapter 2) to evaluate whether the communication network will be blocked, and calculate the time-varying path of the information system performance indicators (transmission delay, data loss rate) in a short period of time;

c) Based on the transmission delay and data loss rate, the power equipment that may lose control is judged;

d) Propose the response model based on the above discussion, and then apply it to evaluate whether the power system can minimize the loss and reserve the operation.

6.2.2 Risks of Cyber Attack

In terms of the CPS demand-side, the majority of the vulnerabilities of cyber intrusion lie in the communication link of the transmission protocol, information exchange strategy and program, network link and routing control. External malicious attacks and sabotage then affect the servers of demand-side major stations and substations and a large number of bottom measurement and control terminal equipment, which further affect the operation of the entire system. There are a variety of malicious attacks from outside, such as fake message, information collection type, Denial of Service (DOS), direct use control type and so on. As mentioned above, in the typical demand-side network information system as shown in Figure 6.1 not only does the adoption of a public network communication mode cause the demand-side network to face a variety of attacks and threats from the information space, but also the reliability problems of the functions of the private communication network. The software environment of the related hardware equipment and the operating system are also at risk from stealing and information tampering.

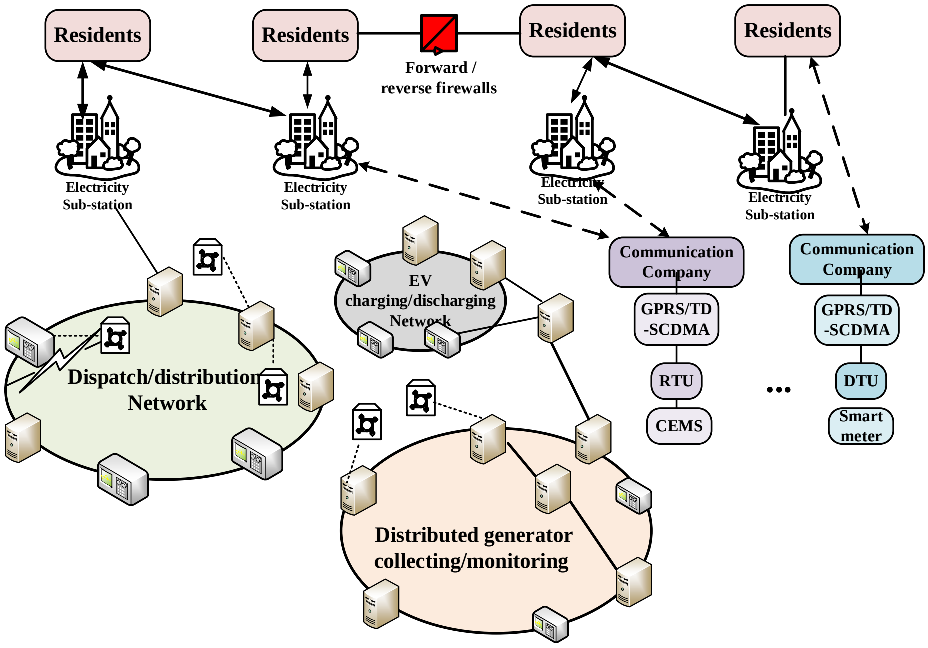


Figure 6. 1 Border of cyber-security in CPS demand side

6.3 Double-Antivirus-Strategy-Development Problem

6.3.1 Terminologies and Notations

A Double-Antivirus-Strategy Development (DASD) is considered in this chapter, which is able to allocate the limited fixing resources to different antivirus strategies to mitigate the potential loss.

Consider there are N nodes in demand-side network $N = \{1,2,3\ldots N\}$ and the network topology referred as $T = (N, L)$ where denotes link of communication among node n and m. The adjacency matrix T represents $\mathrm{A}(T) = (a_{mn})_{N\times N}$, i.e., a_{mn}=0 or1 based on where $\{m,n\} \in L$ or not.

In this chapter, there are two virus, Virus α and Virus β, simultaneously attack the system at time *t*. Four nodes conditions are considered: a) ***Susceptible:*** denotes the nodes which is not tainted and with either of the double viruses; b) ***α-Infected:*** assumes nodes infected virus α but not virus β tainted; c)***β -Infected***: refers to nodes infects virus β but virus α not tainted; d) ***Both-Infected:*** denotes nodes are tainted both virus α and virus β. $Y_n(t)$ =1.2.3.4 refers as the node *n* respectively injected Susceptible, α-Infected, β-Infected and Both-Infected.

$$Y(t) = (Y_1(t), Y_2(t)...Y_N(t)) \tag{6.1}$$

Equation (6.1) represents the network status at time *t*.

$$S_m(t) = \mathrm{M}r\{Y_i(t) = 0\},\ \ Q_m^{\alpha}(t) = \mathrm{M}r\{Y_i(t) = 1\}$$

$$Q_m^{\beta}(t) = Mr\{Y_i(t) = 2\}\ ,\ Q_m^{B}(t) = Mr\{Y_i(t) = 3\} \tag{6.2}$$

Equation (6.2) demonstrates the status of node m at time n, $M_r(t)$ presents the probability of occurrence at time *t*, and $S_m(t)$, $Q_m^{\alpha}(t)$, $Q_m^{\beta}(t)$ and $Q_m^{B}(t)$ represents the status of Susceptible, α-Infected, β-Infected and Both-Infected, respectively

$$Q(t) = (Q_1^{\alpha}(t),....,Q_N^{\alpha}(t), Q_1^{\beta}(t),....,Q_N^{\beta}(t), Q_1^{B}(t),...,Q_N^{B}(t)) \tag{6.3}$$

Since $S_i\ (t) = 1 - Q_i^{\alpha}(t) - Q_i^{\beta}(t) - Q_i^{B}(t)$, the expected status of the system can be described as Equation (6.3).

When antivirus strategy α and β confront Virus α and Virus β with the completed time Tα and Tβ. Therefore, no node is tainted by Virus α at the time t>Tα, and no node is tainted at t>Tβ by Virus β . Thus, for 1<n<N, (i) if $t \ge T1$, $Q_m^{\alpha}(t) = Q_m^{B}(t)$ =0; (ii) if $t \ge T2$, $Q_m^{\alpha}(t) = Q_m^{\beta}(t)$ =0.

6.3.2 Modelling of A Double-Virus Propagation

There are several assumptions of the virus propagation:

(a) Assume that the node n without Virus α may tainted by tainted neighbor m with the θ1 constant rate. Therefore, the Virus α probability is propagated to another node at time t, therefore $\theta 1\sum_{n=1}^{N} a_{mn}[Q_n^{\alpha}(t)+Q_n^{B}(t)]$.

(b) Assume that the node n without Virus β may tainted by tainted neighbor m with the θ2 constant rate. Therefore, the Virus β probability is propagated to another node at time t, as such, $\theta 2\sum_{n=1}^{N} a_{mn}[Q_n^{\beta}(t)+Q_n^{B}(t)]$.

The dynamic variation of expected network status can be stated as follows:

$$
\begin{aligned}
& Q_n^{\alpha}(t)=Q_n^{B}(t)=0, t\geq T1, 1\leq n\leq N,\\
& Q_n^{\beta}(t)=Q_n^{B}(t)=0, t\geq T2, 1\leq n\leq N,\\
& \frac{dQ_n^{\alpha}(t)}{dt}=\theta 1[1-Q_n^{\alpha}(t)-Q_n^{\beta}(t)-Q_n^{B}(t)]\sum_{n=1}^{N} a_{mn}[Q_n^{\alpha}(t)+Q_n^{B}(t)]\\
& -\theta 2Q_n^{\alpha}(t)\sum_{n=1}^{N} a_{mn}[Q_n^{\beta}(t)+Q_n^{B}(t)], t\geq 0, 1\leq n\leq N,\\
& \frac{dQ_n^{\beta}(t)}{dt}=\theta 2[1-Q_n^{\alpha}(t)-Q_n^{\beta}(t)-Q_n^{B}(t)]\sum_{n=1}^{N} a_{mn}[Q_n^{\beta}(t)+Q_n^{B}(t)]\\
& -\theta 1Q_n^{\beta}(t)\sum_{n=1}^{N} a_{mn}[Q_n^{\alpha}(t)+Q_n^{B}(t)], t\geq 0, 1\leq n\leq N,\\
& \frac{dQ_n^{B}(t)}{dt}=\theta 2Q_n^{\alpha}(t)\sum_{n=1}^{N} a_{mn}[Q_n^{\beta}(t)+Q_n^{B}(t)]\\
& +\theta 1Q_n^{\beta}(t)\sum_{n=1}^{N} a_{mn}[Q_n^{\alpha}(t)+Q_n^{B}(t)], t\geq 0, 1\leq n\leq N.
\end{aligned}
\tag{6.4}
$$

With Q (0) $=Q_0$

6.3.3 Modelling of DASD Problem

In order to estimate the expected loss, the following hypotheses are introduced:

(c) V1 represents each node caused economic loss per unit time when only Virus α infected

(d) V2 represents each node caused economic loss per unit time when only Virus β infected

(e) V1+V2 represents each node caused economic loss per unit time when Virus α and Virus β both infected

(f) M1 represents the man-days effort by implementing antivirus strategy α.

(g) M2 represents the man-days effort by implementing antivirus strategy β.

(h) *k* is the total fix program available.

While the number of k1 program allocated to the proposed antivirus strategy α, where $1 \le k1 \le k-1$. There are $k2 = k - k1$ programs assigned to implement strategy β. $T1 = \frac{M1}{k1}, T2 = \frac{M2}{k2}$. Therefore, the expected damages due to the virus can be illustrated as:

$$D(k1) = \int_0^{\max\{\frac{M1}{k1}, \frac{M2}{k-k1}\}} \sum_{n=1}^{N} [v1Q_n^{\alpha}(t) + v2Q_n^{\beta}(t) + v3Q_n^{B}(t)]dt \tag{6.5}$$

The DASD model is able to show a discrete optimization problem as follows.

$$\min D(k1) = \int_0^{\max\{\frac{M1}{k1}, \frac{M2}{k-k1}\}} \sum_{n=1}^{N} [v1Q_n^{\alpha}(t) + v2Q_n^{\beta}(t) + v3Q_n^{B}(t)]dt, 1 \le k1 \le k-1 \tag{6.6}$$

$$Q_{DASD} = (T, \theta1, \theta2, v1, v2, M1, M2, k, Q_0) \tag{6.7}$$

The Equation (6.7) shows the 9-tuple of DASD model.

6.4 The Two-Antivirus Strategy Development Model

There are three representative networks in Chapter 6.4.1 to introduce, and in Chapter 6.4.2, a heuristic DOWNHILL algorithm is proposed to solve the previous DASD model. Furthermore, the algorithm performance is studied to validate the efficiency.

6.4.1 Network Infrastructure

There are representative three major networks in reality as follows.

Small-World Network: relatively small diameter of network can be admitted, and

empirical results show that many networks in real life have the nature of small world network, i.e., a community with a high concentrated resents and smart meters [157]. The

Fig.6.1 (a) shows the synthetic structure of small-work network by Pajek.

Scale-free Network: Distribution followed power-law degree The connection status (degree) of each node in scale-free network is very different, and the distribution is seriously uneven. A few nodes have more connections, while most nodes only have few connections. Therefore, in the world of scale-free network, a few central nodes play a leading role in the operation of the network. Empirical results show that many networks in real life have the nature of scale-free network. Therefore, scale-free network is often regarded as a model of real network, which is widely used in all kinds of research. Fig.6.2 (b) shows the synthetic structure of scale-free network by Pajek [157][158].

Smart Meter Network of A Community: A smart meter network of a random community is demonstrated, the data from “Smart Gird, Smart City”, and the synthetic structure of smart meters network by Pajekhe is shown in Fig.6.2 (c). The connections between the smart meters are strong and the voltage levels are relatively simplified, equipped intelligent, stability communication system. Because this is a randomly selected residential community, users of smart meters are relatively concentrated.

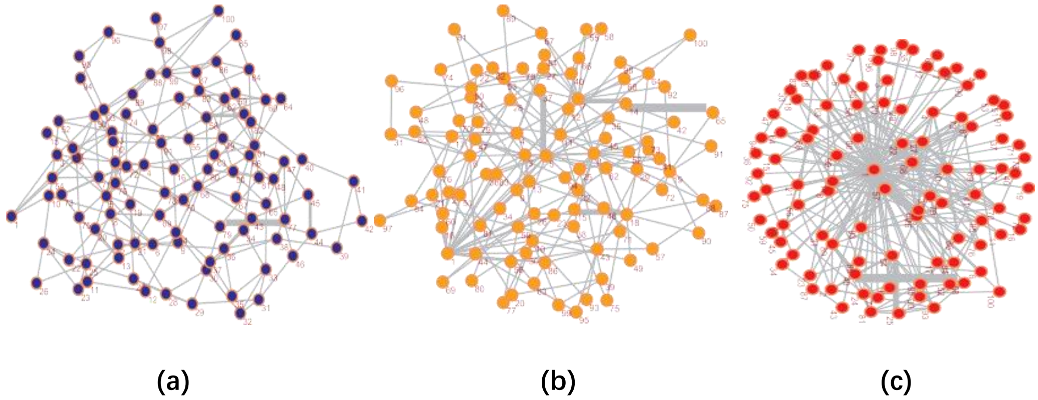


Figure 6. 2 Structure of three networks (a) small-world network (b) scale-free network, and (c) smart-meter of a community network

6.4.2 DOWNHILL-TRADE OFF Algorithm Applied in DASD Scheme

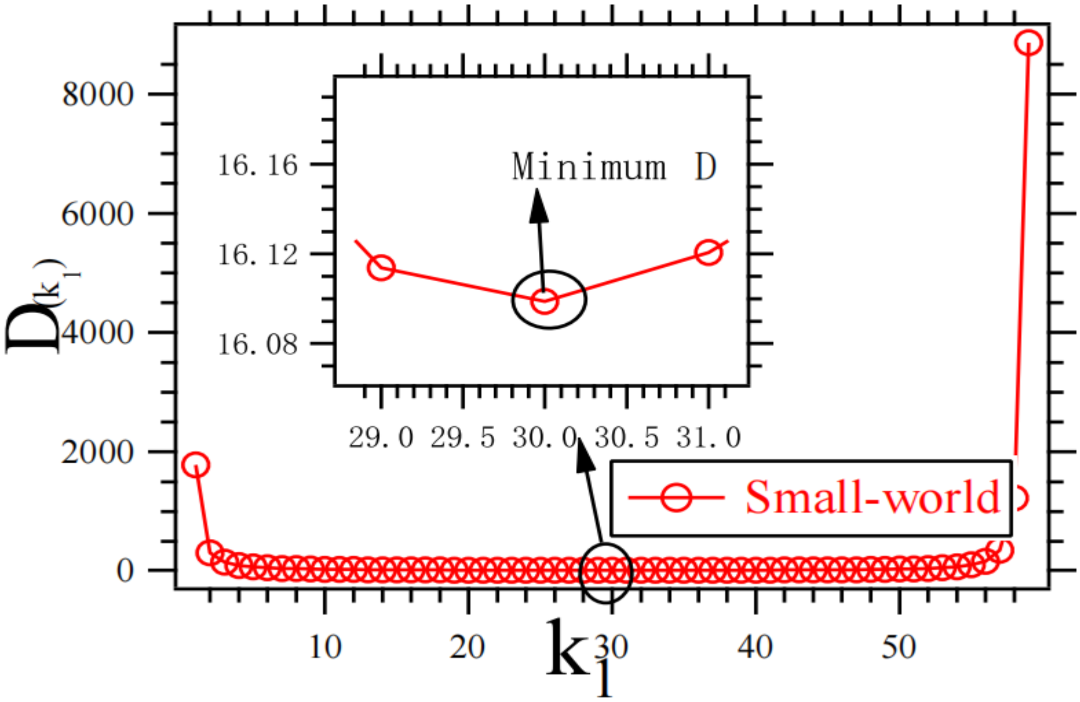
Numerical cases and simulations are implemented in Matlab in a computer with two Intel Xeon processors and 4GB memory.

There are 100,000 simulations with different parameters (i.e., $\theta 1$ and $\theta 2$) for solving DASP model. Fig.6.2 demonstrates three representative cases with each *k1* and corresponding D（k1） as examples.

Case A: consider DASD scheme implemented in the small-world network with θ 1=0.01, θ2=0.02, I(0)=(0.1,...,0.1), M1=80,M2=100,v1=3,v2=2,k=60.

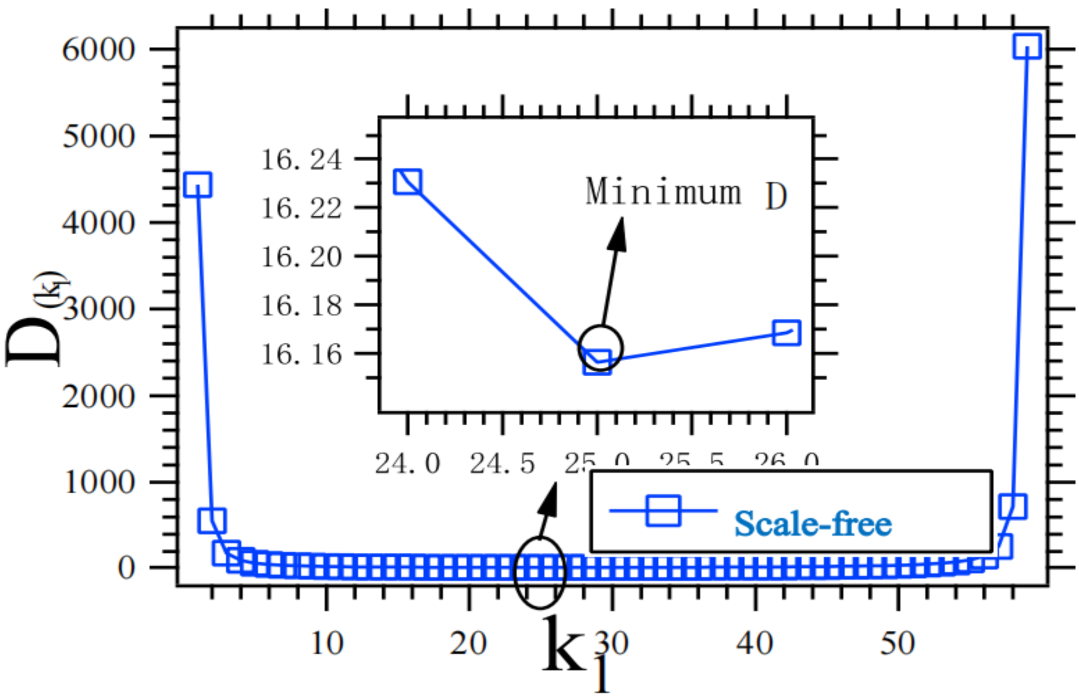
Case B: consider DASD scheme implemented in the scale-free network with θ 1=0.015, θ2=0.02, Q(0)=(0.1,...,0.1), M1=80,M2=100,v1=2,v2=3,k=60.

Case C: consider DASD scheme implemented in the smart-meter network of a community with θ 1=0.03, θ 2 = 0.01, Q(0) = (0.1, ... ,0.1), M1=100, M2=80, v1=1, v2=3, k=60.



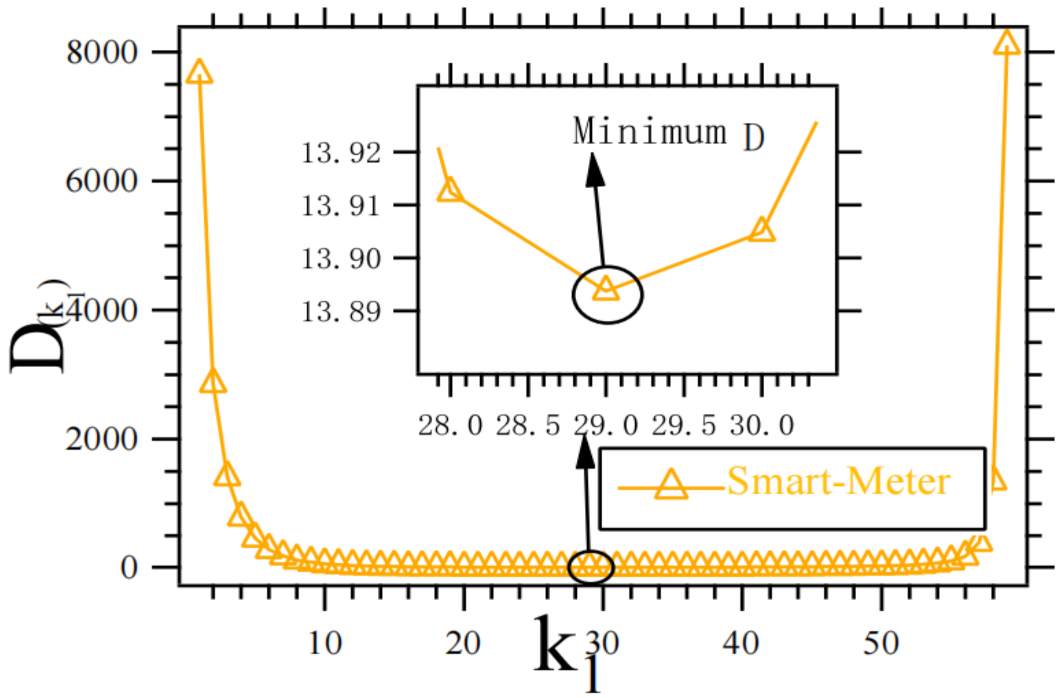
8000
6000
4000
2000
0
$D_{(k_l)}$
16.16
16.12
16.08
Minimum D
29.0 29.5 30.0 30.5 31.0
Small-world
10 20 30 40 50
k_l

(a)



6000
5000
4000
3000
2000
1000
0
$D_{(k_l)}$
16.24
16.22
16.20
16.18
16.16
Minimum D
24.0 24.5 25.0 25.5 26.0
Scale-free
10 20 30 40 50
k_l

(b)



(c)

Figure 6. 3 Node k1 versus D(k1) in case A, case B and case C respectively

According to the Fig.6.3, we can see that the damage of system $D(k1)$ is reduced first and then increased with k1. Therefore, there is an allocation scheme to minimize the expected total loss caused by the virus. To be specific, in Fig. 6.3 (a), $D(k1)$ achieved the minimum value when k1=30 in the small-world, which is the optimal result in this case; in Fig. 6.3 (b), $D(k1)$ achieved the minimum value when k1=25 in the scale-free, which is the optimal result in this case. in Fig. 6.3 (c), $D(k1)$ achieved the minimum value when k1=29 in a smart meter network of the residential community, which is the optimal result in this case. All them have an allocation scheme to minimize the expected total loss caused by the virus.

Therefore, A new algorithm, DOWNHILL-TRADE OFF (DTO), is proposed to solve the DASD model (see Table 6.1). In this algorithm, is the time computational complexity is represented as $C(k)$, $k1$ can be obtained by implementing the algorithm

DOWNHILL-TRADE OFF to the DASD scheme, and the potential damages cased by virus attacks are $D(k1)$.

Table 6.1 DOWNHILL-TRADE OFF Algorithm

Start
Input the DASD Scheme $Q_{TASD} = (T, \theta 1, \theta 2, v1, v2, M1, M2, k, Q_0)$.
Output: $k1$
$k1 := 1;$
while $n1 \le n-2$ and $D(k1) \ge D(k1+1)$ **do**
$k1 := k1+1$;
end while
return *k1;*
End

6.5 Comparison Study and Simulation Analysis

In this section, we consider three heuristic algorithm and a random algorithm to compare with the performance of DOWNHILL-TRADE OFF (DTO) algorithm.

6.5.1 Comparison Study between Heuristic Algorithms and DOWNHILL-TRADE OFF

We consider three heuristic algorithms in this paper to compare with the performance of the proposed DTO algorithm.

Heuristic Algorithm 1: The existing fixing programs of the system are evenly allocated to the two viruses, which also can be called the averaging strategy, as Equation (6.8).

Heuristic Algorithm 2: The allocation followed the workloads of antivirus programming research and development with linearly proportion, as Equation (6.9).

Heuristic Algorithm 3: As the Equation (6.10) he allocation determined by virus infected rate in system.

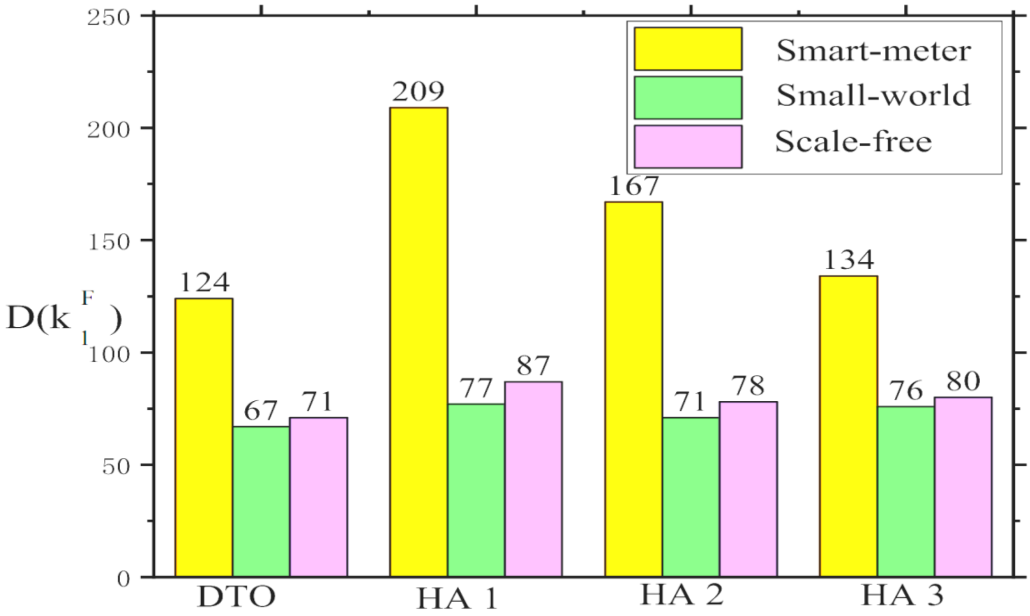
$$K = \left(\left\lfloor \frac{\bar{k}}{2} \right\rfloor, k - \left(\left\lfloor \frac{\bar{k}}{2} \right\rfloor\right)\right) \tag{6.8}$$

$$K = \left(\left\lfloor \frac{\bar{k}\mathrm{M}1}{M1+M2} \right\rfloor, k - \left(\left\lfloor \frac{\bar{k}M1}{M1+M2} \right\rfloor\right)\right) \tag{6.9}$$

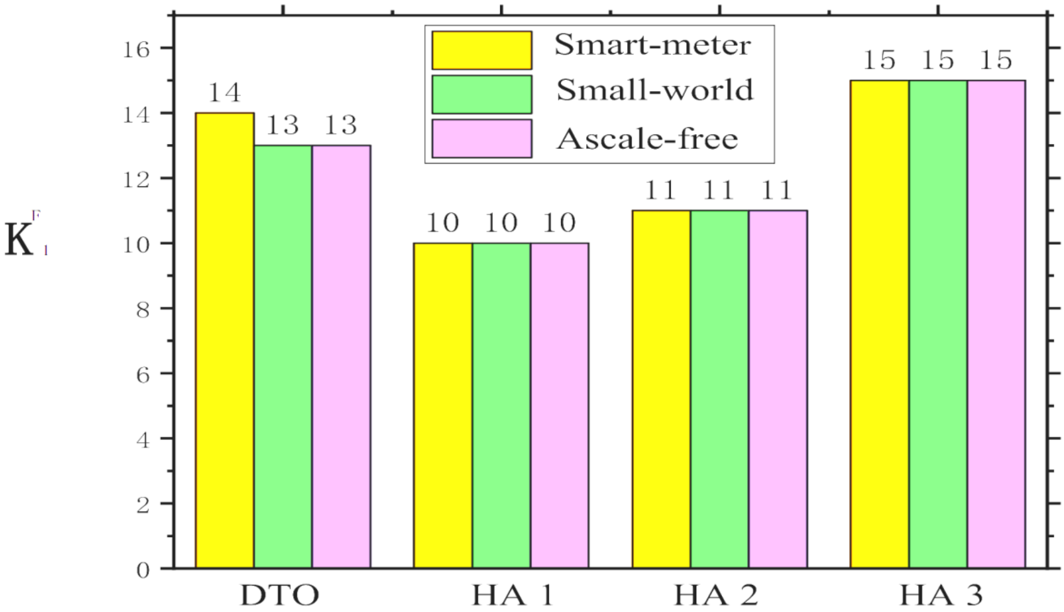
$$K = \left(\left\lfloor \frac{\bar{k}\theta 1}{\theta 1+\theta 2} \right\rfloor, k - \left(\left\lfloor \frac{\bar{k}\theta 1}{\theta 1+\theta 2} \right\rfloor\right)\right) \tag{6.10}$$

We assume the number of limited fixing resources in specific strategy to implement antivirus program α is , whose total corresponding damage defined as .DASD scheme implemented with 1=0.01, 2=0.05, I(0)=(0.1,...,0.1), M1=25, M2=20, v1=1, v2=2, k=20, in the small-world, scale-world network, and smart-meter network of a community, respectively.

As the results, the Fig.6.4 (a) shows the problem is obtained the optimization with the number of allocations on virus α, and total damage of entire system is shown in Fig.6.4 (b) with using Heuristic Algorithm 1, Heuristic Algorithm 2, Heuristic Algorithm 3 and proposed DOWNHILL-TRADE OFF algorithm. We can see the proposed algorithm can achieve the minimum loss in all network conditions.



(a)



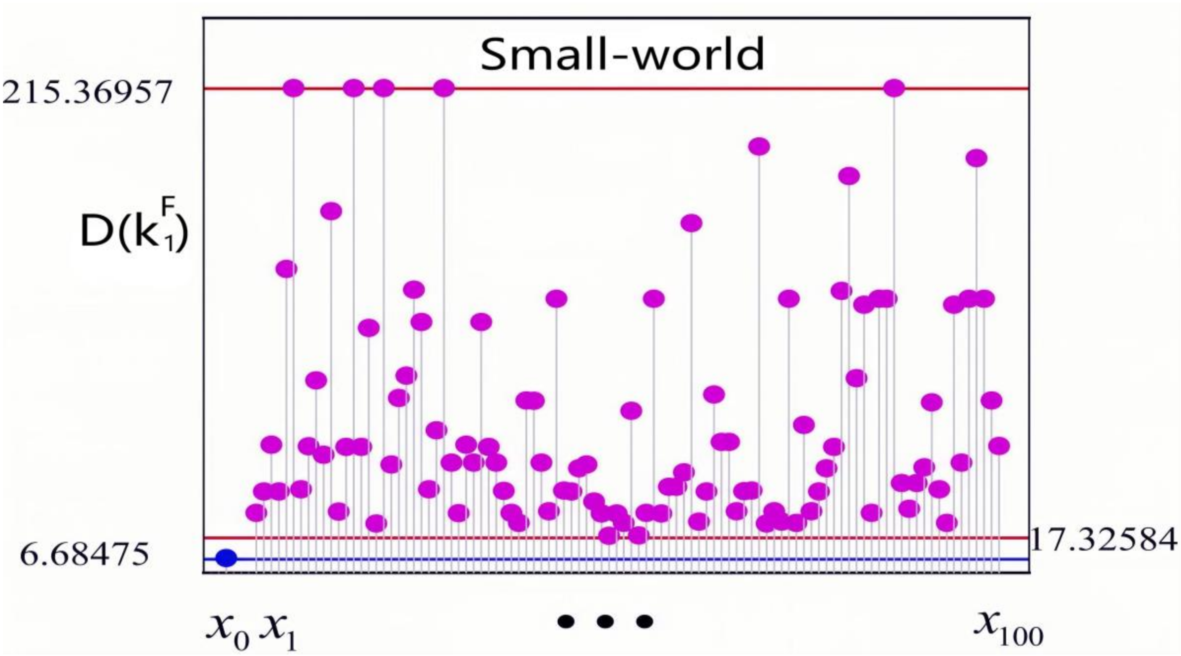
(b)

Figure 6. 4 Comparison results of three heuristic algorithms and proposed DOWNHILL-TRADE OFF.

6.5.2 Comparison Study between Random Algorithm and DOWNHILL-TRADE OFF

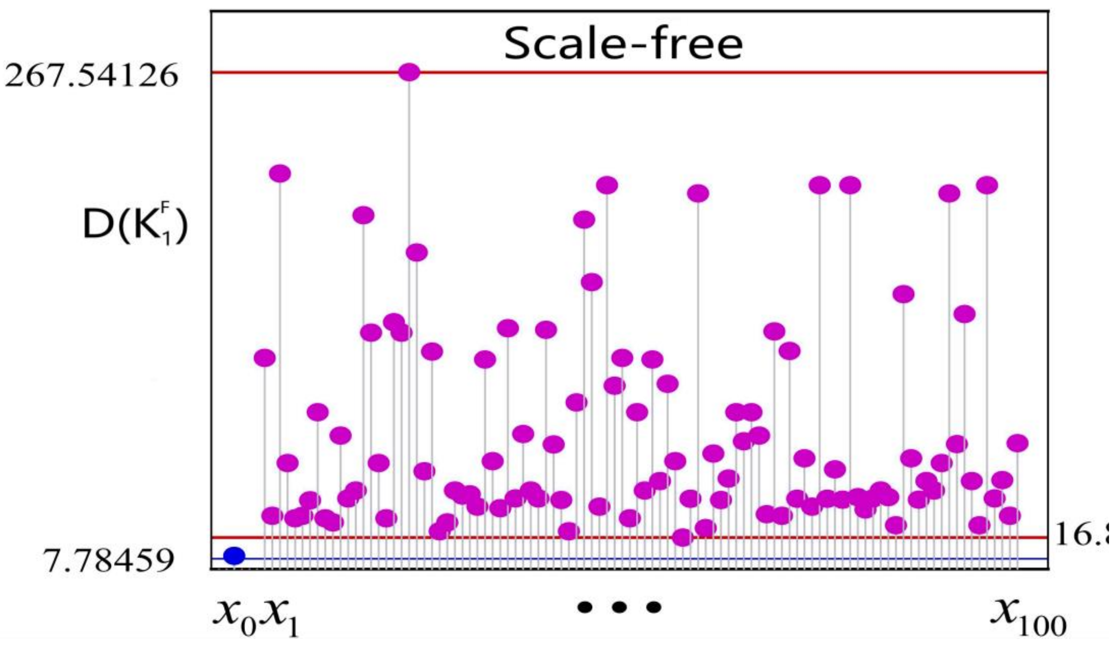
The random algorithm refers as a strategy with assign the resource randomly to the antivirus programs. There are 100 random allocations in this simulation and its comparison results with the DOWNHILL-TRADE OFF algorithm as Fig.6.4. We consider the parameters of two-antivirus strategy are： 1=0.03, 2=0.01, Q(0)=(0.1,...,0.1), M1=100, M2=80, v1=1, v2=3, *k*=100, in the small-world, scale-world network, and smart-meter network of a community, respectively. In Fig.6.4, $x = (x_1, x_1, \ldots, x_{100})$ represents the strategies obtained by implementing the random algorithm, x_0 denotes as DOWNHILL-TRADE OFF algorithm.

As shown in Fig.6.5 (a), the potential damage of in small network run by DOWNHILL-TRADE OFF algorithm is 6.68475，which is much lower than the random algorithm's loss between 17.32584 to 215.36957 in 101 strategies. Fig.6.5 (b) demonstrates in scale-free network, the potential damage of run by DOWNHILL-TRADE OFF algorithm is 7.78459， lower than the random algorithm's loss between 16.85153 to 267.54126. In Fig.6.5 (c), the attacking loss of run by DOWNHILL-TRADE OFF algorithm also is the lowest, which is 10.56875 in a smart-meter network of example community. Therefore, DOWNHILL-TRADE OFF algorithm is proved the most effective for the model solving.



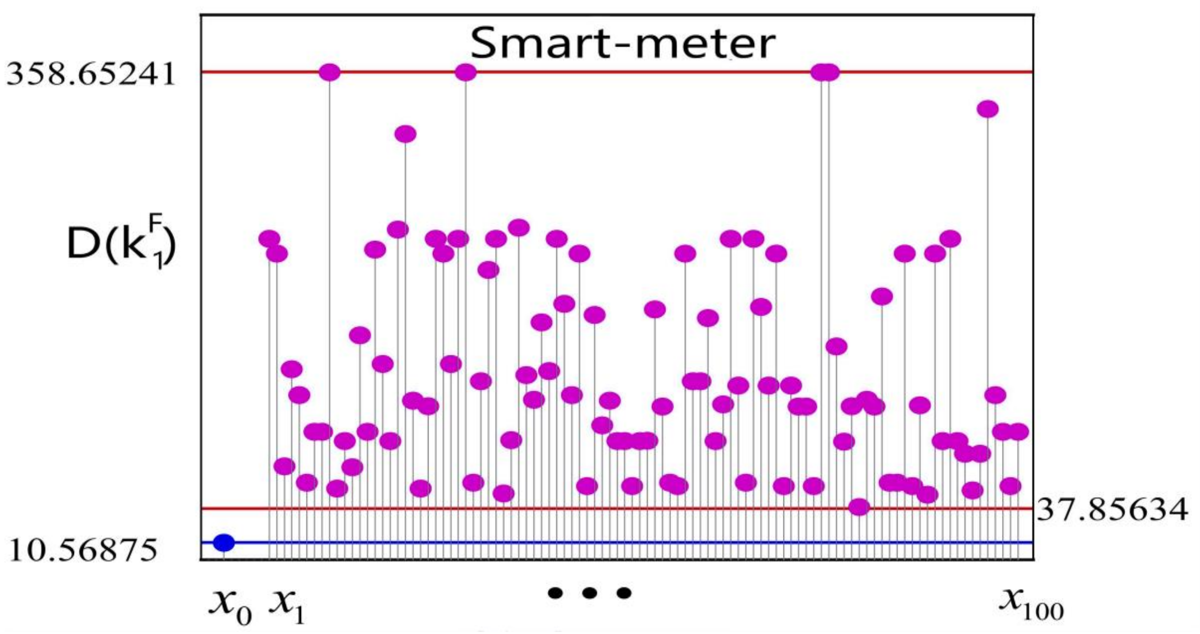
Small-world
215.36957
D(k$_1^F$)
6.68475
17.32584
x_0 x_1
x_{100}

(a)



Scale-free
267.54126
D(K$_1^F$)
7.78459
$x_0$$x_1$
x_{100}

(b)



(c)

Figure 6. 5 The comparison results of random algorithms and proposed DAO algorithm

6.6 Different Factors Impact on DOWNHILL-TRADE OFF

The double-antivirus strategy with different parameters of DOWNHILL-TRADE OFF algorithm is studied in this section. All parameters are chosen randomly and the results will show the same tendency with different data.

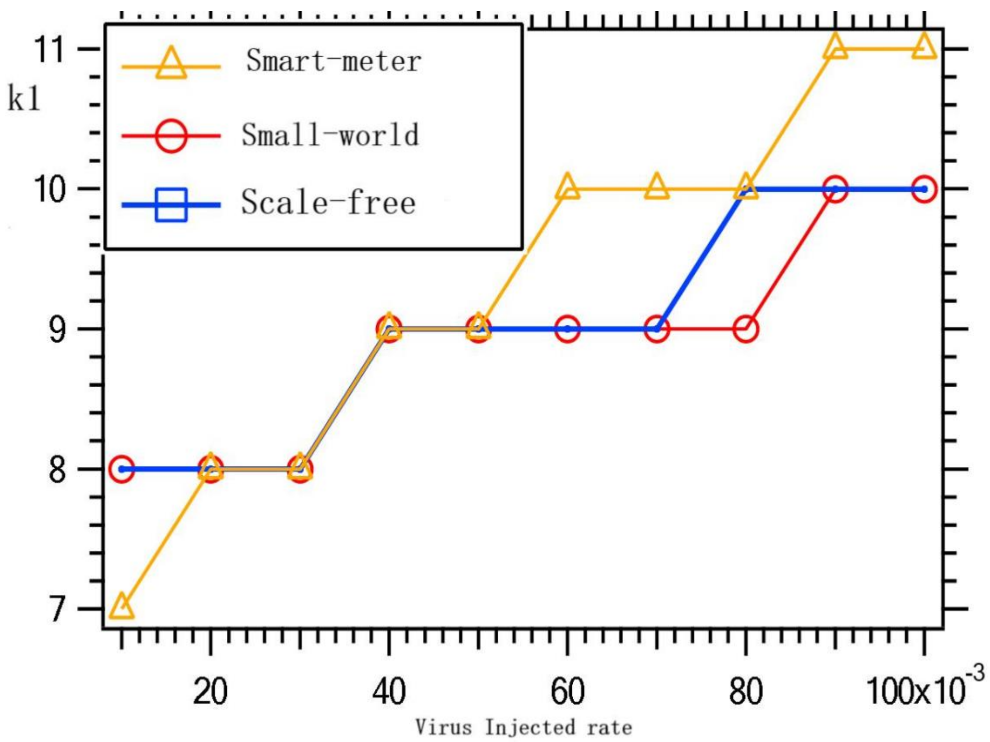
6.6.1 Viruses Infected Rate Impact

This section investigates the impact of infected rate θ1 of virus α and θ2 of virus β for DOWNHILL-TRADE OFF algorithm.

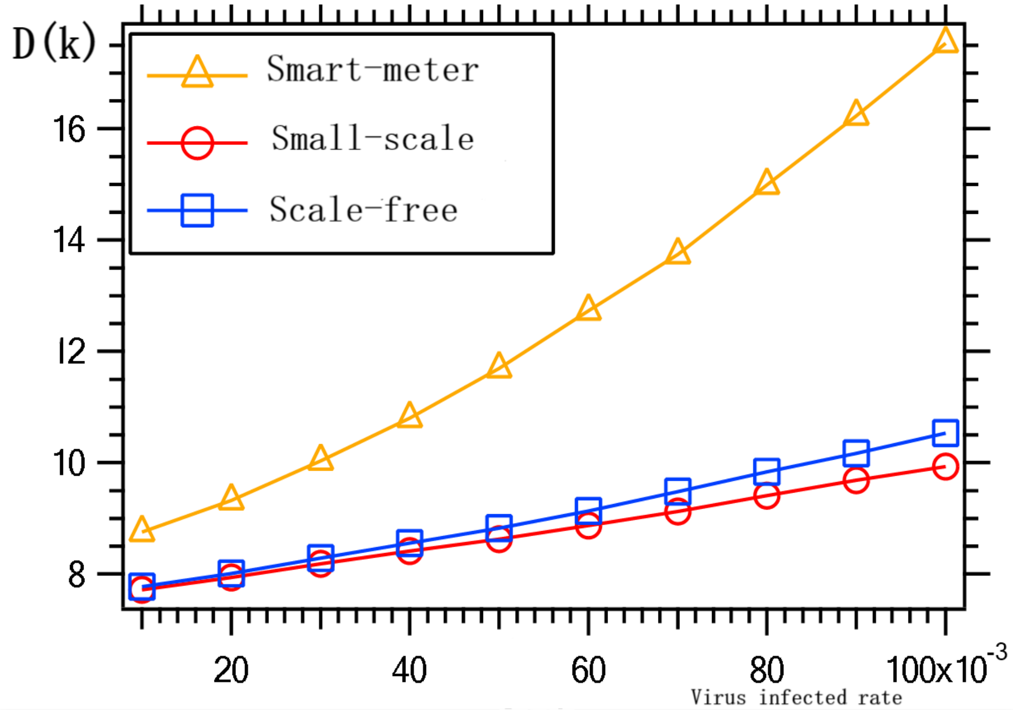
Case set 1: consider DASD model with $\theta 1 \in \{0.01, 0.02, 0.03, \ldots, 0.1\}$, θ 2=0.05, Q(0)=(0.1,...,0.1), M1=25, M2=20, v1=1, v2=2, *k*=19, in the small-world, scale-world network, and smart-meter network of a community, respectively. The results of this set is in Fig. 6.6 (a) and Fig. 6.6 (b), where Fig. 6.6 (a) shows the allocation result k_1^F of antivirus program α and Fig. 6.6 (b) demonstrates the total potential damages under double-virus attacking.

Case set 2: consider DASD model with, 1=0.1, $\theta 1 \in \{0.025, 0.05, \ldots, 0.25\}$, M1=20, M2=25, I (0) = (0.1,...,0.1), v1=1, v2=2, *k*=17 in the small-world, scale-world network, and smart-meter network of a community, respectively. Fig. 6.5 (c) shows its allocation result of antivirus program α and Fig. 6.5 (d) demonstrates the total potential damages under double-virus attacking.

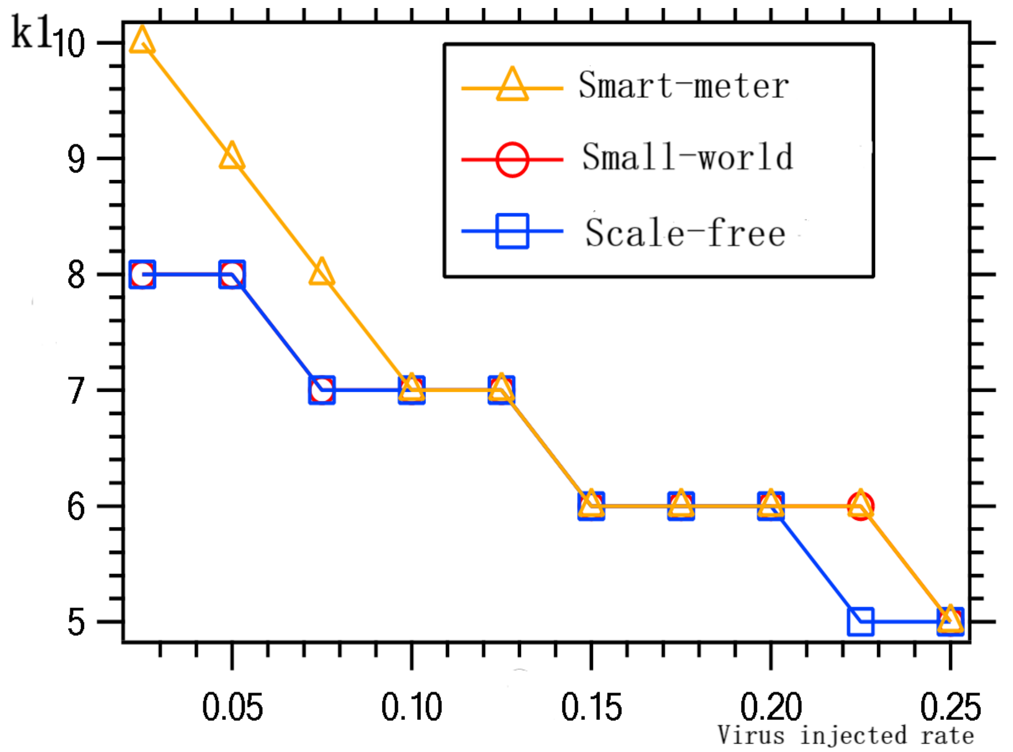
As shown of Fig.6.6, more fixing resources would be assigned to antivirus program α with the increased of $\theta 1$, and the total damage of system would be increased. The result follows the intuition. The increased of $\theta 1$ represents virus α is able to injected more nodes, therefore, more securing resources should be assigned to improve the resistance of virus α and enhance the entire system robustness.



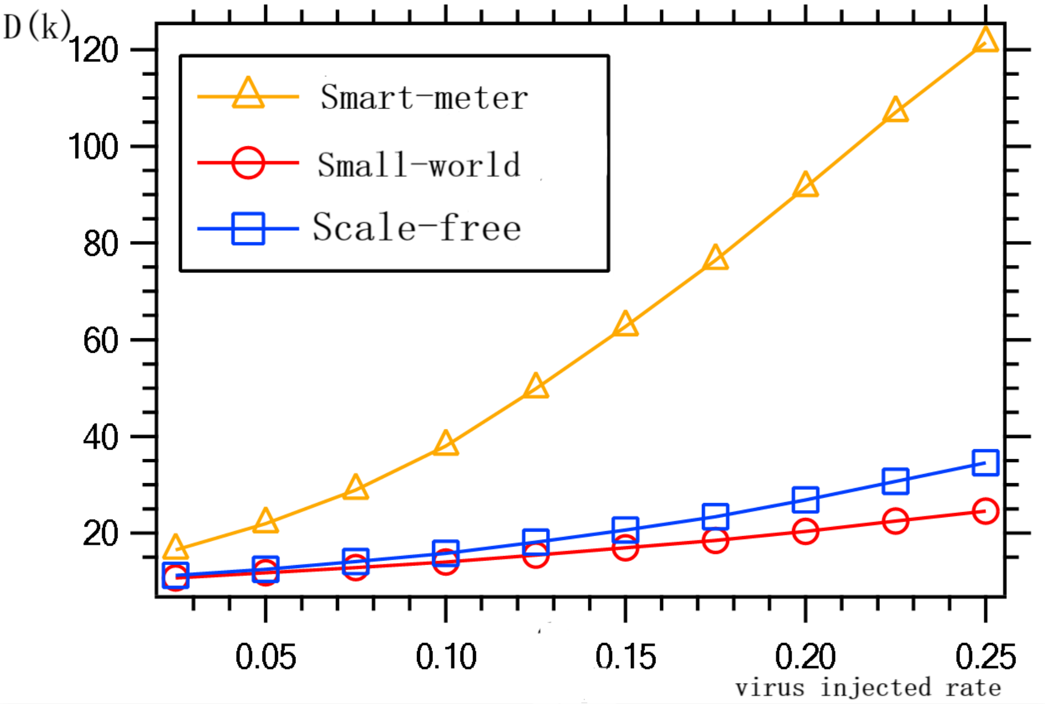
(a)


D(k)
Smart-meter
Small-scale
Scale-free
16
14
12
10
8
20
40
60
80
100x10-3
Virus infected rate

(b)


k1
10
9
8
7
6
5
Smart-meter
Small-world
Scale-free
0.05
0.10
0.15
0.20
0.25
Virus injected rate

(c)



(d)

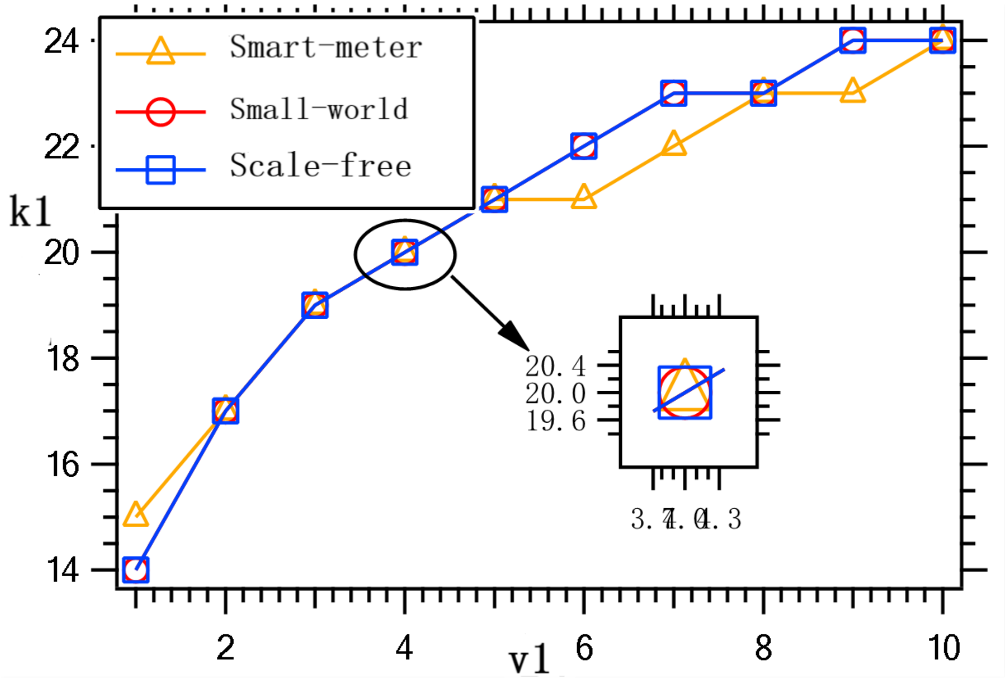
Figure 6. 6 Allocation results of virus infected rate changing

6.6.2 Damage Per Unit of Time of Impact

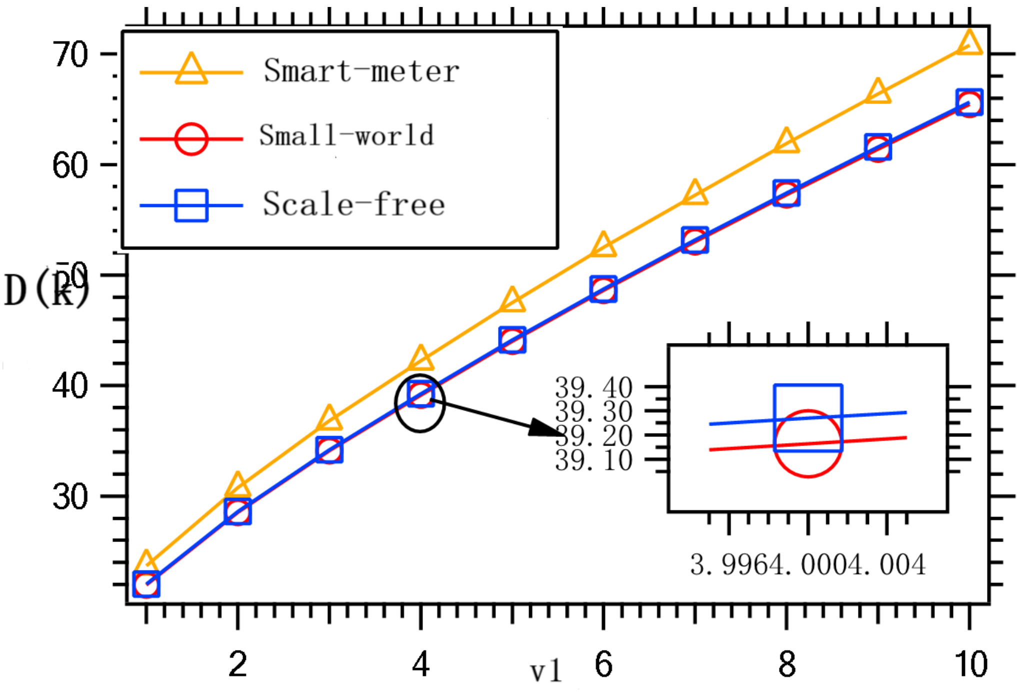
The impact of the damages per unit of time for DOWNHILL-TRADE OFF implementation is discussed in the section. We consider v1 and v2 changed with following parameters.

Case set 3: Assume a set of DASD model with $\theta 1$ =0.01, $\theta 2$ =0.015, Q(0)=(0.1,...,0.1), M1=90, M2=70, $v1 \in \{1.2....,10\}$, v2=5, k=40, in the small-world, scale-world network, and smart-meter network of a community, respectively. The results of this set is in Fig. 6.7 (a) and Fig. 6.7 (b), where Fig. 6.7 (a) shows the allocation result of antivirus program α and Fig. 6.7 (b) demonstrates the total potential damages under double-virus attacking.

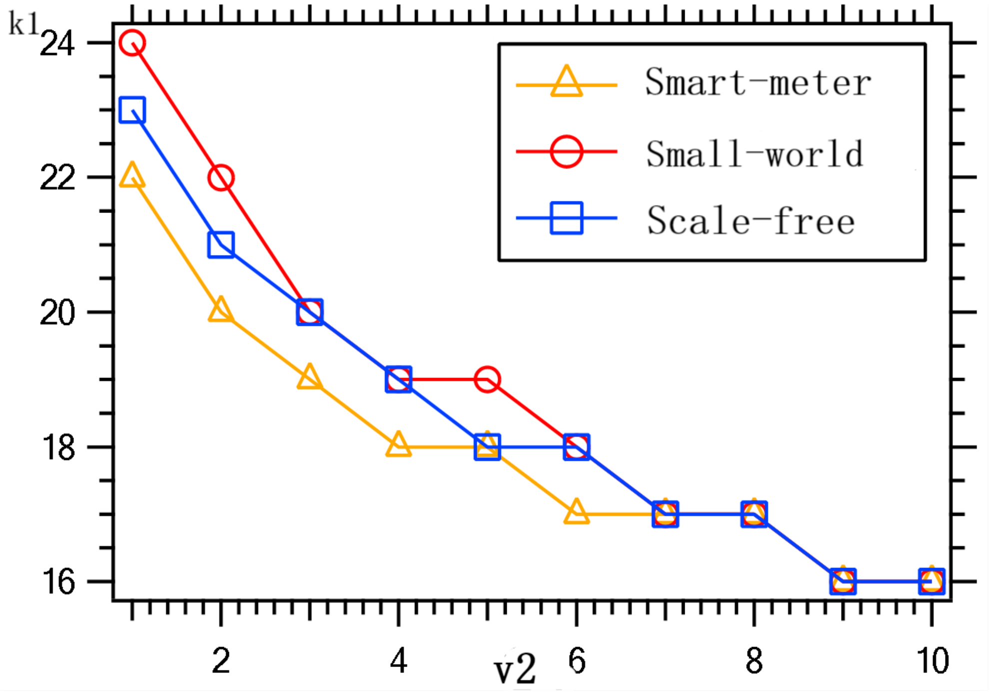
Case set 4: Assume a set of DASD model with 1=0.03, $\theta 2$ =0.04, M1=110,


Smart-meter
Small-world
Scale-free
k1
v1
24
22
20
18
16
14
2
4
6
8
10
20.4
20.0
19.6

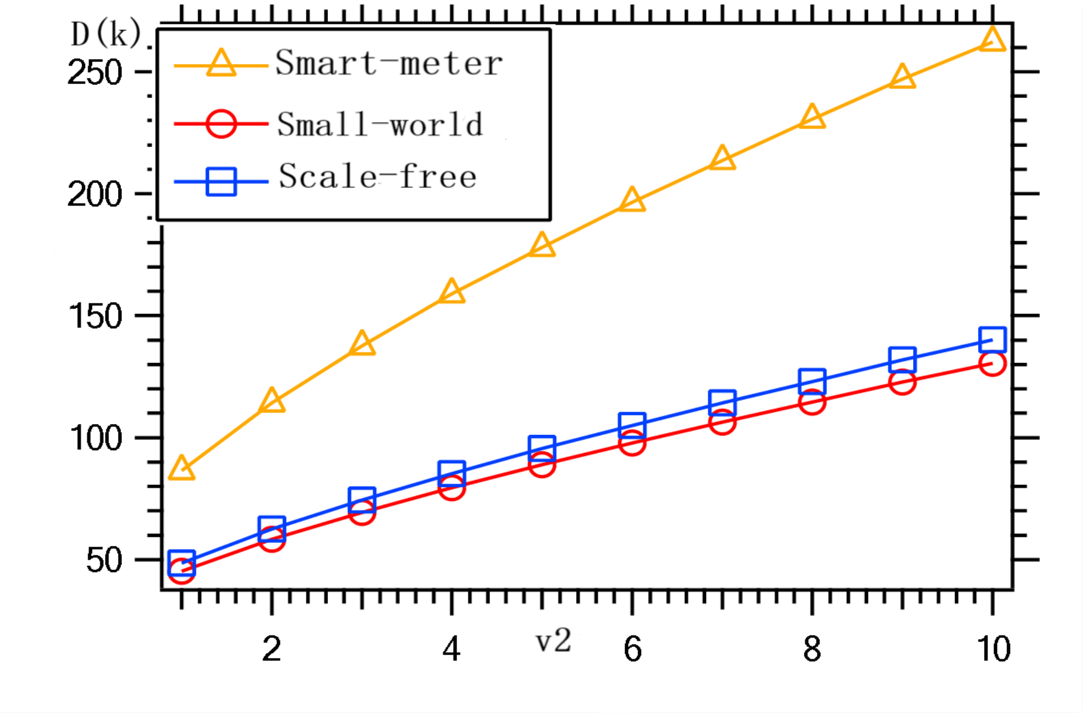
(a)


Smart-meter
Small-world
Scale-free
D(k)
v1
70
60
40
30
2
4
6
8
10
39.40
39.30
39.20
39.10
3.9964.0004.004

(b)



(c)



(d)

Figure 6. 7 Comparison results with per unit of time loss

M2=120, Q (0) = (0.1, ...,0.1), v1=5, $v2 \in \{1.2....,10\}$, k=40 in the small-world, scale-world network, and smart-meter network of a community, respectively. Fig. 6.7 (c) shows its allocation result of antivirus program α and Fig. 6.7 (d) demonstrates the total potential damages under double-virus attacking.

According to the results, with the increased of v2, more fixing resources should be allocated to Program β and the number of antivirus program in α decreased, and total damage increased. It is understandable to improve the antivirus ability for Program β when v2 increased.

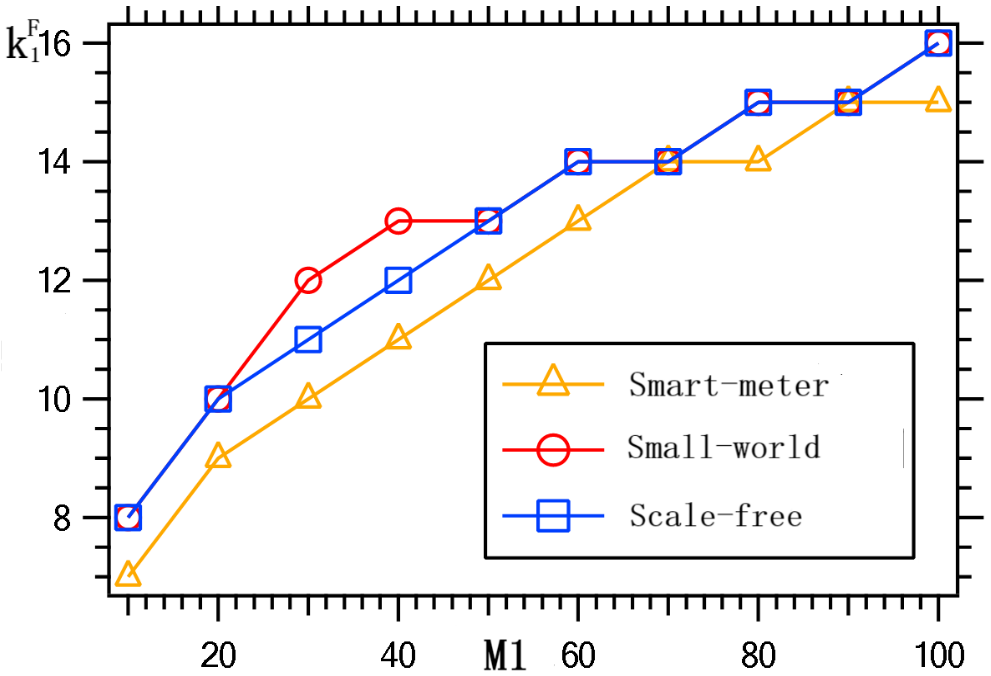
6.6.3 Antivirus Effort Impact

The impact of efforts M1 and M2 for DASD model implemented DOWNHILL-TRADE OFF is studied in this Section.

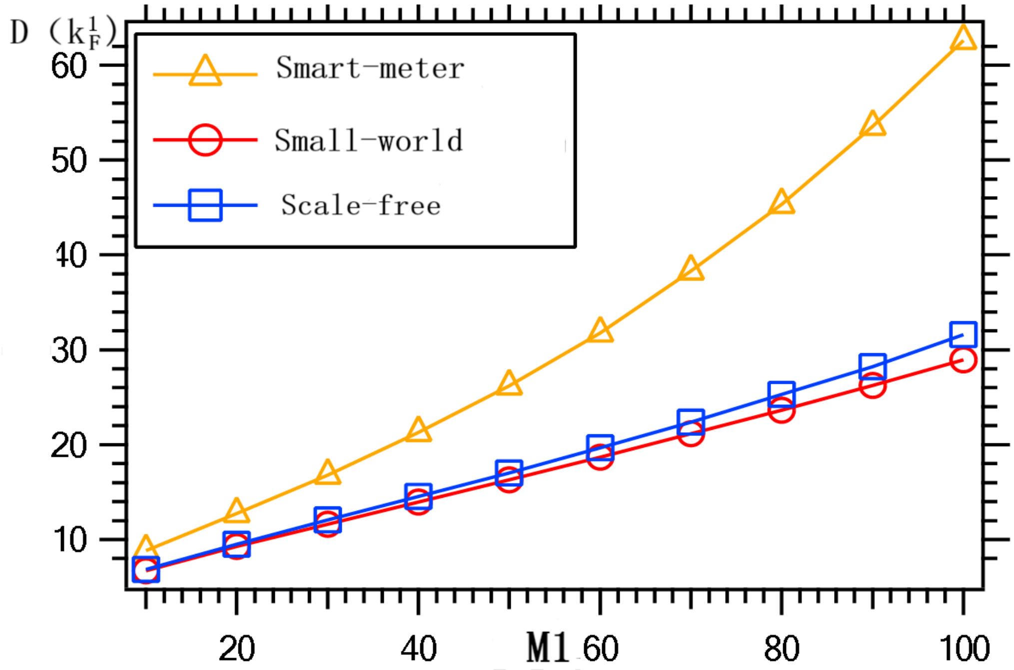
Case set 5: Assume a set of DASD model with =0.03, =0.05, Q(0)=(0.1,...,0.1), , =50, v1=2, v2=1, k=25, in the small-world, scale-world network, and smart-meter network of a community, respectively. The results of this set are given in Fig. 6.8 (a) and Fig. 6.8 (b), where Fig. 6.8 (a) shows the allocation result of antivirus program α and Fig. 6.8 (b) demonstrates the total potential damages under double-virus attacking.

Case set 6: Assume a set of DASD model with 1=0.03, =0.04, M1=110, M2=120, Q(0)=(0.1,...,0.1), v1=5, , k=40 in the small-world, scale-world network, and smart-meter network of a community, respectively. Fig. 6.8 (c) shows its allocation result of antivirus program α and Fig. 6.8(d) demonstrates the total potential damages under double-virus attacking.

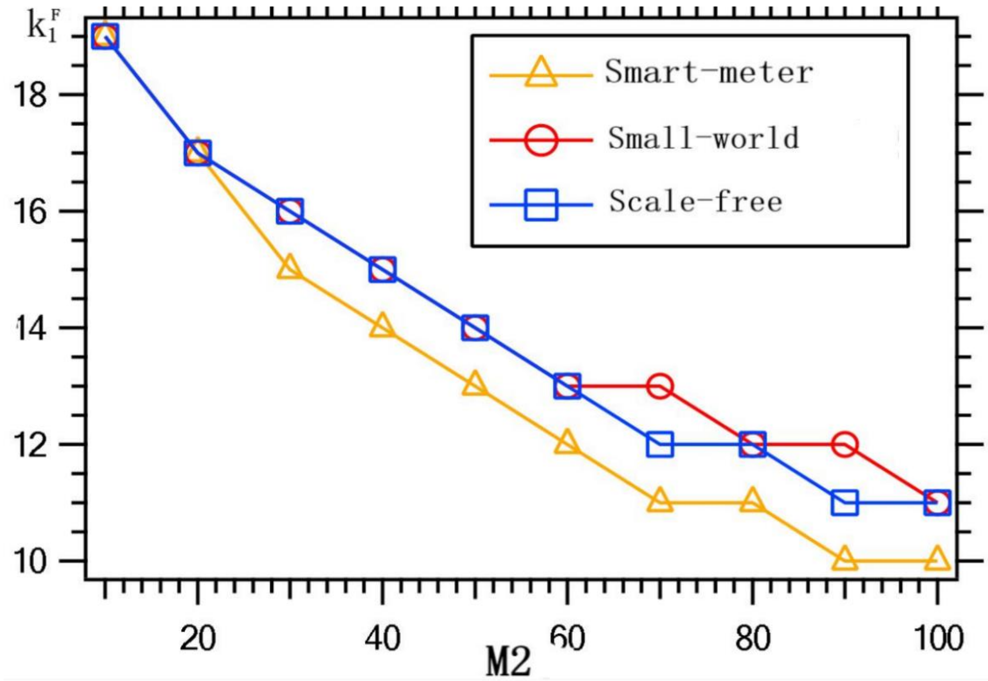
According to the results, with the increased of, more resources should be allocated to Program α and the number of antivirus program of α is increased, and the total damage increased. The results followed the intuition. While the increased of, it requires more time to develop the antivirus programming to secure α vulnerability, which means virus α will inject more nodes and therefore more engineering resources should be assigned to antivirus program α.



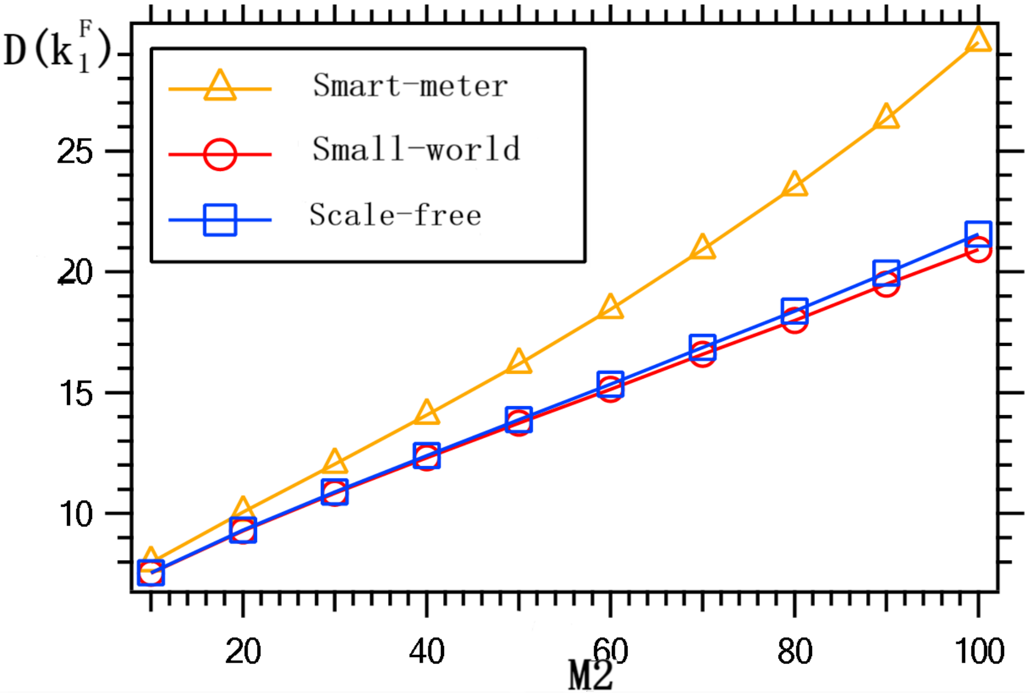
(a)


D（k_F^1）
60
50
40
30
20
10
Smart-meter
Small-world
Scale-free
20
40
M1 60
80
100

(b)


k_1^F
18
16
14
12
10
Smart-meter
Small-world
Scale-free
20
40
60
80
100
M2

(c)



(d)

Figure 6. 8 Comparison results of antivirus-efforts of DOWNHILL-TRADE OFF

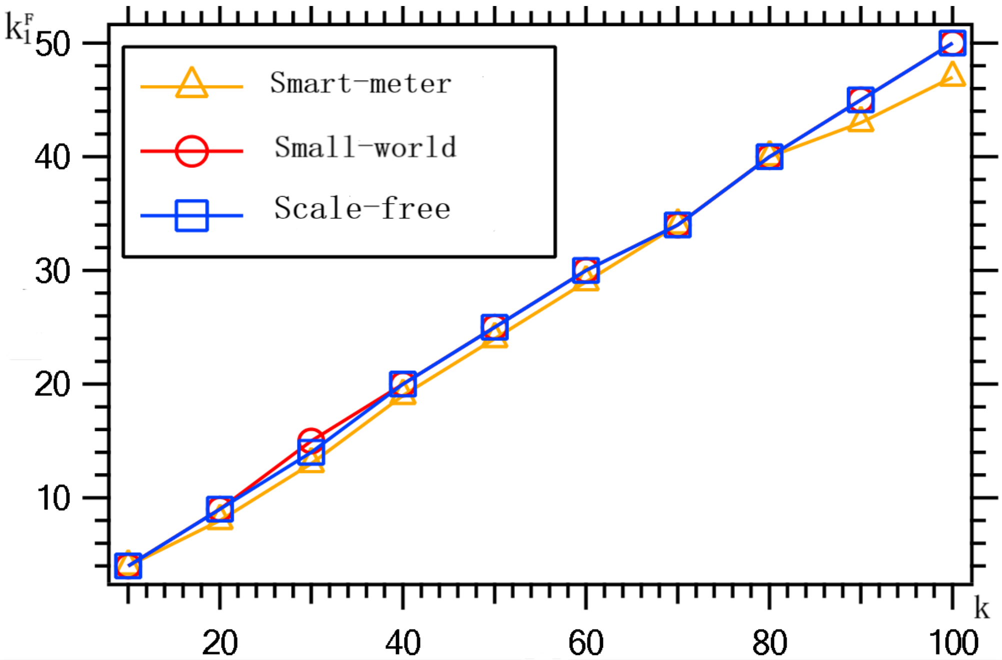
6.6.4 Available Programmers Impact

We simulate the impact of the number of limited antivirus resources (i.e., programmers) for DASD model based on DOWNHILL-TRADE OFF in the section.

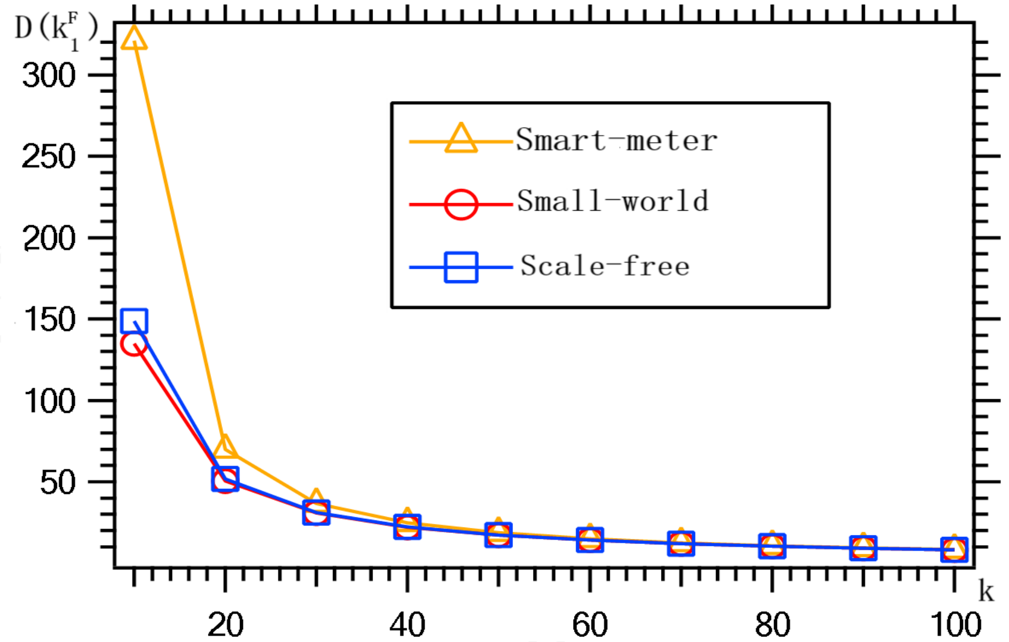
Case set 6: Assume a set of DASD model with =0.01, =0.02, Q(0)=(0.1,...,0.1), =70, =90, v1=3, v2=2, , in the small-world, scale-world network, and smart-meter network of a community, respectively. The results of this set are in Fig. 6.9, where Fig. 6.9 (a) shows the allocation result of antivirus program α and Fig. 6.9 (b) demonstrates the total potential damages under double-virus attacking.

According to the results, with the increased of k, more resources should be allocated to Program α and the number of antivirus program of α is decreased, and the total damage decreased. The results followed the intuition. While the increased of k, there are more resource can be assigned to develop the antivirus programming for α vulnerability, which will enhance the antivirus ability of entire system.

The number of available programmers is taken as an example of the one of limited antivirus resources in this case. Because the demand-side system is implemented multiple distributed appliances in cyber-physical environment, a great number of programmers need to be allocated while multiple viruses attack the grid system. However, there are limited number of engineers in a system, hence, it is important to consider the number of available programmers in reality. The simulation results are shown in Fig. 6.9.



(a)



(b)

Figure 6. 9 Comparison results of different number of limited antivirus resources

6.5 Chapter Summary

Cyber-physical gird is easier to get injected by viruses with the integration of information infrastructures and distributed sensors. There are a great number of private data information and it even to control the operation of power grid in demand side. Therefore, the robustness consideration of the system when virus attacking is more complicated, especially in demand-side. This chapter studies a cyber security strategy under double-virus attacking condition. By modelling the expected state of time evolution, a antivirus- optimization problem is proposed to make a trade-off when two viruses assaulted system simultaneously for minimizing loss. After the numerical simulation studies, a DOWNHILL_TRADEOFF algorithm is developed to validate the effectiveness of the system. The consideration of virus attacking study improve the robust capability of CPS demand-side energy system.

CHAPTER 7

Conclusion and Future Work

7.1 Conclusion

The extreme weather widespread implementation of modern infrastructures has led to grid operation instability. For example, at the end of 2015, Ukraine's power grid suffered from malicious network attacks, and the implantation of computer viruses made the control server lose the ability to perceive and control the physical equipment of the power grid. This led to a large-scale blackout. Therefore, the robust capability of today's power system attracts increasing attention to determine the operation and resilience of the system.

Integration with various distributed energy resources, controllable household appliances, advanced metering infrastructures and the advanced communication facilities, the demand-side information (i.e., users' consumption profile, photovoltaic wind/solar power source, topology and operation data of network, etc.) is able to be monitored, collected, and developed through two-way communication between users and the cyber-physical grid. In this context, consumers are able to manage energy on the demand side and this increases the challenges associated with system robustness.

As mentioned above, this thesis studies cyber-physical robustness enhancements for the demand-side energy system and discusses outage management, communication infrastructure development and cybersecurity challenges from virus attacks. All of these aspects facilitate the capability of the system to self-power and maintain robust operation under extreme conditions and dangerous scenarios. In terms of outage management, there are two levels of resilient energy management for residential system. The first level is the community-level optimization, a resilient energy management scheme which harnesses Battery Energy Storage System (BESS) and the community-scale renewable resources, aiming to improve the self-supply ability of the entire system on the demand side. In addition, the appliance-level optimization is researched in this thesis. Under the power outage scenario, the model schedules the residential energy appliances of multiple households with a bi-level structure, where an individual home energy management system (HEMS) interacts iteratively with a community energy management system (CEMS). It is executed consecutively from community-level to house-level as its constraints. In addition, the communication network layout is considered to improve the robustness of cyber-physical demand management. A complex multi-hop wireless remote metering network with minimal locations and a minimal number of local data centers is developed. A new evolutionary aggregation algorithm (EAA) is introduced and implemented to solve the optimization problem in the n-hop network with the shuffle operation and the switch operation. Furthermore, the cybersecurity strategy to confront virus attacks is researched, and a trade-off scheme to determine the allocation of antivirus programs for avoiding system crash and achieving the minimum potential loss, is proposed. A DOWNHILL algorithm is proposed to address the appropriate allocation strategy under the time evolution of the expected state of the network. The study improves the robustness of the system when it encounters outside virus attacks.

In conclusion, under the research thesis of the cyber-physical robustness study for demand-side energy system, this research work solves feasible solutions for the hierarchical energy management under an outage scenario, communication network layout and antivirus strategies. The contributions of this thesis can be summarized briefly as follows:

Develop a resilient energy management model for residential communities to maximize the self-serve capability, and optimally utilize the household energy consumption and community battery energy storage system. Study on the cooperative energy management at residential community-scale rather than at a single house, which improves the cooperation of multiple houses and facilities the entire community robustness on the demand side.

Propose a hierarchical power management strategy model under power outage which develops an appliance-level schedule of multiple residential houses with a bi-level structure in which individual home energy management system (HEMS) interacts iteratively with community energy management system (CEMS).

Incorporate the load re-shaping ability of controllable resources and the community battery energy storage system into a comprehensive scheme that offers more flexibility under a power blackout.

Provide a decomposed structure, allowing the method to be more practical and scalable for utilization with a different number of units/houses without suffering significant computational burdens.

Secure information security by enabling a user's data to be managed in the Home Energy Management System autonomously rather than exposed.

Propose a complex multiple-hop wireless smart meter network model to improve the communication robustness in a CPS demand-side system.

Develop a new evolutionary aggregation algorithm (EAA) to obtain the minimum number and locations of local data center in the n-hop network with the shuffle operation and the switch operation.

Propose a cyber security strategy under double-virus attacking conditions. By modelling the expected state of time evolution, an antivirus-optimization problem is proposed to make a tradeoff and minimize loss when two viruses assault the system simultaneously.

Propose A DOWNHILL-TRADE OFF algorithm to address appropriate allocation strategy under the time evolution of the expected state of the network. The DOWNHILL-TRADE OFF algorithm considers the representative networks (Small-world network, Scale-free network and Smart-meter network of a community). Experiments under comparison with other algorithms verify the efficiency and effectiveness of the proposed method.

7.2 Future Work

As the future work direction, the security strategy of double-antivirus model will be extended to more sophisticated, such as three or multiple viruses attacks. Multiple more complicated virus spreading models such as the time-varying spreading model, the stochastic spreading, and the impulsive model will be studied in the future. In addition, to solve the multiple virus assaulting problem, the intelligent algorithm will be implemented to optimize effective and efficient, i.e., NAA algorithm and binary algorithm.

Furthermore, in the cyber-physical grid system, there will be a large number of network participants (retailers, large-scale end-users, microgrid systems, power distributors, load aggregators, etc.), which will bring a great challenge to the privacy protection and information security of participants. In the past few years, a technology called secure multi parties computing (SMC) [159] has been widely studied, which is expected to provide a new solution for information security in demand management. Therefore, a secure multi-party computation-based demand-side data communication module will be researched in the future, which utilizes homomorphic encryption to protect the private information of users, and facilities the cyber-physical robustness for demand-side energy management.

Homomorphic encryption technology provides a new solution for secure communication in an active distribution network. Dynamic encryption technology can effectively protect the data privacy of each distributed communication participant in the active demand-side network, and can safely aggregate and cooperate with each other. At present, some research work has carried on the preliminary research. In [160], a data aggregation framework for the distribution network side based on homomorphic encryption technology is proposed. Paillier encryption technology is used to encrypt and aggregate the meter data of end-users and transfer the information to the control center so that the control center can calculate the regional load without decryption. [161] also uses Paillier encryption technology to propose a clearing price settlement framework for the power market. The framework consists of two stages: in the first stage, the load data is encrypted and aggregated by using Paillier encryption technology, and the node load is calculated by using the encrypted data; In the second stage, the market-clearing price is settled by using the load calculated in the first stage. The existing research work mainly relies on additive homomorphism technology for power grid data aggregation. In the future CPS demand-side network, more secure cooperative applications driven by homomorphic encryption can be expected to be researched and developed. On the one hand, more complex distribution network analysis and calculation, such as distribution network power flow calculation, can be carried out by combining more kinds of homomorphic encryption algebraic operation technology; On the other hand, more implementations of demand-side security multi-party cooperation applications can be developed.

Reference

[1] V.C. Gungor, D. Sagin, et al., "Smart Grid Technologies: Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529-539, Nov. 2011

[2] F.J. Luo, Z.Y. Dong, J.H. Zhao, Z. Xu, K.P. Wong., and Y.Y. Chen, "Enabling the Big Data Analysis in the Smart Grid," [C]// Power and Energy Society General Meeting. Denver: IEEE, 2015: 1-6.

[3] F.J. Luo, Z.Y. Dong, Y.Y. Chen, Y. Xu, Meng Ke and Kit Po Wong, "Hybrid Cloud Computing Platform: The Next Generation IT Backbone for Smart Grid," Power and Energy Society General Meeting. San Diego: IEEE, 2012: 1-7.

[4] Y. Tang，Q. Chen，M.Y. Li，et. al., "Overview on cyber-attacks against cyber physical power system[J]．Automation of Electric Power System,"2016, 40(17)：59-69.

[5] Y, B. Jiang, Y.H. Song, et. al., "Review of Risk Assessment for Energy Internet Part I: Physical Level[J]," Proceedings of the CSEE，2016，36(14)：3806-3816(in Chinese．

[6] G. Liang, J. H. Zhao, S.R. Weller et. al., "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017. Blackout: Implications for False Data Injection Attacks," IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017.

[7] J. Casey, M. Fukurai, D. Hernandez, et. al., "Power Outages and Community Health: a Narrative Review.", Current Environmental Health Reports (2020) 7:371–383

[8] Q.L. Guo，S.J. Xin，J.H. Wang，et. al., "Comprehensive Security Assessment for a Cyber Physical Energy System：a lesson from Ukraine's blackout[J]," Automation of Electric Power Systems，2016，40(5):145-147

[9] N. Bui, A. P. Castellani, P. Casari and M. Zorzi, "The internet of energy: a web-enabled smart grid system," in IEEE Network, vol. 26, no. 4, pp. 39-45, July-August 2012.

[10] T. Hong, "Energy forecasting: Past, present, and future," Foresight, no.32,

pp.43-48, 2013.

[11] Y.B. Jiang，Y.H. Song，Yi Ding，et. al ."Review of risk assessment for energy internet part II ： information and market level [J]" .Proceedings of the CSEE，2016， 36(15)， 4023-4033

[12] J. Zhao, F. Wen, Y. Xue and Z.Y. Dong, "The Modeling and control framework Analysis of Cyber-physical system," Automation of Electric Power System, August 2011, Vol. 35, no.16.

[13] P. Palensky, D. Dietrich, "Demand side management: demand response, intelligent energy systems, and smart loads[J]," IEEE Transactions on Industrial Informatics， 2011， 7(3):381-388 .

[14] M. Moness, and M. Mousrafa, "A survey of cyber-physical advances and challenges of wind energy conversion systems： prospects for internet of energy[J]," IEEE Internet of Things Journal， 2016， 3(2):134-145 .

[15] Ali Salman, S.B. Qaisar, H. Saeed, et. al., "Network challenges for cyber physical systems with tiny wireless devices: a case study on reliable pipeline condition monitoring[J]," Sensors， 2015， 15(4):7172-205 .

[16] Y. Wadgawan, N. Clifford, "Evaluating resilience of gas pipeline systems under cyber-physical attacks： a function-based methodology [C]," The 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy，Vienna，Austria，2016： 71-80 .

[17] W. Ling， D. Liu， D. Yang， C. Sun, "The situation and trends of feeder automation in China[J]. Renewable and Sustainable Energy Reviews，"October 2015，（50）： 1138-1147

[18] N. Yu, C. Hui, S. Chen, L. Dong and Y. Liu, "Research on IEC 61968 based message design for intelligent operation and maintenance center[C]," 2014 China International Conference on Electricity Distribution （CICED）， 23-26 September, 2014

[19] Y.M. Lu， S. Chen, G.X. Lu, et.al., "Information modeling of distribution grid's operation situation under disastrous condition and its application[C]," 2016 China International Conference on Electricity Distribution （CICED）， 2016.

[20] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," Third

Symposium on Operating Systems Design and Implementation, Louisiana, USA, 1999, pp.173-186.

[21] E. Lee, “Cyber physical systems: Design challenges,” in ISORC. IEEE, 2008, pp. 363–369.

[22] I. Horvath and B. Gerritsen, “Cyber-physical systems: concepts, technologies and implementation principles,” in TMCE, 2012, pp. 19–36.

[23] K. Schneider, C.C. Liu, J.P. Paul, et.al., “Assessment of interactions between power and telecommunications infrastructures,” IEEE TPWRS, 2006.

[24] Y. Sun et al., “Verifying noninterference in a cyber-physical system the advanced electric power grid,” in QSIC. IEEE, 2007, pp. 363–369.

[25] I. Sharma，J, Dong，A.A., Malikopoulos, et al., “A modeling framework for optimal energy management of a residential building[J],” Energy & Buildings，2016(130):55-63

[26] Y. Li, B. Wang, and F.X. Li. “Outlook and thinking of flexible and interactive utilization of intelligent power[J],” Automation of Electric Power Systems，2015，39(17):2-9

[27] W.H. Sanders, “Progress towards a resilient power grid infrastructure,” in Proc. IEEE PES General Meeting, 2010.

[28] M. Pipattanasomporn，M. Kuzlu，Rahman S., “An algorithm for intelligent home energy management and demand response analysis[J]”, IEEE Transactions on namingSmart Grid，2012，3(4):2166-2173．

[29] C. Wright, D. Daly, F. Kathan, et.al., “Assessment of demand response and advanced metering: 2006 staff report,” 2006.

[30] A. Ipakchi and F. Albuyeh, “Grid of the future,” Power and Energy Magazine, IEEE, vol. 7, pp. 52-62, 2009.

[31] U.S. Department of Energy, “Benefits of demand response in electricity markets and recommendations for achieving them: a report to the United State Congress pursuant to section 1252 of the Energy Policy Act of 2005”, Feb. 2006.

[32] F. Zhang, F.J. Luo, Z.Y. Dong, and G. Ranzi, “Resilient Energy Management for Residential Community under Grid Outage,” 2019 9th International Conference on Power and Energy Systems (ICPES2019)

[33] G. Hart, “Nonintrusive appliance load monitoring[J],” Proceedings of the IEEE,

1992, 80(12): 1870-1891.

[34] M. Berges, E. Goldman, H. S. Matthews, L. Solbelman, “Enhancing Electricity Audits in Residential Buildings with Non-Intrusive Load Monitoring[J],” Journal of Industrial Ecology, 2010, 14(5): 844-858.

[35] H. Lin and H. T. Yang, “Load Recognition for Different Loads with the Same Real Power and Reactive Power in a Non-Intrusive Load-Monitoring System[C],” 12th International Conference on Computer Supported Cooperative Work in Design: 2008: 1-8.

[36] W.C. Kong, Z.Y. Dong, Hill D, F.J. Luo, and Yan Xu. “Improving Nonintrusive Load Monitoring Efficiency via a Hybrid Programming Method[J]”. IEEE Transactions on Industrial Informatics, 2016, 12(6): 2148-2157.

[37] W.C. Kong, Z.Y. Dong, J. Ma, Hill D, J.H. Zhao, and F.J. Luo. “An Extensive Approach for Non-Intrusive Load Disaggregation with Smart Meter Data[J]”. IEEE Transactions on Smart Grid, 2016, DOI: 10.1109/TSG.2016.2631238.

[38] F.J. Luo, J.H. Zhao, Z.Y. Dong, et al. “Cloud-Based Information Infrastructure for Next-Generation Power Grid: Conception, Architecture, and Applications[J]”. IEEE Transactions on Smart Grid, 2015, 7(4): 1896-1912.

[39] K.J. Liu, Yi Gao, F.L. Song, “Risk Assessment Framework Design on Flexibility Power Grid Planning and Its Application Prospect”. ELECTRIC POWER CONSTRUCTION, 2015, 35(12): 1-5.

[40] E.A. Lee，S. A. Seshia. “Introduction to Embedded Systems：A Cyber-Physical Systems Approach[M]”, Beijing：China Machine Press，2012.

[41] E. Lee, “A Cyber-physical systems are computing foundations adequate[C]” Position Paper for NSF Workshop on Cyber-Physical Systems：Research Motivation Techniques and Roadmap. 2006，2.

[42] Y. Susuki，T. J. Koo，H. Ebina et al. “A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance[J]”. Proceedings of the IEEE，100(1)，2012：225-239

[43] M. D. Ili´c，X. Le，Usman A. Khan， M. F. Moura. “Modeling of Future Cyber–Physical Energy Systems for Distributed Sensing and Control[J]”. IEEE Transactions on Systems，Man And Cybernetics—Part A:Systems And Humans，2011，40(4)：825-838.

[44] B.Sayak “Cyber-physical modeling analysis and optimization-a shipboard smart grid reconfiguration case study [Doctor’s Dessertation]. “Manhattan, Kansas: Kansas State University, 2004

[45] Y. Wang, D. Liu, C. Sun. “A Cyber Physical Model Based on a Hybrid System for Flexible Load Control in an Active Distribution Network[J]”. Energies, 2017, 10, 267.

[46] Y. Wang, D. Liu, etc., “Research on hybrid system modeling method of power grid information physical system [J]”. China Electrical Engineering Acta Sinica, 2016, 36 (6): 1464-1470

[47] A Giani et al., “The viking project: An initiative on resilient control of power networks,” in ISRCS. IEEE, 2009, pp. 31–35

[48] F. Tullio, L. Marco, V. Della, “Real-Time Modeling for Direct Load Control in Cyber-Physical Power Systems[J]”. IEEE Transactions on Industrial Informatics, 2011, 7(4): 689-698.

[49] M. Ni, Q. Chen, M. Li, et al. “A Frequency Control Model for Cyber Physical Power System Considering Demand Response Strategy[C]. In: Applied Energy Symposium and Forum 2017: Renewable Energy Integration with Mini/Microgrid. (EI)”

[50] Y. Sun and F. Zhang, “Modeling Method Applied to Load Control of Cyber Physical Power System. China Academic Journal Electronic Publishing House,” Available on: http://www.naki.net

[51] Y. Xue, and M. Li, “Coupling modeling method of power grid information physical system based on correlation characteristic matrix [J]. Power system automation, 2018. (EI)”

[52] X. Ye. F. Wen, et al, “Propagation mechanism of cyber physical security risks in power system. Power System Technology”, 2015

[53] Guo Jing, L. W., etc. “Reliability modeling and assessment of island cyber physical microgrid and assessment of island cyber physical microgrid system”. Power System Technology, 2018, 42(5): 1441-1450.

[54] Z. Jiang, J. Liu, etc. “Key technology for reliability assessment of distribution network cyber physical system.” Electric Power Automation Equipment, 2017,37(12):30-42

[55] M. Ghanavati and A. Chakravarthy, “Demand-Side Energy Management by Use of a Design-Then- Approximate Controller for Aggregated Thermostatic Loads”, 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009

[56] Y. Tan, M. C. Vuran, S. Goddard Spatio-Temporal Event Model for Cyber-Physical Systems[C]. In: IEEE International Conference on Distributed Computing Systems Workshops. IEEE Computer Society, 2009, 44-50.

[57] Bhave A, Garlan D, Krogh B. Krogh, et al., “Multi -domain modeling of cyber-physical systems using architectural views[C],” In: Proceedings of the 1st Analytic Virtual Integration of Cyber-Physical Systems. California, USA, 2010, 43-50.

[58] A.Castelluccia, D. Francillon, and C. B. Soriente “On the difficulty of software-based attestation of embedded devices”, in Proc. 16th ACM Conf. Comput.

[59] “A Systems View of the Modern Grid”, National Energy Technology Laboratory (NETL), U.S. Department of Energy (DOE), 2007.

[60] A.Y. Saber, “Efficient utilization of renewable energy sources by gridable vehicles in cyber-physical energy systems,”Systems Journal, IEEE, vol. 4, no. 3, pp. 285–294, 2010

[61] S. Karnouskos, “Cyber-physical systems in the smartgrid,” in INDIN. IEEE, 2011, pp. 20–23.

[62] B.M. Lei， D. Yi， S.C. Zheng ．Reference of international energy system transformation to energy internet construction in China [J] ．Distributed Energy，2017， 2(2):11-19

[63] Q. Zhu et al., “Robust and resilient control design for cyber-physical systems with an application to power systems,” in CDC-ECC, 2011.

[64] S. Karnouskos, “Cyber-physical systems in the Smart Grid,” in INDIN. IEEE, 2011, pp. 20–23.

[65] Common Cybersecurity Vulnerabilities in Industrial Control Systems, Department of Homeland Security (DHS) Control Systems. Security Program (CSSP), May 2011.

[66] P.Q. Li, X. Li, W. Tang， et al ．Consumer choice for an industry in statistical synthesis method-based load modeling [J] ．Automation of Electric Power

Systems, 2005, 29(14):34-38.

[67] Y. Sun et al., “Verifying noninterference in a cyber-physical system the advanced electric power grid,” in QSIC. IEEE, 2007, pp. 363–369.

[68] C. Song, J. Song . Parameter optimization for BP neural network with GA on short-term gas load prediction[J] . Industrial Control Computer, 2012, 25(4):82-84

[69] Y. Ding, H.P. Jia, Y.H. Song, et al . Review of reliability evaluation methods for the smart grid considering the interaction between wind power and flexible demand resources[J] . Proceedings of the CSEE, 2016, 36(6):1517-1526

[70] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, BCyber attack in a two-area power system: Impact identification using reachability, in Proc. Amer. Control Conf., Jul. 2010, pp. 962–967.

[71] W. Shao, M.H. Yang, X. Zheng, et al . Functions and methods of load forecasting in power generation market[J] . Electric Power, 2000, 33(11)

[72] Q. Zhu et al., “Robust and resilient control design for cyber-physical systems with an application to power systems,” in CDC-ECC, 2011

[73] Lee K H, Hong J H, Kim T G .System of systems approach to formal modeling of CPS for simulation-based analysis[J] . ETRI Journal, 2015, 37(1): 175-185 .

[74] B.Lei, Q.X. Wang, X. Chen et al, “Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior[J] “" ACM SIGBED Review, 2011, 8(2): 7-10

[75] F. S. Gonçalves, D. Pereira, E. Tovar et al . Formal verification of AADL models using UPPAAL[C]//2017 VII Brazilian Symposium on Computing Systems Engineering (SBESC) . Curitiba, Brazil: IEEE, 2017: 117-124 .

[76] Y.M. Lu. “Formal modeling and verification of intelligent distribution network information model [doctoral dissertation],” Shanghai: Shanghai Jiaotong University, 2013

[77] B.Y. Qin, D. Liu, P. Zhang, et.al., “Formal modeling and verification of smart distribution grid based on common information model[C]//2016 China International Conference on Electricity Distribution (CICED) . Xi'an, China:

IEEE, 2016: 1-6 .

[78] Y. Mo et al., “Cyber–physical security of a smart grid infrastructure,” Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012.

[79] Sridhar S, Hahn A, Govindarasu M . Cyber-physical system security for the electric power grid[J] . Proceedings of the IEEE, 2012, 100(1): 210-224 .

[80] H. Lei, C. Singh, A. Sprintson Reliability modeling and analysis of IEC 61850 based substation protection systems[J] . IEEE Transactions on Smart Grid, 2014, 5(5): 2194-2202 .

[81] Y.H. Zhu, J. Yan, Sun Yan, et al . Revealing cascading failure vulnerability in power grids using risk-graph[J] . IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12):3274-3284 .

[82] E.C. Martins, F.G. Jota, “Design of networked control systems with explicit compensation for time-delay variations,” IEEE Trans on System, Man, and Cyberneties: Part C, 2010, 40(3): 308-318.

[83] A Cardenas et al., “Challenges for securing cyber physical systems,” in Workshop on Future Directions in Cyber-physical Systems Security. DHS, 2009.

[84] X. Zhan, G. Xiao, J. Qing-Shan, W. Jiang, et al., “Performance Analysis and Comparison on Energy Storage Devices for Smart Building Energy Management,” Smart Grid, IEEE Transactions on Smart Grid, vol. 3, pp. 2136-2147, 2012.

[85] Z.L. Zhao, B. Zou, “The optimal operation strategy and simulation for CCHP system,” IOP Conference Series: Earth and Environmental Science, vol. 168, pp. 012007, 2018.

[86] C. Rottondi, M. Duchon, D. Koss et al., “An Energy Management Service for the Smart Office,” Energies, vol. 8, pp. 11667, 2015.

[87] S.Y. Gao, C. Wang, H.C. Zhang et al., “Research and Control Strategy of Air-conditioning Load Model Based on Demand Response,” 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), 2018.

[88] J.A. Primbs and C.H. Sung, “Stochastic receding horizon control of constrained liner systems with state and control multiplicative noise,” IEEE Trans. Autom. Control, vol. 54, no. 2, pp. 221-230, Feb. 2009.

[89] H.H. Qian, X.W. Huang, H. Yu et al., “Cyber-physical thermal management of 3d multi-core cache-processor system with microfluidic cooling,” JOLPE, 2011.

[90] V. Rafe, A.T. Rahmani, L. Baresi, P. Spoletini, “Towards automated verification of layered graph transformation specifications [J],” IET Software，3(4): 276-291, 2009.

[91] N. Koch, “Classification of model transformation techniques used in UML-based Web engineering [J],” IET Software, 2007, 1(3):98-111

[92] S.L. Bao，J. Zhou, “Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model [J],” Automation of Electric Power Systems, 2016, 40(17): 99-105

[93] Y. Ding, L. Cheng, Y. Zhang et al., “Operational reliability evaluation of restructured power systems with wind power penetration utilizing reliability network equivalent and time-sequential simulation approaches[J],” Journal of Modern Power Systems and Clean Energy, 2014, 2(4): 329-340 .

[94] Y. Susuki, T.J. Koo, H. Ebina et al., “A hybrid system approach to the analysis and design of power grid dynamic performance,” Proceedings of the IEEE, 100(1): 225-239, 2012.

[95] J. Munoz, J.N. Redondo, P.J. Ruiz et al., “ Natural gas network modeling for power systems reliability studies[C],” in 2003 IEEE Bologna Power Tech Conference Proceedings, Bologna, Italy: IEEE, 2003.

[96] H. Zhu, J. Lu, C.H. Tang et al., “Research on the Mechanism of Distribution Network CPS Security Impact,” in 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), 2019

[97] Byrd, S. Matthewman, “Exergy and the city: the technology and sociology of power,” in Journal of Urban Technology, Vol.21, 2014.

[98] U.S. Energy Information Administration [Online]. Available: https://www.eia.gov/electricity, accessed on 28/07/2018.

[99] M. Mylrea, S. Gourisetti, “Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security,” Proceedings of the Resilience Week (RWS) 2017, IEEE, 2017, p

[100] H.Y Shin and B. Ross, “Plug-In Electric Vehicle to Home (V2H) Operation Under a Grid Outage,” IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 2032-2041,

2016.
[101] P. Tuttle, R. L. Fares, R. Baldick, and M. E. Webber, “Plug-in vehicle to home (V2H) duration and power output capability,” in Proc. IEEE Transp. Electrif. Conf. Expo (ITEC), USA, Jun. 2013, pp. 1–7.
[102] P. Tian, X. Xiao, K. Wang and R. Ding, “A hierarchical energy management system based on hierarchical optimization for microgrid community economic operation,” IEEE Transaction on Smart Grid, Vol.7, issue 5, 2016.
[103] N. Gatsis, G. Giannakis, “Residential load control: distributed scheduling and convergence with lost AMI Message,” IEEE Transaction on Smart Grid, Vol.3, No. 2, 2012.
[104] F. Ye, Y. Qian and R.Q. Hu, “A real-time information-based demand-side management system in smart grid,” IEEE Transaction Parallerl Distrib. Syst., vol27, no. 2, pp. 329-339, 2016.
[105] Y.P. Cai, G.H. Huang, Q. Tan, and Z.F. Yang, “Community-scale renewable energy systems planning under uncertainty—An interval chance-constrained programming approach,” Renewable and Sustainable Energy Reviews, vol.13, no. 4, pp. 721-735, 2008.
[106] M.S., S. Sirouspour, “Priority-based microgrid energy management in a network environment,” IEEE Transactions on Sustainable Energy, Vol.9, issue 2, 2017.
[107] N. Pogaku, M. Prodanovic, T.C, Green, “Energy management in autonomous microgird using stability-constrained droop control of inverters,” IEEE International Conference on System Engineering, 2007.
[108] Y. Li, C. Ruiz, “An intergrated framework of agent-based modelling and robust optimization for microgrid energy management,” Applied Energy, Vol. 129, 2914
[109] Y.K. Chen, Y. Wu, C. Song, Y. Chen et al, “Design and implementation of energy management system with fuzzy control for DC microgrid systems,” IEEE Transactions on Power Electronics, vol. 28 (4): 1563-1570, 2013
[110] J. Mengelkamp, J. Garttner, K. Rock, etc., “Designing microgrid energy markets--a case study: the Brooklyn microgrid,” Applied Energy, vol. 210, pp. 870-880, 2018.
[111] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, “Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers,” IEEE

Transactions on Power Systems, vol. 32, no. 5, pp. 3569-3583, 2017.
[112] N. Liu, X. Yu, W. Fan, C. Hu, T. Rui, Q. Chen, and J. Zhang, “Online energy sharing for nanogrid clusters: a Lyapunov optimization approach,” IEEE Transactions on Smart Grid, vol. 14, no. 8, pp. 1-13, 2016.
[113] Y.X. Zuo, and H.W. Kuek, “Design and implementation of bluetooth energy meter,” in Proc. Fourth International Conference on Information, Communications & Signal Processing, Singapore, Dec. 2003, pp. 1474 – 1477
[114] Y.S. Son, T. Pulkkinen, K.Y. Moon, and C. Kim, “Home energy management system based on power line communication,” IEEE Trans. on Consumer Electronic, vol. 56, pp: 1380 – 1386, Aug. 2010.
[115] P.K. Lee and L.L. Lai, “A practical approach of smart metering in remote monitoring of renewable energy applications,” IEEE Power & Energy Society General Meeting, Calgary, Canada, July 2009, pp. 1 – 4.
[116] M. Tasdighi and A. K, “Residential Microgrid Scheduing Based on Smart Meters Data and Temperature Dependent Thermal Load Modeling,” IEEE Transactions on Smart Grid, 2014
[117] B. Ugale, P. Soni, T. Pema, and A. Patil, “Role of cloud computing for smart grid of India and its cyber security,” in Proc. of IEEE, 2011.
[118] Byrd and S. Matthewman, “Exergy and the city: the technology and sociology of power,” Journal of Urban Technology, vol.21, 2014.
[119] U.S. Energy Information Administration [Online]. Available: https://www.eia.gov/electricity, accessed on 28/07/2018.
[120] Ausgrid reported power outages [Online]. Available: https://www.ausgrid.com.au/poweroutages, accessed on 28/07/2018.
[121] Z. Zhao, W. Lee, Y. Shin, and K. Song, “An optimal power scheduling method for demand response in home energy management system,” IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1391-1400, 2013.
[122] M.A. Pedrasa, T. Spooner, and I. MacGill, “Coordinated scheduling of residential distributed energy resources to optimize smart home energy services,” IEEE Transactions on Smart Grid, vol. 1, no. 2, 2010.
[123] F. Luo, G. Ranzi, C. Wan, Z. Xu, and Z.Y. Dong, “A multi-stage home energy management system with residential photovoltaic penetration,” IEEE Transactions on Industrial Informatics, early access.
[124] D.P. Tuttle, R.L. Fares, R. Baldick, and M.E. Webber, “Plug-in vehicle to home

(V2H) duration and power output capability," in Proc. IEEE Transp. Electrif. Conf. Expo (ITEC), USA, Jun. 2013, pp. 1–7.

[125] R. Roche, F. Berthold, F. Gao, F. Wang, "A model and strategy to improve smart home energy resilience during outages using vehicle-to-home," IEEE International Electric Vehicle Conference (IEVC), Florence, 2014, pp. 1-6.

[126] H.Y Shin and B. Ross, "Plug-In Electric Vehicle to Home (V2H) Operation Under a Grid Outage," IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 2032-2041, 2016.

[127] Nissan's Vehicle-to-Home Electricity Supply System [Online]. Available at: https://www.nissanglobal.com/EN/TECHNOLOGY/OVERVIEW/vehicle_to_home.html

[128] F.J. Luo, J. Zhao, Z.Y. Dong, Y. Chen, Y. Xu, X. Zhang, and K.P. Wong, "Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications," IEEE Transactions on Smart Grid, vol.7, no.4, pp.1896-1912, 2016.

[129] J. Bracken and J. McGill, "Mathmatical programs with optimization problems in the constraints," Oper. Res., vol. 21, no. 1, pp. 37-44, 1973.

[130] Mosek Optimizer [Online]. Available at: https://www.mosek.com/

[131] F. Luo, J. Zhao, and Z.Y. Dong, "A new metaheuristic algorithm for real-parameter optimization: natural aggregation algorithm," in Proc. IEEE Congress on Evolutionary Computation, Vancouver, 2016.

[132] F. Luo, Z.Y. Dong, Y. Chen, and J. Zhao, "Natural aggregation algorithm: A new efficient metaheuristic tool for power system optimizations," in Proc. 7th IEEE International Conference on Smart Grid Communications, Sydney, Oct 2016.

[133] A. Barbato, A. Capone, G. Carello, M. Delfanti, M. Merlo, and A. Zaminga, "House energy demand optimization in single and multi-user scenarios," in Proc. IEEE International Conference on Smart Grid Communications, Oct 2011.

[134] S. Kakran and S. Chanana, "Energy scheduling of residential community equipped with smart appliances and rooftop solar," in Proc. 7th International Conference on Power Systems, India, Dec 2017.

[135] K. Mikhaylov, M. Pettissalo, J. Janhunen, and J. Iinatti, "Per- formance of a low-power wide-area network based on lora technology: Doppler robustness,

scalability, and coverage," Int. J. Distrib. Sensor Netw., vol. 13, no. 3, 2017, doi: 10.1177/1550147717699412.

[136] Y. Miao, Y. Hao, and K. Hwang, "Narrow band internet of things," IEEE Access, vol. 5, pp. 20 557–20 577, 2017.

[137] X. Luan, Z. Zheng, T. Wang, J. Wu, and H. Xiang, "Hybrid cooperation for machine-to-machine data collection in hierarchical smart building networks," IET Commun., vol. 9, no. 3, pp. 421–428, Feb. 2015.

[138] Y. Cao, D. Duan, X. Cheng, L. Yang, and J. Wei, "QoS-oriented wireless routing for smart meter data collection: Stochastic learning on graph," IEEE Trans. Wireless Commun., vol. 13, no. 8, pp. 4470–4482, Aug. 2014.

[139] Y. Xu and W. Wang, "Wireless mesh network in smart grid: Modeling and analysis for time critical communications," IEEE Trans. Wireless Commun., vol. 12, no. 7, pp. 3360–3371, Jul. 2013.

[140] S. Aust and T. Ito, "Sub 1 GHz wireless LAN propagation path loss models for urban smart grid applications," in Proc. Int. Conf. Comput., Netw., Commun., Jan. 2012, pp. 116–120.

[141] E. K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," IEEE Commun. Mag., vol. 50, no. 8, pp. 46–52, Aug. 2012.

[142] S. Aust, R. V. Prasad, and I. G. M. M. Niemegeers, "Performance evalu- ation of sub 1 GHz wireless sensor networks for the smart grid," in Proc. 37th Annu. IEEE Conf. Local Comput. Netw., Oct. 2012, pp. 292–295.

[143] A Sydney, C. Scoglio, and D. Gruenbacher, "The impact of optimizing algebraic connectivity in hierarchical communication networks for transmission operations in smart grids," in Proc. IEEE PES Innovative Smart Grid Technol. Conf., Feb. 2013, pp. 1–6.

[144] S. Gormus, Z. Fan, Z. Bocus, and P. Kulkarni, "Opportunistic communications to improve reliability of ami mesh networks," in Proc. 2nd IEEE PES Int. Conf. Exhib. Innovative Smart Grid Technology, Dec. 2011, pp. 1–8.

[145] C. Qian, Z. Luo, X. Tian, X. Wang, and M. Guizani, "Cognitive transmis- sion based on data priority classification in WSNs for smart grid," in Proc. IEEE Global Commun. Conf., Dec. 2012, pp. 5166–5171.

[146] N. Lu, and L. Cai, "Reliable wireless communication networks for demand response control," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 133–140, Mar. 2013.

[147] Z. Yang, S. Ping, H. Sun, and A. H. Aghvami, “CRB-RPL: A receiver- based routing protocol for communications in cognitive radio enabled smart grid,” IEEE Trans. Veh. Technol., vol. 66, no. 7, pp. 5985–5994, Jul. 2017.

[148] J. Gharavi and C. Xu, “Traffic scheduling technique for smart grid advanced metering applications,” IEEE Trans. Commun., vol. 60, no. 6, pp. 1646–1658, Jun. 2012.

[149] H. Miao, G. Chen, and Z. Dong, “Enhanced evolutionary heuristic ap- proaches for remote metering smart grid networks,” IET Netw., vol. 5, no. 6, pp. 153–161, Nov. 2016.

[150] S. Usharani, V.V. Ananth, and D. Velmurugan, “A survey on software effort estimation,” in Proc. Int. Conf. Elect., Electron., Optim. Techn., Chennai, India, Mar. 2016, pp. 505–509.

[151] A.L. Barabási and R. Albert, “Emergence of scaling in random net- works,” Science, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

[152] O. Kephart and S. R. White, “Directed-graph epidemiological models of computer viruses,” in Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy, May 1991, pp. 343–359. J. R. C. Piqueira, A. A. de Vasconcelos, C. E. C. J. Gabriel, and

[153] V. O. Araujo, “Dynamic models for computer viruses,” Comput. Secur., vol. 27, nos. 7–8, pp. 355–359, 2008.

[154] S. Xu, W. Lu, and Z. Zhan, “A stochastic model of multivirus dynamics,” IEEE Trans. Depend. Sec. Comput., vol. 9, no. 1, pp. 30–45, Jun./Feb. 2011

[155] W.J. Bai, T. Zhou, and B.H. Wang, “Immunization of susceptible- infected model on scale-free networks,” Phys. A, Statist. Mech. Appl., vol. 384, no. 2, pp. 656–662, Oct. 2007.

[156] T. Zhou, J.G. Liu, W.J. Bai, G. Chen, and B.H. Wang, “Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity,” Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top., vol. 74, no. 5, Nov. 2006, Art. no. 056109.

[157] R. Albert and A. Barabási, “Statistical mechanics of complex networks,” Rev. Modern Phys., vol. 74, no. 1, pp. 47–97, Jan. 2002

[158] A.-L. Barabási and R. Albert, “Emergence of scaling in random networks,” Science, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

[159] R. Pibernik, Y. Zhang, F. Kerschbaum, and A. Schropfer, “Secure Collaborative

Supply Chain Planning and Inverse Optimization," The JELS Model[J]. European Journal of Operational Research, 2011, 208: 75-85.

[160] C. Thoma, T. Cui, and F. Franchetti, "Privacy Preserving Smart Metering System Based Retail Level Electricity Market[C]," Power and Energy Society General Meeting. Denver: IEEE, 2013: 1-5.

[161] L. Liu, H. Wang, X. Liu et al. "Green Cloud: A New Architecture for Green Data Center[C]," 6th International Conference on Autonomic Computing and Communications, Barcelona: 2009: 29-38.