THE UNIVERSITY OF SYDNEY

COPYRIGHT AND USE OF THIS THESIS

This thesis must be used in accordance with the provisions of the Copyright Act 1968.

Reproduction of material protected by copyright may be an infringement of copyright and copyright owners may be entitled to take legal action against persons who infringe their copyright.

Section 51 (2) of the Copyright Act permits an authorized officer of a university library or archives to provide a copy (by communication or otherwise) of an unpublished thesis kept in the library or archives, to a person who satisfies the authorized officer that he or she requires the reproduction for the purposes of research or study.

The Copyright Act grants the creator of a work a number of moral rights, specifically the right of attribution, the right against false attribution and the right of integrity.

You may infringe the author's moral rights if you:

- fail to acknowledge the author of this thesis if you quote sections from the work
- attribute this thesis to another author
- subject this thesis to derogatory treatment which may prejudice the author's reputation

For further information contact the University's Director of Copyright Services

sydney.edu.au/copyright

THE UNIVERSITY OF SYDNEY

Secure Data Management and Transmission Infrastructure for the Future Smart Grid

By

Xin Zhang

B.E. (Computer Science and Technology)

A thesis submitted in fulfilment of the requirements for the degree of

Master of Philosophy

in

School of Electrical and Information Engineering

Faculty of Engineering and Information Technology

The University of Sydney

NSW 2006, Australia

March, 2016

Declaration

This thesis is original and the work which is presented is on my own work, to the best of my knowledge and brief, except where due reference has been made in the text. It has not been accepted for the award of any other degree or diploma in any university or other tertiary institution.

Signature (Candidate):

Xin Zhang

Acknowledgement

This thesis is finished with the University of Sydney. It marks the completion of my 2-year MPhil study, and it also means the beginning of a next stage in my life. There are so many people I want to thank for.

I would like to express my genuine gratitude to my supervisor, Prof. Zhao Yang Dong. I am honored to be one of his students. When I decided to pursue my higher degree in Australia, Prof. Dong provided loads of valuable information for me and guided me through my application. His insight, hard work and leadership have had a great influence on me. I would also like to thank Dr. Jin Ma for being my auxiliary supervisor. Whenever I met with difficulties, they were there with me. Their help and advice gave me confidence to face any difficulty.

I am also grateful to my colleagues, we have been through hundreds of days, working, studying and discussing together. They selflessly helped me solve many problems. They made the past two years become a wonderful memory.

I appreciate my family for their unconditional love. It is impossible to complete my study without their support. Their understanding is a solid foundation for me to live up to my aspirations.

Acknowledgement

Abstract

Power grid has played a crucial role since its inception in the Industrial Age. It has evolved from a wide network supplying energy for incorporated multiple areas to the largest cyber-physical system. Its security and reliability are crucial to any country's economy and stability [1]. With the emergence of the new technologies and the growing pressure of the global warming, the aging power grid can no longer meet the requirements of the modern industry, which leads to the proposal of 'smart grid'. In smart grid, both electricity and control information communicate in a massively distributed power network. It is essential for smart grid to deliver real-time data by communication network. By using smart meter, AMI can measure energy consumption, monitor loads, collect data and forward information to collectors.

Smart grid is an intelligent network consists of many technologies in not only power but also information, telecommunications and control. The most famous structure of smart grid is the three-layer structure. It divides smart grid into three different layers, each layer has its own duty. All these three layers work together, providing us a smart grid that monitor and optimize the operations of all functional units from power generation to all the end-customers [2].

To enhance the security level of future smart grid, deploying a high secure level data transmission scheme on critical nodes is an effective and practical approach. A critical node is a communication node in a cyber-physical network which can be developed to meet certain requirements. It also has firewalls and capability of intrusion detection, so it is useful for a time-critical network system, in other words, it is suitable for future smart grid.

The deployment of such a scheme can be tricky regarding to different network topologies. A simple and general way is to install it on every node in the network, that is to say all nodes in this network are critical nodes, but this way takes time, energy and money. Obviously, it is not the best way to do so. Thus, we propose a multi-objective evolutionary algorithm for the searching of critical nodes.

A new scheme should be proposed for smart grid. Also, an optimal planning in power grid for embedding large system can effectively ensure every power station and substation to operate safely and detect anomalies in time. Using such a new method is a reliable method to meet increasing security challenges. The evolutionary frame helps in getting optimum without calculating the gradient of the

objective function. In the meanwhile, a means of decomposition is useful for exploring solutions evenly in decision space. Furthermore, constraints handling technologies can place critical nodes on optimal locations so as to enhance system security even with several constraints of limited resources and/or hardware. The high-quality experimental results have validated the efficiency and applicability of the proposed approach. It has good reason to believe that the new algorithm has a promising space over the real-world multi-objective optimization problems extracted from power grid security domain.

In this thesis, a cloud-based information infrastructure is proposed to deal with the big data storage and computation problems for the future smart grid, some challenges and limitations are addressed, and a new secure data management and transmission strategy regarding increasing security challenges of future smart grid are given as well.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

List of Publications

During the whole research period, the candidate was responsible for designing concepts and algorithms, conducting simulations and numerical experiments, and writing up papers and response to reviewers for publications. Several journal papers and conference papers has been accepted, which are listed below.

- *Journal Papers*

  [1] “Cloud-Based Information Infrastructure for Next-Generation Power Grid: Conception, Architecture, and Applications”. Fengji Luo, Junhua Zhao, Zhao Yang Dong, Yingying Chen, Yan Xu, Xin Zhang, Kit Po Wong. Paper has been accepted by the IEEE Transactions on Smart Grid, 2015.

  [2] “Rational and Self-Adaptive Evolutionary Extreme Learning Machine for Electricity Price Forecast”. Chixin Xiao, Zhaoyang Dong, Yan Xu, Ke Meng, Xun Zhou and Xin Zhang. Paper has been accepted by the special issue on Memetic Computing, 2015.

- *Conference Papers*

  [1] “Enabling the Big Data Analysis in the Smart Grid”. Fengji Luo, Zhao Yang Dong, Junhua Zhao, Xin Zhang, Weicong Kong, and Yingying Chen. Paper has been accepted by IEEE Power and Energy Society 2015 General Meeting, 2014.

  [2] “Quantum Cryptography Based Cyber-Physical Security Technology for Smart Grids”. Xin Zhang, Chixin Xiao, Fengji Luo, Zeya Wang, Zhao Yang Dong, Paper has been accepted by APSCOM 2015, 2015.

List of Figures

Chapter 1. The Era of Big Data

I. INTRODUCTION

Since its proposal in the early 21th century, the smart grid has been undergoing a rapid development [3]. With the integration of various advanced technologies, a smart grid has become the complicated system covering multiple domains. Benefit from the wide area sensor infrastructure, the smart grid will continuously generate the unprecedented data volume, which could be used to support the decision making of the utilities and optimize the grid operation. The big data generated can be from different data sources, such as the advanced measurement infrastructure (AMI), the scattered distributed generators, the widely deployed phase measurement units (PMUs), etc. For example, in the smart grid, a PMU can generate 50 or 60 phase measurements per second [4].

One significant challenge faced by a smart grid is how to collect, manage, and analyze the big data in an efficient, reliable and secure manner. The challenges exist in each segment of the data flow: data transferring, data storage, and data analysis. Some basic requirements of the big data analysis of the smart grid can be drawn as below.

A. Data Transferring and Sharing

In a smart grid, data is transferred and shared among multiple parties at different levels. In the lower level, the big data generated by the sensor infrastructure is transferred to the cyber resources (such as the database, data warehouse, etc.). In the higher level, different parties share the critical private data to collaboratively achieve a specific objective. In either level, ensuring the data security would be the primary objective of the communication. Here the data security refers to two-fold meanings. The first one is the confidentiality of the data, meaning that the data cannot be disclosed to the external environment during the communication; the second one is the data integrity and consistency, which means the data cannot be falsified by the irrelevant parties. The unsecure data communication may lead to serious consequences. For example, a cyber-attacker may inject the falsified data to distort the grid state estimation process and lead to improper control actions [5]. Or a generation company may lose its profit by disclosing his confidential bidding information to the other parties.

B. Data Storage and Management

The vast amounts of the data generated in the smart grid impose new challenges to the data storage and management infrastructure. In the smart grid, the big data is from wide area data sources, with high dimension, unstructured organizations and noises, and often generated on the real-time basis. These characteristics makes the big data in the smart grid can hardly be effectively stored by the traditional database management systems.

Firstly, since the sensors are distributed deployed, it is un-practical to store the big data in a centralized manner. It would be more practical to design and develop a distributed data storage network to provide the platform-level support for the big data in the smart grid. The data storage platform also should be robust enough to resist the cyber-attacks.

Secondly, the wide area data generated in the smart grid will be accessed by different parties to do the specific tasks, ranging from the local scheduling to wide area control. Therefore, how to effectively route the data packages among the under-lying distributed storage nodes to the query points would be a challenge. A certain data routing algorithm would be developed to optimize the performance of the whole distributed data storage network.

Thirdly, the challenges not only arise in the data storing and routing, but also in data querying and retrieving. Due to the fast changing environment of the smart grid, the big data generated in the smart grid are often with noises and uncertainties. When respond to the queries from the users, the data management system should be smart enough to take the uncertainty nature of the data into account, which means the traditional precise data querying techniques might not be adapted to this new environment.

C. Data Analysis and Mining

Generally, it is meaningless to just aggregate and store the big data. The different parties in the smart grid need to gain the knowledge from the data to make decisions. In despite of the wide study of applying data mining techniques on power systems, new challenges arise under the new context of big data. In the traditional data mining techniques, the training data is often assumed to be precise. However, similar with the uncertain data querying issue, the inherent uncertainties of the big data needs to be considered in the data mining process.

In the literature, there are just a few papers focusing on designing the architecture of the information infrastructure to support big data management in the smart grid. [6] proposed a cloud computing based information infrastructure for the future power grid; [7] proposed a cloud-based bargaining model for the demand response to enhance the security and robustness of the communication process between the load aggregators and the utility; [8] proposed a data-centric information platform to manage the information flow in the smart grid in a secure manner. The new challenges discussed above require the integration of new technologies into the smart grid operation and development of the new applications.

II. EMERGING TECHNOLOGIES

In recent years, there have been some significantly new technologies emerged, which can be employed in the different aspects of the big data analysis in the smart grid. In this section, we will give a brief review of these technologies.

A. Cloud Computing

Cloud computing [9] [10] is a new computing mode whose core component is the data center. In cloud computing, the multiple data centers are often constructed and each one consists of a large number of servers to facilitate the high performance processing. Unlike traditionally distributed computing, cloud computing uses the hardware virtualization technology to generate virtual machines based on the underlying physical servers. The life cycles of the virtual machines and the map-ping of the virtual machines to the physical servers are often managed by the firmware, and the upper-level applications run on the virtual machines. In this way, cloud computing has strong scalability and can deliver the virtual resources to the users on demand.

According to the level of the abstraction, the services pro-vided by the cloud computing are often classified as: 1) infra-structure as a service (IaaS), where the virtual resources are directly delivered to the users; 2) platform as a service (PaaS), where users develop applications directly through the programming and development environment provided by the cloud side; 3) software as a service (SaaS), where the software is directly published in the cloud side through the web service interface, and the users access the software through the web portals.

B. Secure Multi-Parties Computation

In the practical world, the collaboration of multiple parties often involves the exchange and sharing of data to enable joint decision making. There are thus strong motivations for the multiple parties to keep the confidentiality of their sensitive data. Secure Multi-parties Computation (SMC) [11] [12] is a technique which addresses the data security issue in the collaboration. That is, is it possible to perform the collaborative computations directly on the encrypted data without decrypting it?

SMC itself is not new. The study of the SMC can be traced back to the 1980s. In recent years, the widely deployment of the Web and cloud computing make the electronica collaboration more convenient and efficient. This gives the SMC technique a more important role. SMC is based on a data encryption technique called the homomorphic encryption. The homomorphic encryption technique allows the encrypted data to be processed by certain operators (additions, multiplications, etc.), and the results are the same with that of processing the plain data. Based on this, the basic idea of the SMC is that given a computation function, a set of specific protocols can be designed between the collaborators to enable them to only share data encrypted with homomorphic encryption and use the encrypted data to do the computation so that each party can only decode the computation result, rather than others' contributed data.

In despite of its attractive security features, SMC have not been widely used in the industry due to two reasons: one is that the SMC solution is not generic for a variety of computations, and another is that the SMC would be computational intensive when the number of collaborators increases. How-ever, with the recent advances of the high performance computing (e.g., cloud computing), the barriers between the SMC and the industrial applications can be expected to be re-moved.

C. MapReduce Parallel Processing Framework

MapReduce [13] is a programming model to parallel process parallelizable problems across huge datasets using a large number of computing nodes. In recent years, MapReduce has been applied widely on many cloud computing platforms to do the large scale big data analysis. There are three major steps in the MapReduce model:

a) "Map" step. In this step, each worker node invokes the "map()" function to the local data, and sends the output to a temporary storage;

b) “Shuffle” step. Each worker nodes redistributes data ac-cording to the output keys generated by the “map” function, so that all data belonging to one key is located on the same worker node;

c) “Reduce” step. The worker nodes process each group of the output data, per key, in parallel.

In the MapReduce framework, the “map’ step can be highly paralleled. Assuming each mapping operation is independent of the others, all map operations can be performed in parallel. The MapReduce framework is also fault-tolerant. If there are partial failures of servers or storage devices during the computation, the work load can be rescheduled.

D. Data-Centric Data Storing and Routing Technology

The vast amount of data generated by the wide area sensor networks require scalable, self-organizing and efficient data dissemination and routing algorithms. Instead of the common host-to-host communication pattern, in the last decades the data-centric data storing and routing technology [14] [15] has been developed. This technology is based on a simple observation: the content of the data is more important than the identity of the node that gathers them.

In the data-centric data storing and routing technology, the identity of the data storage node is less relevant, and the data are named and routed referring to these names rather than the storage node addresses. Users can define certain conditions to query the data. Certain name-based data routing algorithms are often adopted (such as the Greedy Perimeter Stateless Routing (GPST) algorithm [15]). In these algorithms, a data object is associated with a key and each data storage node stores a certain range of keys. These algorithms allow any node in the system to locate the data storage node for an arbitrary key. Nodes can put and get files based on their keys, thereby supporting a hash-table-like interface.

E. Stream Computing

As a new computational paradigm, stream computing has the capability to process the unbounded data streams in a real-time and reliable manner. Stream computing provides a computing framework to effectively capture and process the data streams. Currently, there are some widely used streams computing platforms, such as S4 [16], Storm [17], Stream-Base [18], etc.

Here we use the Storm system to explain the basic mechanism of the stream computing. There are 4 kinds of key abstractions in Storm:

a) Tuple. A tuple is a named list of values where each one can be any type (string, integer, decimal value, etc.);

b) Spout. A spout is a logical computing node representing the source of the data stream. Spout will read the tuples from an external source and emit them into the topology;

c) Bolt. A bolt is a logical computing node which process the input streams and generate the output streams;

d) Topology. Topology is a network of spouts and bolts which represent the overall computation. A topology can be modelled as a directed acyclic graph composed of a series of Bolt and Spout nodes.

The organization of the Storm components can be depicted in Figure 1-1.

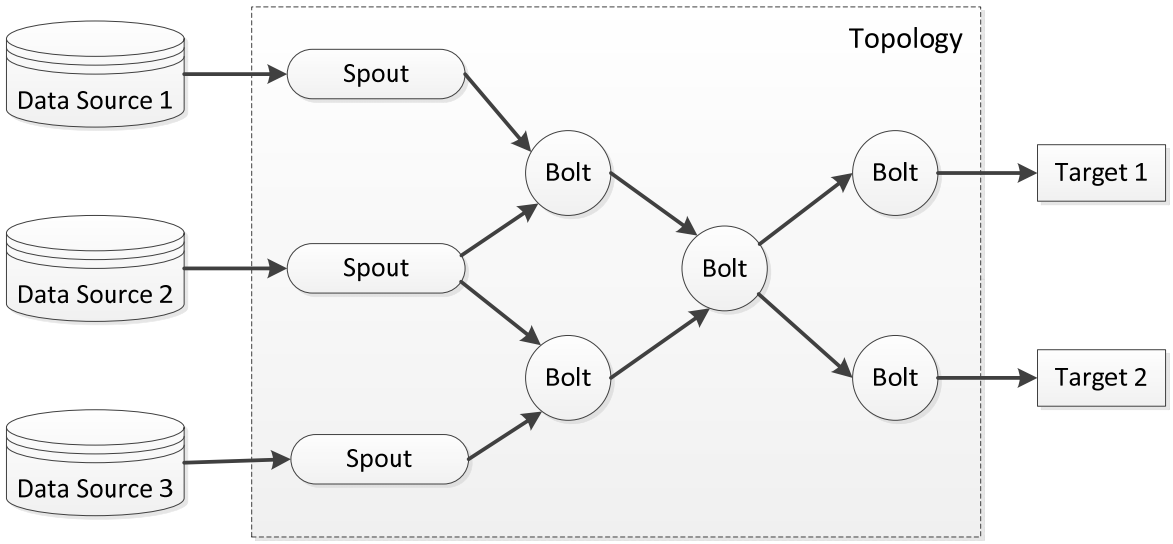

Figure 1-1. Architecture of the Storm [81]

F. Imprecise Data Querying

In the traditional data querying techniques, the database management system (DBMS) returns the precise results ac-cording to the query conditions. In recent years, a series of querying and indexing techniques are developed to take into account the uncertainty of the data [19] [20]. Instead of generating the precise response, these techniques evaluate data uncertainties and provide probabilistic guarantees. For example, [19] modelled the uncertainty of the data as the stochastic value within a

certain bounds, and classified the data queries as different classes. It then developed different algorithms to compute the probabilistic answers.

G. Uncertain Data Mining

In the traditional data mining techniques, the data samples are often assumed to be precise or with definite values. How-ever, in the latest years, there has been some research works conducted to capture the uncertain features of the data, which is common in the big data applications [21] [22] [23]. These techniques often assume a probabilistic distribution for the values of the data, and then generate the probabilistic data mining results. For example, [21] extended the K-means clustering algorithm to be the UK-means clustering algorithm by specifying a data object by an uncertainty region with an uncertainty probabilistic distribution function. In the UK-means clustering algorithm, the expected sum of squired errors of a data object and the clusters are minimized. In [22], a decision tree classifier for uncertain data is developed and the related pruning algorithms are proposed.

III. POTENTIAL APPLICATION SCENARIOS

In this section, we briefly identify some potential smart grid application scenarios which are related to the big data analysis. Obviously, the possible big data applications are not restricted to the ones discussed.

A. Uncertain Data Mining

Up to now, there are just a few papers in the uncertain data mining, and it is still a relatively new research direction. A common feature of the existing methods in the literature [21] [22] [23] is that they assume the possible values of the uncertain data follow a certain pdf. And the normal distribution is often used to represent the worst scenario where the actual pdf is not known. However, this assumption cannot be always true in many practical applications. Therefore, a possible re-search direction in the uncertain data mining is to develop a robust technique to relax this assumption to make it more practical.

The research in uncertain data mining can be considered more like a fundamental research than a smart grid application. However, it makes significant role in big data environment can effectively support many smart grid application where the underlying data is uncertain in nature.

B. Non-Intrusive Load Monitoring

With the deployment of the AMI, data of load consumption at the end user level can be a huge mine for load model-ling. Such models at granular level would be beneficial to en-courage interactions between the utility and electricity customers. Non-Intrusive Load Monitoring (NILM) is one of the applications to make use of smart meter data for big data analysis and enhance load modelling in future grid.

The concept of NILM is to disaggregate the total power consumption into combination of power consumption at appliance level based on some extent of prior knowledge of electric devices which may be included. The prior knowledge of electric devices is analyzed to form the signatures for individual devices. Typical inherent signatures for devices usually include active and reactive power range, harmonic content range, V-I trajectory, and start-up spike [24]. Some research also considered external signatures such as time of use of a day, average duration and times of operation per day [25].

Combining affluent signature database and smart meter data, customer behavior, composition of power consumption, more accurate user load model and better load forecasting can be analyzed through NILM. Such information is useful to further facilitate renewable generation penetration and enhance general efficiency of future smart grid.

C. Real-Time System Peak Load Tracking

A typical smart grid application of the real-time data flow processing is the real-time system peak load tracking. With the fine-gained data collection of the SCADA (supervisory control and data acquisition) system and the widely deployment of the AMI, the volume of the real-time data generated is huge. The current data collection rate of the SCADA system and AMI are every 3-5 seconds and every 15 minutes, leading to the gigabyte-level cached data for a regional distribution net-work. In this context, the system operator needs to analyze the data to track the system peak load and take appropriate control actions.

The real-time processing of such vast amounts of data can be a big challenge of the traditional computing modes. With the stream computing technology, the effectively real-time system peak load tracking can be achieved. Taking the Storm architecture as an example, by properly designing the data flow processing topology, the real-time data generated by the wide area sensors can be collected by the

distributed spouts. The data flow then can be sent to the other bolts to do step-by-step further analysis, and the extracted load information can be finally sent to the utility side to support the decision making.

D. Demand Response

There are two common approaches to do the demand side management: demand response (DR) and direct load control (DLC). In DR, the end users actively adjust their energy usage patterns to respond to the incentive schemes provided by the utility. The incentive policy making of the utility is thus crucial to the optimal operation of the DR programs. For example, the most straightforward policy might be the time-of-use pricing system. A more sophisticated strategy could be that the utility publishes various energy usage discount packages, and the users purchase different packages based on their own situation [26]. However, these strategies are relatively coarse-grained due to the lack of analysis for the user's energy usage patterns.

In the big data context, more sophisticated energy retailing policies can be made based on analyzing the energy usage data of the users. The cloud computing platform and the da-ta-centric data storage technology could be utilized to aggregate the energy usage data of the users, which could be generated by the AMI or the NILM techniques. The uncertain data mining techniques could be then employed in the utility side to extract the users' energy usage characteristics and patterns. Then the utility can design highly customized incentive schemes which mostly fit the individual users. In this way, both of the profits of the utility and the electricity costs of the end users can be optimized.

In the practical deployment, the mining process of the end users' energy usage data can be deployed in the cloud plat-forms, and the MapReduce framework can be employed to improve the mining performance.

E. Direct Load Control

In addition to the DR, another effective demand side management approach is the DLC, where the utility directly dispatches and controls the ON/OFF actions of the loads. The DLC is often subjected to a specific object (e.g. system peak load reduction) while minimizing the interruption of the users. In the existing methods, the DLC is completely based on the approximately dynamic models of the appliances [27] (air conditioner, water heater, etc.). In the big data context, with the availability of the users' energy usage data of the users, the users' energy usage characteristics can be taken into ac-count when designing the DLC strategies. For instance, the utility can discovery the appliance usage

preferences of the users from the data, and then design more effective DLC strategies to minimize the discomfort of the users.

F. Electric Vehicle Charging System Planning and Electric Vehicle Real-Time Dispatch

The large scale plug-in electric vehicles (EVs) will significantly affect the power grid operation. The layout of the EV charging infrastructure and the driving routes of the EVs will alter the power flow distribution, and further affect the power loss and voltage distribution of the distribution system. The big data analytics would be meaningful in both of the EV charging system expansion planning and the EV real-time dispatch.

In the EV charging system expansion planning, the large scale historical route records of the EVs can be aggregated, and the utility can discover the EV driving route clusters from it, which can be used to determine the charging system expansion plans. For example, the utility might choose to construct more charging stations in the areas to which the EVs intensively drive.

In the EV real-time dispatch, the driving routes of the EVs could be able to be guided through some devices (such as GPS), by considering both of the traffic and distribution network conditions. The route guidance of the EVs involves the querying of the real-time EV positions through the wireless sensor networks, which can be classified as an imprecise data querying problem in a moving object environment. Therefore, the imprecise data querying introduced in the Section II can be employed in the process of the EV route guidance.

G. Secure Collaboration Framework for Smart Grid Applications

In the smart grid, there are many application scenarios where different parties will work together to achieve certain objectives. In such applications, the SMC technology introduced in the Section II can be employed to form the secure collaboration frameworks. For example, in the application described in [28], multiple virtual power plants (VPPs) cooperatively sell energy to the grid. The cooperation process involves the sharing of the capacity and bid information of the VPPs, which can be considered as the sensitively private data. By using the SMC, the cooperative calculations can be performed on the encrypted data, and thus can better protect the privacy of the VPPs.

Another application scenario could be the DLC process, where the utility negotiates the load shedding prices with the load aggregators. Here the sensitive data, such as the price and the load

capacity, also needs to be exchanged through the communication channels. Again, the SMC can enhance the cyber-security of the DLC process.

IV. SUMMARY

This chapter discusses the feasibility of enabling big data analysis in the smart grid context. Firstly the importance of the big data analysis in smart grid by extracting some fundamental data requirements in the future grid is emphasized. Then, a brief overview for some new technologies emerged in the recent years is given. These technologies can be used as the 'bricks' to develop the big data applications in the smart grid. Lastly, this chapter identifies some potential big data application scenarios in the smart grid.

The next chapter will give a data based cloud computing framework for the big data challenges we are facing nowadays in a smart grid.

Chapter 2. Data Based Cloud Computing Framework

I. INTRODUCTION

Driven by the new emerging technologies and the increasing pressure of the global warming, the conception of 'smart grid' is proposed in the last a few years [29-31]. According to the definitions given by the National Energy Technology Laboratory (NETL) of the U.S [29], smart grid should have the features of self-healing, attack-tolerance, running more efficiently, motivating demand side management, high penetration of the renewable energy, etc. These features make the future grid to be a complex cyber-physical system and impose some significant requirements on the information infrastructure of the next-generation power grid, including: fast reaction to disturbances and faults, wide area data management, high performance computing and real-time analysis, data security, etc.

A. Limitations of Current Information Infrastructure

Currently, the information structure of the grid adopts the centralized structure, where the control entities of a utility are directly connected to the energy management system (EMS) and the EMS acts as the main control center. The control activities are also performed in a centralized manner. The Remote Terminal Unit (RTU) of each substation interacts with the EMS to report the state information of the underlying power devices.

This centralized information infrastructure cannot satisfy the information requirements of the future grid. The first limitation is that the control center can hardly manage the mass data generated by future grid due to its storage bottleneck. For instance, in the future grid a PMU generates 50 or 60 phasor measurements per second [32]. Such big data cannot be fully transmitted to the control center due to the bandwidth limit. It can be expected that even a small number of PMU will generate a large amount of data and reach the bandwidth bottleneck. Even the bandwidth can be upgraded to serve the peak-rate data transmission (obviously this is not a cost efficient solution), the storage capacity limitation of the control center restricts the storing of the big data centrally. Therefore, to effectively aggregate the wide area distributed data, a decentralized, platform-centric infrastructure is desired.

With the exploration of the big data, the computing power consumption of the future grid will become a big challenge for the centralized information infrastructure. In order to be self-healing and fast react to online disturbances, the control center needs to process the big data quickly. Also, many online/offline applications will run on the servers simultaneously, which imposes heavy load for the computational resources of the control center. A new platform-centric information infrastructure is thus needed to deliver scalable and reliable computational powers to the future grid.

Today's centralized structure is also vulnerable to the cyber-attacks. For example, one attacker may attack the transmission channel between the EMS and the control entity by injecting a large number of malicious data packages to make the congestion. Since the current information infrastructure is a star network, the significant data transmission delay is unavoidable under this attack. Or the attackers may impose distributed denial of service (DDoS) attacks to breakdown the control center server. To ensure the reliable and secure operation of future's grid, a robust information infrastructure is needed.

B. Related Works and the Scope

There have been a few initial works discussing the vision of applying cloud computing on future power grid. Authors in [6] presented a prototype of hybrid cloud computing platform for smart grid and discussed some potential cloud-based smart grid applications; the authors in [33] gave a conceptual design of the power cloud data center to deliver multi-layer services to smart grid; Authors in [34] discussed how smart grid applications can benefit from cloud computing framework, and described a cloud computing platform for SCADA (supervisory control and data acquisition) data monitoring application; Authors of [35] proposed a coordination dispatch algorithm for cloud computing and smart power grids. The power flow constraints are incorporated into the cloud datacenter dispatch algorithm, so that the impact of the dispatch of computational resources on power grid is considered; [36] analyzed the limitation of the data management infrastructure of the current grid, and then proposed a cloud framework for smart grid data management; authors of [37] established a cloud-based demand response application for smart grid, where the utility negotiated load shedding price with the large number of energy consumers.

Most of above works only described general models of the cloud platform for power grid, and summarize some conceptual applications. The major contributions of this chapter are 2 folds:

a) An explicitly layered model of the cloud computing based information infrastructure for the next generation power grid is proposed in this Chapter. Just as the well-known layered model of the TCP/IP protocol, the layered cloud-based information infrastructure model explicitly decouples different cyber-physical entities and identifies their roles; and

b) How power applications can benefit from the cloud-based information infrastructure are discussed, and three specific cloud-enabled power applications are developed. The first two aim to demonstrate how to develop compute-intensive and data-intensive power applications on the state-of-the-art public cloud platform while the third one develops a cloud-based collaborative DLC architecture based on the proposed layered model.

II. LAYERED MODEL of the CLOUD-BASED INFORMATION INFRASTRACUTRE

A. Basic Conception of Cloud Computing

According to the definition of Foster [38], cloud computing is a large scale distributed computing mode which can form a virtualized, dynamically scalable resource pool to deliver services to users on demand through the Internet. As a new computing mode, cloud computing is an integration of multiple major technologies (shown in Figure 2-1), including grid computing, hardware virtualization, utility computing, web service, automation computing, etc. The more details of cloud computing can be referred to [39].

Supported by these core technologies, cloud computing can deliver different level of services to users.

(1) Infrastructure as a Service (*IaaS*): *IaaS* offers virtualized resources to users in an on demand manner. Users can access and use the virtualized resources directly on demand;

(2) Platform as a Service (*PaaS*): *PaaS* offers a programmable environment where developers can construct applications directly on the cloud side; and

(3) Software as a Service (*SaaS*): The complete developed software is delivered to users through cloud portals. *SaaS* makes users shift from locally installed computer programs to on-line software services that offer the same functionality.

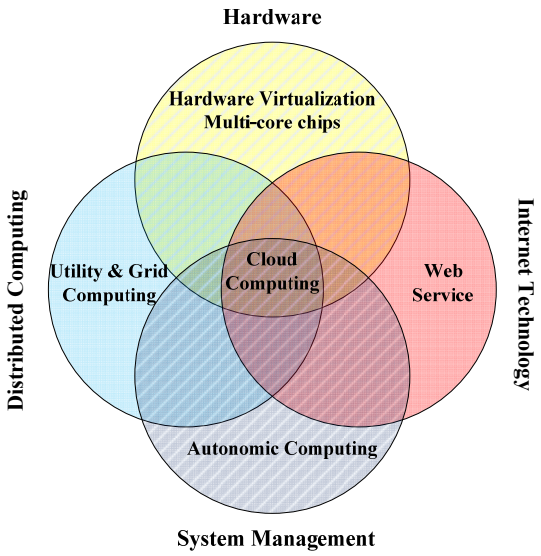

Figure 2-1. Core technologies of cloud computing [39]

B. Layered Information Infrastructure Model

In the future grid, the information flow and decision making process can be supported by the cloud-based information infrastructure, in all of the generation, transmission and distribution sides [33] [36]. The proposed layered model for the information infrastructure of the future grid is shown in Figure 2-2.

A well-designed layered model often decouples the dependencies of different elements and defines role boundaries of each layer. A well-known example is the layered OSI model of the TCP/IP protocol [40]. In our model, each layer relies on underlying layers and only communicates with its neighbored layers.

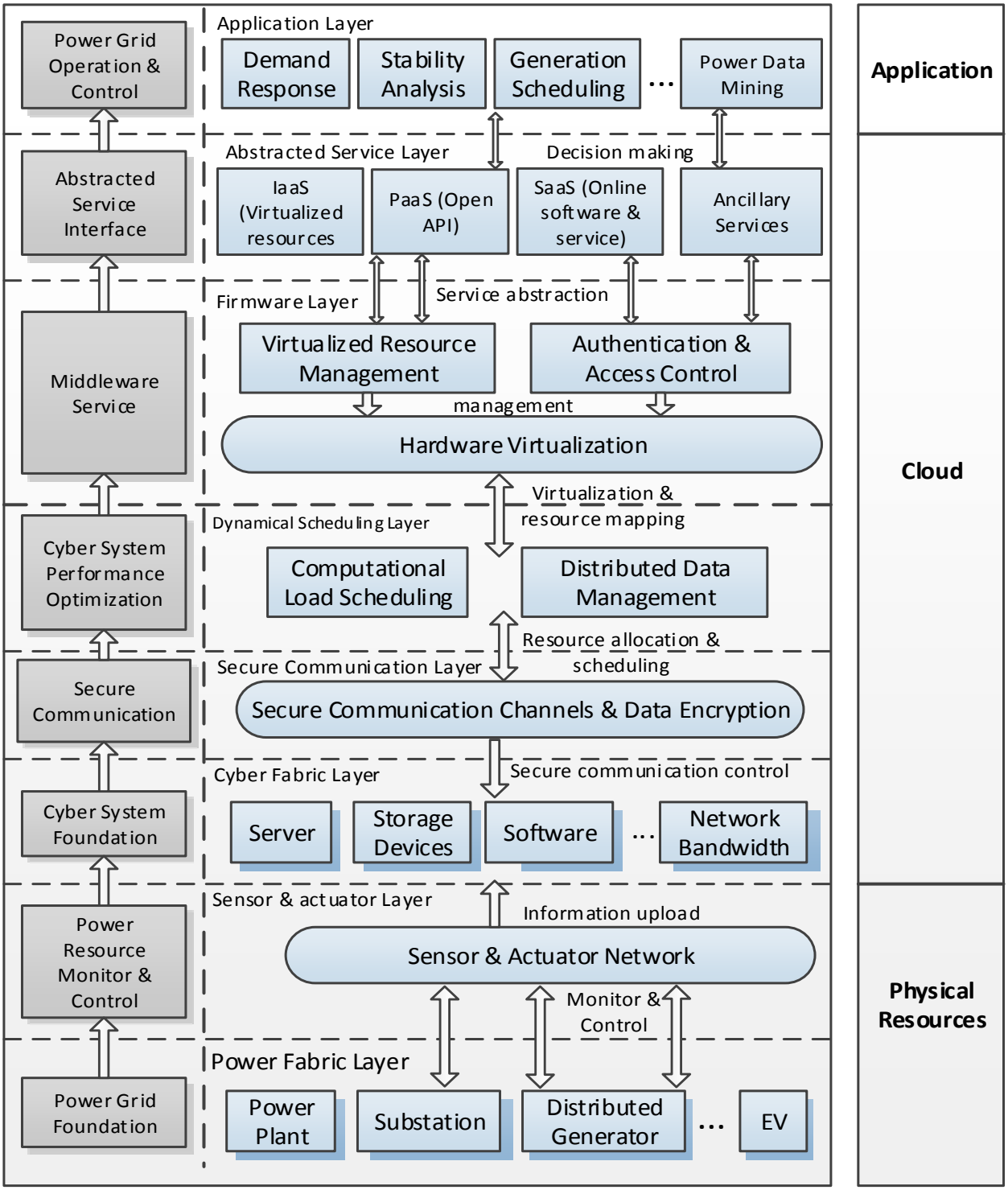

Figure 2-2. Layered model of the cloud-based information infrastructure [174]

1). Power Fabric Layer

The *Power Fabric Layer* includes the wide-area physical resources of the power grid. Those resources are involved in the generation side (power plants, wind turbines, etc.), transmission side (transmission lines, transformer, etc.), distribution side (substations, feeders, EVs, etc.), and other control elements. This layer forms the foundation of the power grid.

2). Sensor and Actuator Network Layer

The *Sensor Network Layer* monitors the state of the power resources and collects the raw data. The elements of this layer may include SCADA system, phase measurement unit (PMU), smart meters, etc. In addition to the hardware sensors, the software & services which generate data for some specific objectives are also classified into the sensor network (e.g. the wind speed forecasting system).

3). Cyber Fabric Layer

This layer consists of the cyber resources, including computational resources (servers, workstations, PC clusters, etc.), storage resources (disks, database, data warehouse, etc.), software systems, communication network infrastructure, etc. Here the cyber resources may be invested and owned by different parties, such as the public cloud service providers.

4). Secure Communication Layer

This layer encrypts and authenticates the data to ensure it cannot be read or interfered during communication. Different secure communication technologies can be applied in this layer. For example, the data encryption can be implemented by establishing the *secure channels*, where each channel is secured by the *session key*. The communication parties assign the key to the *secure channel* through the *key exchange* (KE) procedure [41]. For establishing the *secure channels*, the *public key infrastructure* (PKI) can be used.

5). Dynamical Scheduling Layer

This layer implements the dynamical scheduling algorithms for the cyber system performance optimization. Computational tasks are scheduled among different computational resources to achieve high performance computing efficiency and optimize the computational load balance of the computational resources. Critical & large volume data of the power grid are storage & cached distributed.

6). Firmware Layer

Firmware Layer performs the hardware virtualization for the cyber resources. It dynamically generates the virtualized machines with different scale and configurations. It also maintains the life cycles of the virtualized machines and does low-level scheduling tasks, such as mitigating the operation environment from one server to another when physical fault happens. The *Firmware Layer* also provides authenticate & access control services to ensure the secure access of the virtualized machines.

7). Abstracted Service Layer

This layer provides various power grid-oriented services in different cloud service layers (*IaaS*, *PaaS*, and *SaaS*). In the *IaaS*, it delivers the virtualized machines on demand to power grid participants; the *PaaS* provides open API to power grid participants to develop different applications; the *SaaS* provides online services such as data analytics, stability analysis, system modeling, etc., to support decision making of power grid participants.

8). Power Application Layer

Based on the web service interfaces of the cloud-based information infrastructure, power grid participants can develop various applications, ranging from local to wide-area operation and control.

C. Merits of the Cloud-based Information Infrastructure

Based on the aforementioned architecture, we summarize some merits of the cloud-based information infrastructure for the power grid, which are significantly different with the current centralized information infrastructure.

1). Scalable and Elastic Virtualized Resource Provision

By utilizing the hardware virtualization technology, the *Firmware Layer* can create virtualized resource instances on top of the hardware resources. Each virtual machine can run its own operation system and software stacks. Backed by the massively powerful physical resources in the *Cyber Fabric layer*, the *Firmware Layer* can provide nearly unlimited capacities of virtualized resources to the power users, and it can dynamically scale the resource provision according to the different power applications requirement.

2). Distributed Power Data Management

In the cloud-based information infrastructure, the *Dynamical Scheduling Layer* will aggregate and manage the wide area power data. The advanced data dissemination, routing and replication methods implemented in this layer can support the fast data transferring and retrieving by the power

control centers and other different smart grid participants, and optimize the performance of the whole underlying data storage network. The higher-level data management services and data analytical tools implemented in the *Web Service Layer* can let the power users effectively manage and analyze the underlying large scale data to optimize the operation of the grid.

3). Scalable High Performance Computing

The elastic computational resource provision feature of the cloud-based information infrastructure enables the high performance processing for different scale of the power applications. Such powerful computing capacities can hardly be achieved by the centralized computing mode. Also, the fast parallel processing capability of the cloud infrastructure can effectively support the power users to do the real-time analysis and make online decisions.

4). Security and Fault-Tolerance

Compared with the centralized structure, the cloud-based information infrastructure is more robust and fault-tolerant. The *Secure Communication Layer* can enhance the data security and integrity of the communications. The authentication and access control services in the *Firmware Layer* and the secure computing services in the *Web Service Layer* can ensure the confidentiality of the users. And many cyber-attack defending techniques for the specific power applications can be implemented in the Abstracted Service Layer and the Power Application Layer to enhance the cyber security of the grid.

The hardware virtualization technology in the *Firmware Layer* can significantly improve the fault-tolerance of the system. Given there is any hardware failure occurs, the virtualized resource management schemes in the *Firmware Layer* can mitigate the virtualized resources images to other hardware to avoid the single point breakdown. Also, the data & task scheduling mechanisms in the *Dynamical Scheduling Layer* will enhance the robustness of the whole system.

5). Cost Reduction

In the cloud-based information infrastructure, the cyber hardware is maintained in the cloud side, and the services are delivered to the users in the on-demand manner. By mitigating the applications to the cloud side, the power users only need to pay-on-demand and thus can largely reduce the local investment & operation costs on the hardware and software. This will also encourage the information sharing & application integrity of different power entities, and promote the economical operation of the grid.

6). Access the Cloud at Any time & Any where

Since the communication media of the cloud computing is the Internet, the power users can access the cloud through the web service interface as they want, by using various lightweight media (PAD, smart phone, etc.)

D. Implementation Technologies

After introducing the architecture of the cloud-based information infrastructure, in this section we will give some overview discussions about the implementation technologies of the different layers of the infrastructure. The technologies discussed in this sections can be used as 'bricks' to construct the cloud-based information infrastructure. It also should be mentioned that the technologies introduced below are just some representative technologies summarized by us. More technologies can be found in both of the industry and academic circle. And since each layer in our layered model represents an open research area, more useful tools can be developed in future.

In the *Secure Communication Layer*, the RSA public-key based encryption method [42] has been widely applied in most of Internet-based communications. The theoretical foundation of the RSA is the decomposition of large prime number, which can therefore fundamentally resist the eavesdropping of the cyber-attackers. In addition to RSA, there are also some other data encryption technologies which is promising to be widely deployed in the foreseeable future. One significant technology is the quantum cryptography technology [43], whose theoretical foundation is the quantum mechanics. Instead of transmitting bits, in quantum cryptography the data is encoded as qubits. Qubits are polarized by different directions. The quantum key distribution starts by sending a large number of qubits from the sender to receiver. If a eavesdropper wants to get the information of any qubit, he or she will have to measure it. Since the eavesdropper knows nothing about the qubit's polarization, he or she can only measure it by guess, and then send another randomly polarized qubit to the receiver. But all these operations will be discovered at the end of quantum key distribution. After a brief communication, the key will be identified to be safe or not.

In the *Dynamical Scheduling Layer*, there are several technologies can be applied in the computational load scheduling. For example, Cloud Scheduler [44] is a commercial software system for scheduling the tasks among the cloud resources. Many researchers also proposed some computational load scheduling strategies. [45] proposed a task scheduling scheme to schedule the task groups in cloud computing platform, where resources have different resource costs and computation performance. [46]

proposed the cost and time models for the computational tasks in the cloud computing environment, and studied an optimal task scheduling model. Some other works can be referred to [47-50]. There are also some technologies for the distributed data management in the cloud environment. Brocade Vyatta Virtual Router [51] delivers advanced routing for the data packages in physical, virtual, and cloud networking environments. It includes dynamic routing, policy-based routing, etc. in a platform that is optimized for virtualized environments. The HP VSR 1000 router series [52] is a virtualized application that provides functionality similar to a physical router. It enables significant operational savings as a result of its agility and ease of deployment. Spanner [53] is a data synchronous replication system adopted by Google's cloud infrastructure, which stores data in multiple data centres to avoid the data lost in case of the hardware disaster. [54] proposed a cost-effective dynamic data replication scheme. By adjusting replica number and location according to workload changing and node capacity, this scheme can dynamically redistribute workloads among data nodes in the heterogeneous cloud. [55] proposed a dynamic data replication strategy to improve the data availability in the cloud computing environment. Another promising technology is the data-centric data dissemination and routing technology [56], [57].This technology is based on a simple observation: the content of the data is more important than the identity of the node that gathers them. In the data-centric data dissemination and routing technology, the identity of the data storage node is less relevant, and the data are named and routed referring to these names rather than the storage node addresses. Users can define certain conditions to query the data. Certain name-based data routing algorithms are often adopted.

In the *Firmware Layer*, some mature industrial products can be applied to perform the virtual resource management. For example, the Dell virtualization management solutions [58] can provide a series of services to users, including performance and availability monitoring, capacity planning for the resources, etc. Right Scale [59] is a platform for managing and deploying cloud resources across public and private environments, providing users the tools to configure, monitor, automate deployments, and govern controls and access. VMWare Workstation [60] provides a suite of software solutions for creating and managing the virtualized resources and construct the cloud data centers.

In the *Abstracted Service Layer*, many sophisticated services can be developed. There have been many industrial products which can be deployed in this level. These products provide higher-level services in many aspects. As a *SaaS*-level product, Google Cloud SQL [61] runs on the Google cloud data center. It allows users to perform higher-level data management in the cloud. Amazon Elastic Compute Cloud (Amazon EC2) [62] provides the *IaaS*-level services by delivering the virtualized server instances

directly to the users; CloudFuzion [63] provides the PaaS-level services on which the users can develop and fast solve different engineer problems. It also provides a suite of power grid application solutions. MapReduce [64] is a parallel data processing framework which have been widely used in the cloud platforms. It can parallel process parallelizable problems across huge datasets using a large number of computing nodes. A famous software implementation of the MapReduce framework is the Apache Hadoop [65]. CloudBroker [66] is a software which provide higher-level task scheduling services among the resources belonged to different cloud providers. Some other products (such as Cloudyn [67], Cloud Cruiser [68], etc.) can provide some ancillary services such as cost tracking, resource monitoring, task tracking, etc.

Supported by the powerful cloud virtualized resources, some other promising technologies can also applied in the *abstracted service layer*. For example, stream computing is a software framework designed to support the fast real-time stream data processing. It can be seamlessly deployed on the cloud resources to do the fast data flow process. The widely used stream computing software include Storm [69], S4 [70], and StreamBase [71]. The Secure Multi-parties Computation (SMC) [72] is another technology which is promising to be widely applied to enhance the data security in the cloud environment. SMC addresses the data security issue in the collaboration. SMC makes it possible to perform the collaborative computations directly on the encrypted data without decrypting it. The theoretic foundation of SMC a data encryption technique called the homomorphic encryption [73]. The homomorphic encryption technique allows the encrypted data to be processed by certain operators (additions, multiplications, etc.), and the results are the same with that of processing the plain data. Based on this, the basic idea of the SMC is that given a computation function, a set of specific protocols can be designed between the collaborators to enable them to only share data encrypted with homomorphic encryption and use the encrypted data to do the computation so that each party can only decode the computation result, rather than others' contributed data.

III. APPLICATIONS

This section discusses how different power applications can benefit from the cloud-based information infrastructure. Firstly, we identify 4 categories of the power applications, and discuss how they can be effectively solved by cloud computing. Followed by this, we give 3 specific technical applications for the demonstration purpose. The first two demonstrate how to build compute-intensive and data-intensive power applications by utilizing the practical cloud platforms, respectively; in the third

one, we develop a cloud-based architecture for a collaborative smart grid application to show how smart grid applications can benefit from the proposed layered model.

A. Enabling Power Applications by the Cloud-based Information Infrastructure

Relying on the powerful computing capability and layered functional services, the cloud-based information infrastructure can be adapted to various kinds of power applications. In this section, we summarize the power application as 4 categories, and each of which covers some common computational features.

1). Compute-Intensive Power Applications

The compute-intensive power applications represent the power applications which needs a lot of computations. This category of power applications is very common in modern power system analysis. For example, a complex large-scale transmission network planning problem often requires a long-time optimization process (several hours to even several weeks) [74]. Another example could be the system stability analysis, where the '*N-1*' or even '*N-2*' fault analysis [75] are often performed to study the post-fault stability of the grid. For a large system, this will lead to a huge number of fault scenarios. Other compute-intensive power applications include voltage stability analysis [76], unit commitment [77], distribution network optimization [78], etc.

In order to get the compromise between the accuracy of the analysis result and the computation time, the power engineers often need to do some numerical approximations and relax the complexity of the analysis method (e.g. reduce the iteration number of the optimization method, reduce the number of the analysis scenario, etc.). In many cases, such compromise will affect the achievement of the optimal solution.

In order to accelerate the compute-intensive applications without significantly sacrificing the analysis result accuracy, the HPC resources are also applied, such as the multi-core server or multi-node cluster [79], [80]. There are some limitations for these traditional HPC approaches:

(1) The software configuration and hardware maintenance of those HPC resources are often time-consuming and need the expert knowledge;

(2) The investment & maintenance costs of those HPC resources are often very large, which makes them hardly accessible or affordable for small-scale research & industrial organizations, specialized applications purposes or short-term projects;

(3) There lacks of the standard open API for those local HPC resources, which makes them hardly to integrate with existing systems and processes;

(4) The local HPC resources are often operated at capacity limit. There is no elastic service providing mechanisms for them to operate in a cost-effective and energy-effective manner.

The power industry can benefit a lot by running the compute-intensive applications on the 'cloud'. Firstly, since the communication media of cloud computing is Internet, the power users can immediately access to the information infrastructure in on-demand manner; secondly, the power users can easily operate the HPC resources in the cloud, which are not existed in-house; thirdly, supported by the large-scale computational resources, the cloud infrastructure can provide nearly unlimited capacity to applications, which allows the power users to quickly solve their problems without sacrificing the computation accuracy. And the resource provision of the HPC resources are virtualized and elastic (implemented in the *Firmware Layer* in the proposed layered model), meaning that the power users can dynamically scale the utilization of the resources based on the problem scale, budget, and other practical considerations. Fourthly, all the resources are managed by the cloud side, which reduces the investment & operation costs of the power users to the minimal level.

2). Data-Intensive Power Applications

Data-intensive power applications represent the power applications which have strong demand in storing, managing and analyzing data. Based on the workload of the data analysis, a data-intensive power application would also be compute-intensive. With the data explosion of the modern power systems, data-intensive applications have increasingly important roles [81]. For example, a machine learning based system security assessment & control needs to learn knowledge from a large number of high-dimensional system operation points to predict the security of the system [82]. Another example is that in the smart grid, an electricity retailer would aggregate the big data of the energy consumption records of the end users, and analyze the big data to find the energy consumption patterns of the users [83]. Based on it, the retailer can optimize the retailing price schemes for each individual user, so as to optimize the operation of the distribution system. Other data-intensive power applications include data-driven wind power forecasting [84], data-driven wind turbine allocation [85], data-driven battery energy storage system capacity determination [86], non-intrusive appliance load monitoring [87], fault diagnosis [88], etc.

Traditionally, the development of the data-intensive applications are often developed from scratch by the power engineers and researchers, and the data analysis is often performed in the local resources. This pattern is costly, low-efficient, and can hardly cater for the big data requirements in the future grid. With the widely deployment of the various high-frequency data sources (e.g. the distributed renewable sources, PMUs, two-way communication infrastructure, etc.), the wide-area data aggregation and analysis can hardly be performed in the centralized pattern. With the cloud-based information infrastructure, the data-intensive power applications can be significantly strengthened in 3 aspects:

(1) Unlimited data aggregation and management resources. Just as the HPC resources, the *Firmware Layer* of the layered model can elastically provide data collection & storage resources on-demand, which can well satisfy the big data management of the future grid. In addition to the physical resources, the advanced data management services in the *Abstracted Service Layer* (one example is the Google Data Store [76]) can be utilized to support the transparent retrieving and querying of the wide-area data;

(2) Advanced data network performance control. The distributed data management techniques in the *Dynamical Scheduling Layer* will effectively optimize the performance of the data network. For example, the data package routing & replica techniques can dynamically optimize the transfer routes of the data packages and the locations of the replicas, so as to fast response to the users' requests as well as maintain the robustness of the data network;

(3) Advanced data processing framework. As an important part of cloud computing, the big data processing frameworks can make the power engineers & researchers effectively develop the data-intensive applications. These frameworks can be seamlessly integrated with the virtualized resources in the 'cloud', and can be easily scaled to parallel processing the large datasets. A famous big data processing tool is the MapReduce framework and its implementation software Apache Hadoop.

3). Collaborative Power Applications

The third category of power applications we discuss here is the collaborative power applications. With the development of smart grid and the ongoing trend of deregulation, there will be many applications where multiple parties need to collaboratively accomplish a specific task. A simple example would be the bidding process of the electricity market, where different generation companies (GENCOs) submit the bids to the independent system operator (ISO), and the ISO matches the bids to determine the market clearance prices [89]. Another example is the electric vehicle (EV) dispatch in a distribution

system. The EV owners submit their individual driving demands to the system operator (e.g., the estimated driving distance, plug-in time, plug-out time, expected SOC, etc.). By gathering such information, the system operator decides the optimal charging plans for the EVs, and sends the plans to the EV owners [90]. Other collaborative power application include the cooperative dispatch of virtual power plant resources [91], agent intelligence based demand response [92], etc.

A collaborative power application could be compute-intensive and/or data-intensive. Or it could be neither compute-intensive nor data-intensive. Anyway, some basic requirements can be drawn from the collaboration process:

(1) Scalability. The collaboration should be scalable to support different number of collaboration parties;

(2) Security & confidentiality. When multiple parties share data in the collaboration process, the secure data access and authority are desired. And the confidentiality of the data should be ensured during the whole collaboration process, meaning that the private data should not be revealed to the irrelevant parties;

(3) Efficiency,. The collaboration should be efficient and fast.

By applying the cloud-based information infrastructure to manage the collaboration process, the cloud platform will act as the collaboration coordinator, which is responsible for hosting the collaboration system (data and computation), as well as managing and enforcing the agreed access policies. The *Firmware Layer* can provide the access authentication services and perform the policy-based access control. In addition to this, the services provided by the *Secure Communication Layer* and the secure collaboration techniques (such as the SMC technology) in the *Abstracted Service Layer* can significantly keep the security & data confidentiality of the collaboration process.

By running the collaborative power applications in the cloud side, the elastic virtualized resource provision capability of the cloud-based information infrastructure can also ensure the high scalability and efficiency of the collaboration process.

4). Applications in Real-Time Power System Operations

The future power grid is expected to have the ability of self-healing and fast respond to various disturbances, which drives the establishment of the different kinds of real-time operation & control applications. Here although a real-time power application can also be one of above 3 categories, an

application which is classified as one of above 3 categories is not always be a real-time power application. For example, a long-term network planning application could be compute-intensive, but in most of cases it is considered as an offline task. Another example is that the large scale EV dispatch problem is a typical collaborative application which requires a large number of information exchanges among the system operator, load aggregator and EV owners, but the dispatch is often performed in the day-ahead stage, based on the various forecasted information [90].

A noticeable feature of the real-time power applications is the capturing and fast processing of the real-time data streams. The processing of the online data might also be organized as a complex work flow, where multiple parties can be involved. From this, we can summarize two main requirements of the real-time applications:

(1) High processing speed. For the real-time applications, the power operators (or the software agents) often need to make decision and take control actions in a short time, thus the high computing speed is required for processing the real-time data streams, which are often with noises and unpredictable arrival rates;

(2) Fault-tolerant and reliable service provision of the computing environment. The efficient operations of the real-time power applications need to be supported by the robust computing infrastructure to prevent the underlying hardware breakdowns from halting the online data processing work flow.

A typical example of the real-time power application could be the real-time system peak load tracking [93]. With the fine-gained data collection of the SCADA system and the widely deployment of the AMI, the volume of the real-time data generated is huge. The current data collection rate of the SCADA system and AMI are every 3-5 seconds and every 15 minutes, leading to the gigabyte-level cached data for a regional distribution network. In this context, the system operator needs to analyze the data to track the system peak load and take appropriate control actions. Other real-time power applications include the system restoration [94], real-time frequency regulation [95], predictive control based energy management of the buildings [96], etc.

The real-time processing of such vast amounts of data can be a big challenge of the traditional computing modes. As an integrated technique of cloud computing, stream computing (located in the *Abstracted Service Layer*) provides a highly flexible and effective solution for the online data processing and decision making. In the stream computing architecture, by properly designing the data flow

processing topology, the real-time data generated by the data sources can be collected by the distributed nodes. The data flow then can be sent to the other processing nodes to do step-by-step further analysis, and processed data flow can be finally sent to the target node to support the decision making. And the advanced data processing framework (such as the MapReduce) could be seamlessly integrated with the stream computing platform to accelerate the data processing.

The real-time power system applications will also significantly benefit from the virtualization technology of the cloud computing, which is located in the *Firmware Layer* of the proposed layered model. The virtualization technology provides an ideal solution for addressing the hardware exception problem. When the underlying hardware exception occurs, the virtualized resource management system can mitigate the virtualized computing instances on which the real-time applications run to other physical resources, so as to ensure the secure and effective running of the real-time power applications.

B. Compute-Intensive Application Demonstration: Cloud-enabled Load Shedding Scheme for Voltage Stability

In [76], reserchers developed a parallel processing framework for the event-driven load shedding (LS) against voltage collapse, and deploy it in a local PC cluster. The parallel process can be easily mitigated into the cloud side by utilizing the *IaaS*-level services, where users can apply for the virtualized resources and operate them just as local resources.

1) Problem Overview

When the voltages of the buses of a power system violate the allowable scopes, the data-driven load shedding strategy is performed to shed the power loads on different buses, so as to restore the voltages. The load shedding problem can be modelled as an optimization problem, where the decision variable is the shed load vector, representing the shed load amount of each bus. The optimization objective is to minimize the total interruption cost of LS. The model is also subjected to the voltage stability margin constraint, voltage limits constraint, branch current limits constraint, and the power flow equations constraint. The details of the problem can be found in [76].

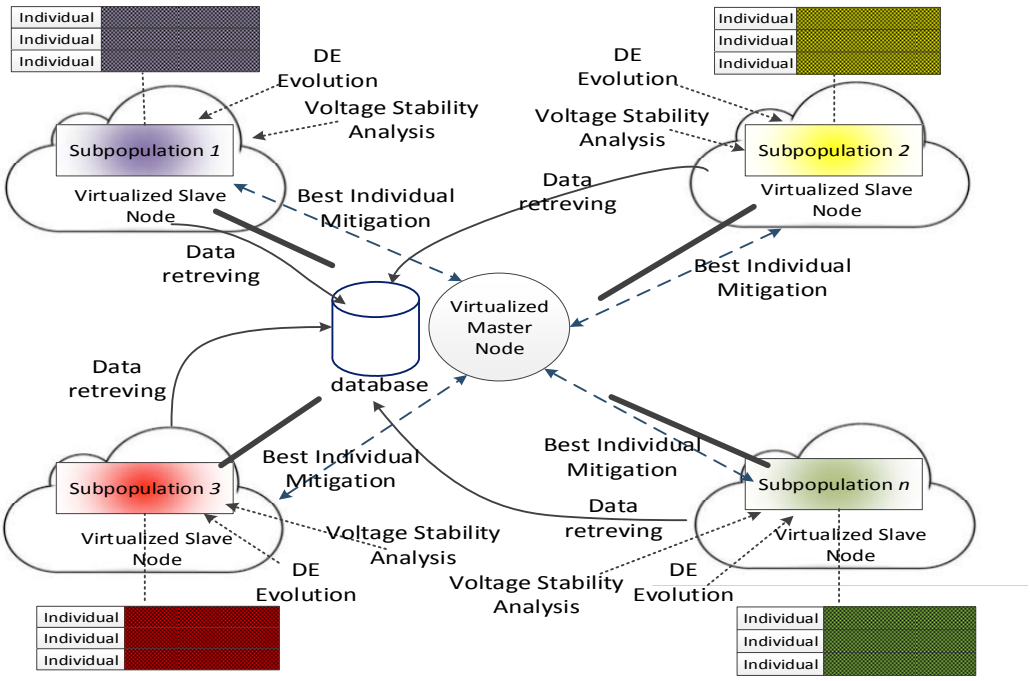

Figure 2-3. Parallel process model of the load shedding strategy on Amazon EC2.[174]

To support online application, the load shedding decision making process must be performed very fast to prevent the system from voltage collapse. Therefore the Parallel-DE algorithm is employed to solve the model. The parallel strategy follows the master-slave pattern. The master process divides the whole population into *N* subpopulations and distributes them to the slave processes. The slaves connect with each other through the master in a predefined topology such as a 'ring'. Then each subpopulation evolves separately in a parallel pattern. To promote the information sharing among the subpopulations, in each iteration, the best individual of each subpopulation is moved to the next subpopulation via the master process. The details of the parallel scheme can be referred to [76].

2) Cloud-based Parallel LS Framework

As a large *IaaS* service provider, Amazon EC2 provides a resizable compute capacity. We mitigate the parallel computing framework to a 16-core virtualized cluster of Amazon EC2, shown in Figure 2-3. Through the *IaaS* Web portal (located in the *Abstracted Service Layer*), the simulation programs can be easily hosted and ran on the virtualized resources, which are managed by the Amazon EC2's virtual machine management schemes (located in the *Firmware Layer*). The parallel programs are scheduled by Amazon EC2's underlying task scheduling schemes (located in the *Dynamical Scheduling*

Layer) on the physical resources. All the data communications are encrypted by the RSA to ensure the data security.

We use the same experimental setup with [76]. The total execution time of the simulation on a local PC is 1800s. We evaluate the total computation time under different number of slave processes created on the cloud. The result is shown in Figure 2-4. The total execution time significantly reduces with the increase of the slave processes. Figure 2-5 reports the convergence curves of the parallel-DE on the cloud. It shows the parallel-DE find a good enough solution only after 9 iterations.

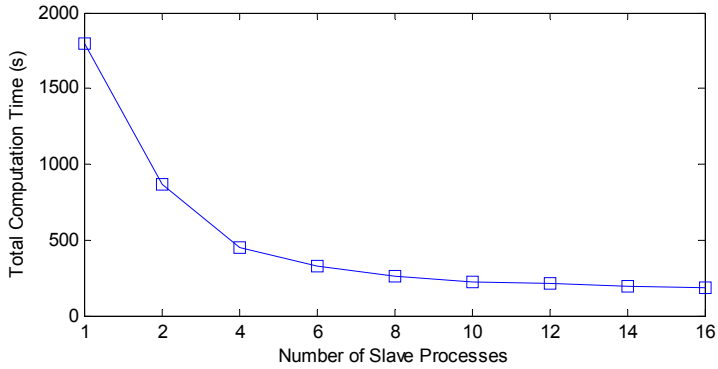

Figure 2-4. Total execution time of the simulation

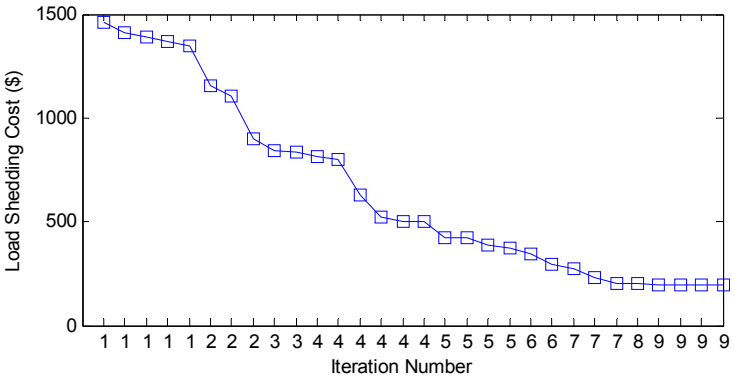

Figure 2-5. Convergence curves of the parallel-DE and the original DE

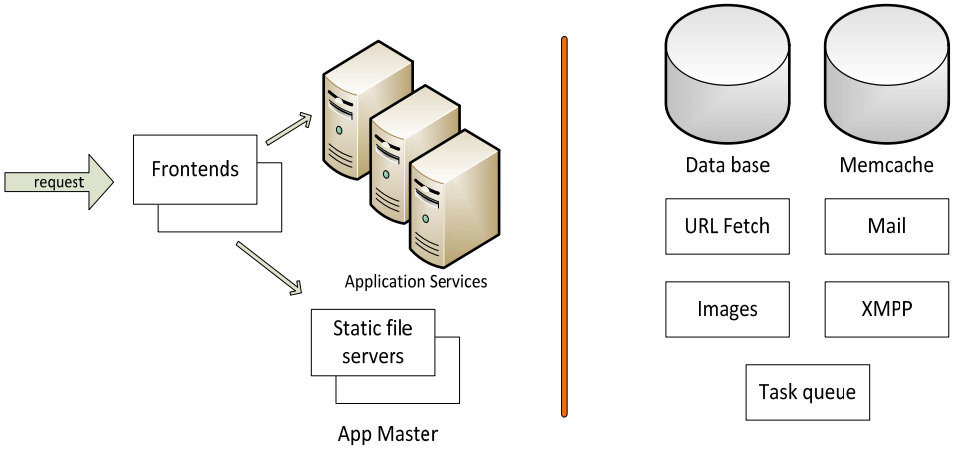

Figure 2-6. Architecture of the Google Application Engine [71]

C. Data-Intensive Application Demonstration: Cloud-Enabled Pattern Discovery-based Power System Dynamic Security Assessment

This section demonstrates how to utilize the cloud-enabled development tool to develop a dynamic security assessment (DSA) application and deploy it into the Google Application Engine (GAE) as an online service.

1) Introduction of GAE

GAE [97], [98] is a cloud service which provides an integrated framework (located in the *Abstracted Service Layer*) for users to develop scalable web applications directly on Google's infrastructure, rather than pain access to the physical hardware. Users only need to focus on the logic of the applications while GAE automatically handles the common issues in other layers, such as load balancing, server environment set up and maintaining. Figure 2-6 shows the GAE architecture.

Basically, every request is handled firstly by the App frontends, and then the App frontends read the configuration information of the application and dispatch it to an application server according to a certain load balancing mechanism. All the communications are encrypted by the RSA framework. The application then starts and runs in the application server.

2) Introduction of PD-based Dynamic Security Assessment

Our previous works [99], [100] applied a pattern discovery algorithm on the DSA. PD trains *n*-dimension data turples, and partitions each dimension into several segments. By combining the partitions segments of each dimension, multiple hyper rectangles are identified in the *data* space, which

are called *event*s. Some events might be recursively partitioned. The hyper rectangles where the numbers of data points they contained are statistical meaningful are called *pattern*s. Each pattern is labeled as *secure*/*insecure* according the percentage of the secure training data points it contains. After discovering the patterns, each online operating point (OP) can be assessed to be *secure* or *insecure*. The further details of the PD-based DSA can be found in [99], [100].

3) Cloud-based Framework for PD Driven DSA

Although PD can provide high accurate assessment results [99], one performance bottleneck of PD is that when the data dimension is high, the recursive process might be very time-consuming. Imaging a 20 dimension data space where each dimension will be divided into 2 segments during the partition, 2^{20} events will be formed. PD then needs to check the 2^{20} events one by one to see whether it should be further portioned. If so, then repeats the partition process on the sub space covered by that event. If there are too many events need to be recursive partitioned, the total execution time will become very large. Therefore, it is necessary to design some parallel mechanism to improve the performance of PD. On the other hand, it is desirable to publish the program as an online service, so that engineers can access it when they want to assess the OPs.

The parallel strategy here is to share the event checking task with multiple processes. The master process starts multiple processes to conduct the event checking and recursive partition task. Each process checks part of the events and send the result back to master. The parallel framework is shown in Figure 2-7.

The training data is stored in the data store of GAE, which is a persistence database storing the data shared by all application instances. The master application reads the tanning data to do partition, and forms the event list. Then the master stores the in-formation of the events into data store, and sends *n* HTTP requests to slave application, where each request encapsulates start and end indexes of the events to be processed. For every HTTP request, GAE starts and manages an instance of the slave application automatically. That instance reads the training data from data store, extracts the event indexes from the HTTP request, and do the checking & recursive partition. Finally, each slave updates the event information in data store and sends HTTP response back to the master.

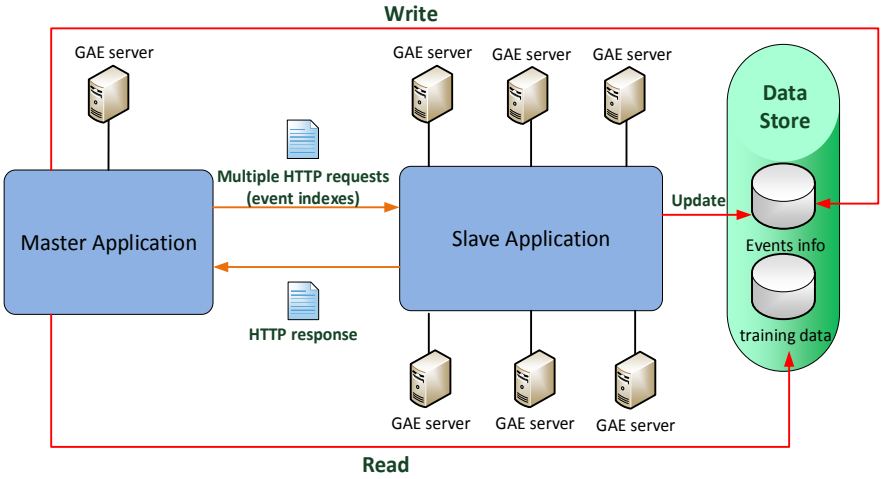

Figure 2-7. Parallel framework of pattern discovery process

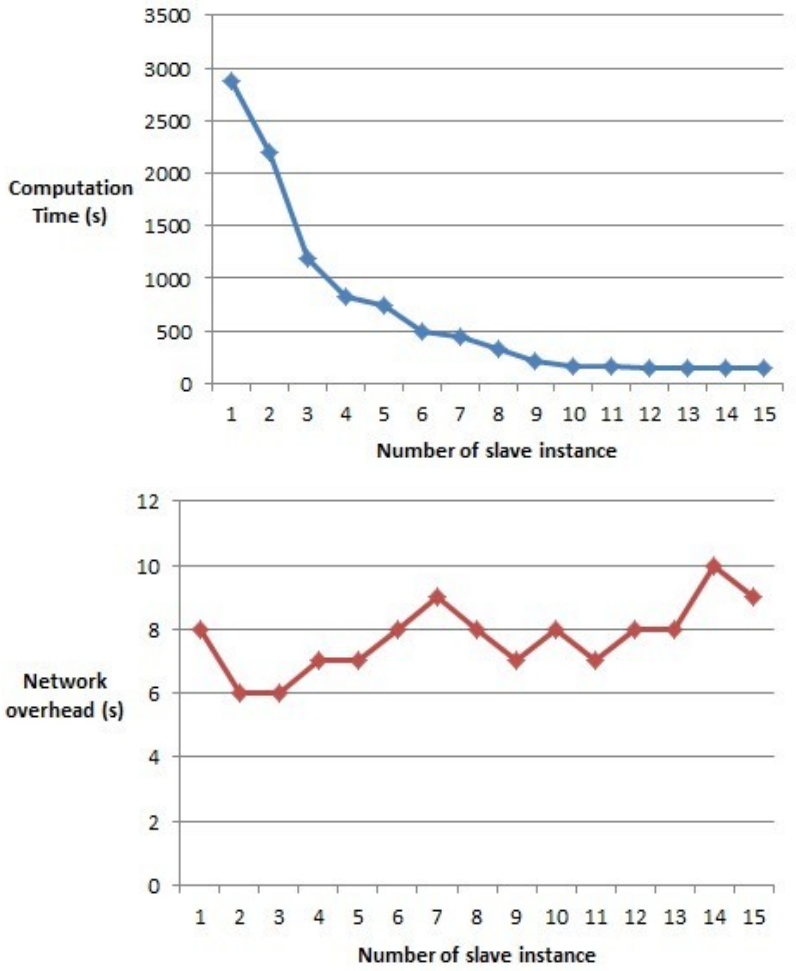

Figure 2-8. The computation time (up) and network overhead (down) on GAE

4) Simulation Result

Firstly, a transient stability database is artificially generated as the training database. Totally 6,000 different OPs are simulated and the time-domain simulations are performed on the OPs under various disturbances. According to the time-domain simulation result, the OPs are labeled as *secure* or *insecure*. Then, 20 critical features are selected by employing the RELI-FF algorithm [101]. Afterwards, the PD algorithm is employed to discover patterns in the 20-dimension data space. We repeat the experiments 15 times on GAE by increasing the number of the parallel slave instances, and observe the computation time and network overhead shown in Figure 2-8.

It can be seen that the computation time is dramatically reduced along with the increase of parallel jobs, while there exist a little overhead, about 6-10 seconds. Those overheads are mainly incurred by starting the instances, TCP communications, and database access.

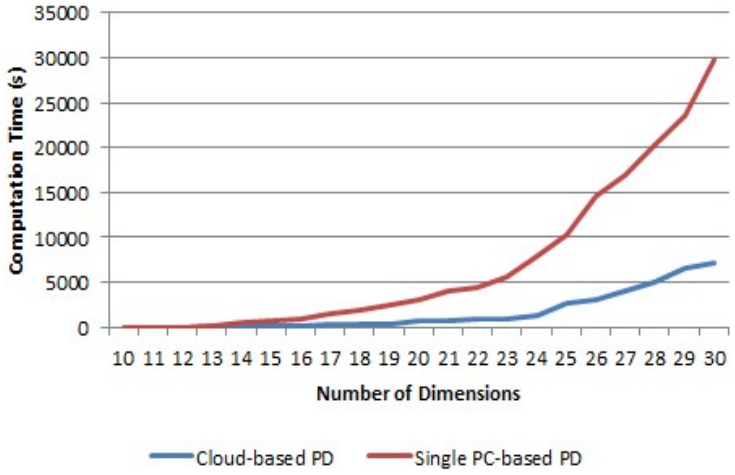

Figure 2-9. The computation time comparison between the single PC-based PD and the cloud-based PD

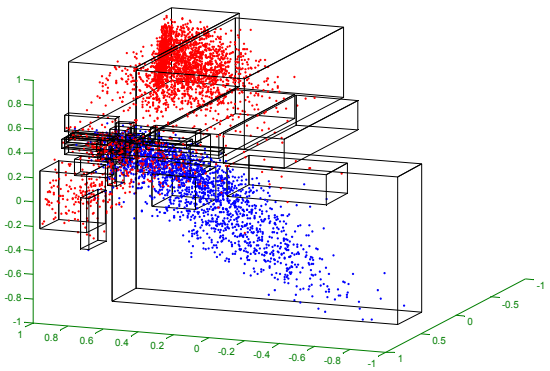

Figure 2-10. PD demonstration on 3-dimension data space [73]

The performance of the cloud-based PD and single PC-based PD is compared by setting the number of the slave instance of the cloud-enabled PD to be 10 and varying the number of dimensions from 10 to 20. The single PC-based PD is performed on a 64-bit, Dual CPU DELL PC, with Windows 7 operation system. The computation time comparison and the corresponding network overheads of the cloud-based PD are shown in Figure 2-9. It can be seen that when the data dimension increases, cloud-based PD shows significantly better performance than the single PC-based PD.

When the data dimension is 2 or 3, the pattern discovery can be visualized. Figure 2-10 shows the patterns discovered with 3 selected critical features. Each rectangle represents a pattern. The technique guide of developing and publishing the Web applications through GAE can be found in [98].

D. Collaborative Application Demonstration: A Cloud-Enabled Direct Load Control Framework

1) Application Overview

In this application, we propose a dispatch application of the large scale of thermostatically controlled loads (TCLs). It is assumed that the large scale TCLs are grouped and managed by multiple TCL aggregators. The aggregators participate in the direct load control (DLC) program launched by the utility, where the utility needs to dispatch the TCLs to achieve a specific objective (e.g. peak load shaving). The dispatch schematic of the TCLs is shown in Figure 2-11. It is a collaboratively hierarchical dispatch model:

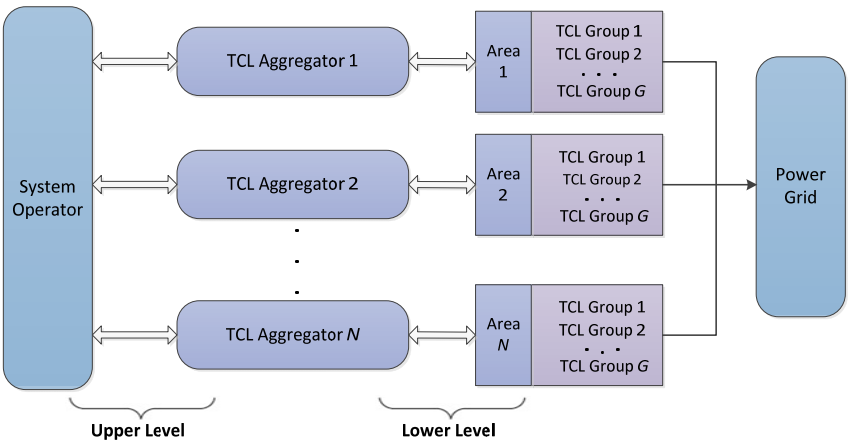

Figure 2-11. Hierarchical dispatch model for large scale TCLs

a. The aggregators submit the load shedding bids to utility;

b. The utility solves the upper-level day-ahead dispatch model according to the specific objective, and then sends the load shedding instructions to the aggregators;

c. After receiving the load shedding instructions, the TCL aggregators solve the lower-level day-ahead operational planning model and send the dispatch deviations back to the utility;

d. Based on the received dispatch deviations, the utility adjusts the load shedding instructions and sends the new instructions to the aggregators;

e. Repeat steps d. and e. until the pre-defined termination conditions are satisfied.

2) Utility Side: Upper-Level Dispatch Model

After receiving the bids, the utility solves the dispatch model to make the dispatch plan by assigning instructed load shedding amount to each aggregator. The day-ahead dispatch model of the utility aims to minimize the sum of the total load shedding cost and the penalty cost of the dispatch deviation between the upper and lower levels,

$$\min\left(\sum_{t=1}^{T}\sum_{a=1}^{A} pr_a^{bid}(t)\cdot D_a(t)+\sum_{t=1}^{T}\sum_{a=1}^{A}\alpha\cdot dev_a(t)\right) \tag{1}$$

$$dev_a(t)=\left|SL_a(t)-D_a(t)\right| \tag{2}$$

s.t.

$$0\le D_a(t)\le CP_a^{TOTAL}(t) \tag{3}$$

$$\sum_{a=1}^{A} D_a(t)\ge P^{sys}(t) \tag{4}$$

where *t* and *T* are the index and number of the dispatch time intervals; *a* and *A* are the index and set of the TCL aggregators; $pr_a^{bid}(t)$ is the bidding price of aggregator *a* at time *t* ($); $D_a(t)$ is the instructed load shedding amount for aggregator *a* at time *t* (MW); $SL_a(t)$ is the scheduled LS amount of aggregator *a* at time *t* (MW); α is the penalty cost factor of the dispatch deviation between the two levels; $CP_a^{TOTAL}(t)$ is the total controllable TCL capacity in the bid of aggregator *a* at time *t* (MW), which can be determined by a certain bidding strategy; $P^{sys}(t)$ is the totally required LS of the system at *t* (MW);

3) Aggregator Side: Lower-Level Dispatch Model

The objective of the operational planning of the TCL aggregators is to maximize the total profit in the power market.

At time *t*, the scheduled total shed ACL of aggregator *a* is,

$$SL_a(t) = \sum_{g=1}^{G_a} s_a^g(t) \cdot CP_a^g \tag{5}$$

where G_a is the number of the TCL groups of aggregator *a*; $s_a^g(t)$ is the state of the *g*th TCL group at *t* (1-ON, 0-OFF); CP_a^g is the capacity of the *g*th TCL group of aggregator *a* (MW), which is calculated by the sum of the rated power of each TCL in the group. The income of the aggregator *a* from the power market is represented as,

$$Profit(a) = \begin{cases} \sum_{t=1}^{T} pr^{clear}(t) \cdot D_a(t) \cdot \Delta t & SL_a(t) \geq D_a(t) \\ \sum_{t=1}^{T} \left(pr^{clear}(t) \cdot SL_a(t) - \beta \cdot \gamma_a(t) \right) \cdot \Delta t & SL_a(t) < D_a(t) \end{cases} \tag{6}$$

$$\gamma_a(t) = \max[0, (dev_a(t) - dev_{max})] \tag{7}$$

where Δt is the time interval duration; $pr_a^{clear}(t)$ is the electricity clearance price in the day-ahead market at *t* ($); β is the penalty cost factor of the lower level dispatch deviation.

The load shedding cost of the aggregator *a* is calculated as,

$$cost(a) = \sum_{t=1}^{T} pr_a^{retail} \cdot SL_a(t) \cdot \Delta t \tag{8}$$

where pr_a^{retail} is the retailing price of the aggregator *a* to its customers ($). The aggregators solve model (9) to schedule the control actions of the ACL groups to maximize its total revenue.

$$Revenue(a) = Income(a) - cost(a) \tag{9}$$

s.t.

a) TCL group state constraint

$$s_a^g(t) \in (0,1) \quad \forall a = 1:A, g = 1:G_a, t = 1:T \tag{10}$$

b) Minimum online time constraint.

$$\tau_{a,g}^{on}(t) \geq \tau_{\min}^{on} \tag{11}$$

$$\tau_{a,g}^{on}(t)=\left(\tau_{a,g}^{on}(t\text{-}1)+s_a^g(t)\cdot\Delta t\right)\cdot s_a^g(t) \tag{12}$$

where $\tau_{\min}^{on}$ is the minimal required TCL online time (hour); $\tau_{a,g}^{on}(t)$ is the accumulated online time of the *g*th TCL group of aggregator *a* at time *t*.

4) Cloud-Based DLC Architecture

The proposed DLC framework involves a big data aggregation process, where the TCL aggregators need to collect the state data of the large scale TCLs managed by them to do the lower-level dispatch. It also involves a typical distributed optimization process, where the utility and the aggregators communicate with each other to converge to the final solution iteratively. There are some basic communication requirements in this collaborative process. Firstly, the communication architecture should be scalable, so as to support a large number of TCLs and TCL aggregators to participate in the DLC program; secondly, the communication system should be robust enough to ensure the reliable operation of the distribution network; thirdly, the transferred data should be kept secure and confident during communication; lastly, the communication must be efficient.

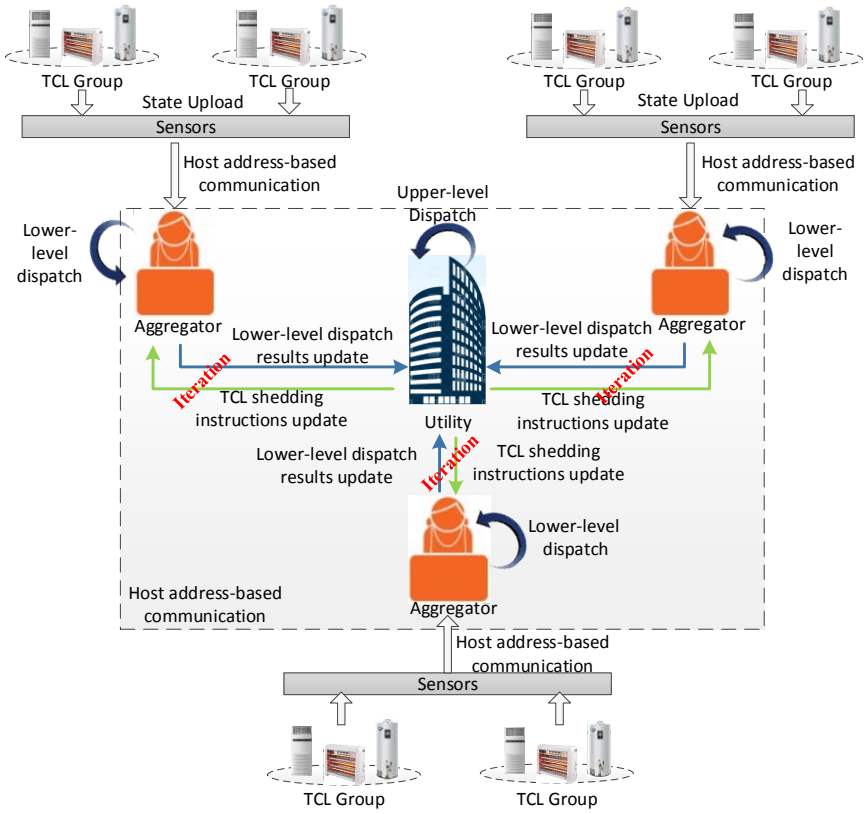

Figure 2-12. Centralized DLC architecture [174]

In the current centralized system structure, the DLC process will be centrally performed in the EMS of the utility and the EMSs of the aggregators, respectively. In the upper level dispatch, the utility establishes communications with the aggregators, and iteratively exchange information with them until the algorithm converges. In the lower level dispatch, each aggregator communicates with the TCL groups, and solves the lower-level planning model. This can be depicted in Figure 2-12.

Such centralized architecture has many limitations. Firstly, it is a host address-centric architecture, meaning that the EMS of the utility and the aggregators need to know the host address of each other to communications. Such host address centric communication pattern is vulnerable to cyber attackers, because the cyber attackers can easily launch the DDoS attack to break down the EMS server; secondly, although the centralized architecture is suitable for small scale networks, it is very difficult to be scaled to cater for the large deployment of TCLs due to the bandwidth bottleneck and the computing capacity limit of the EMS.

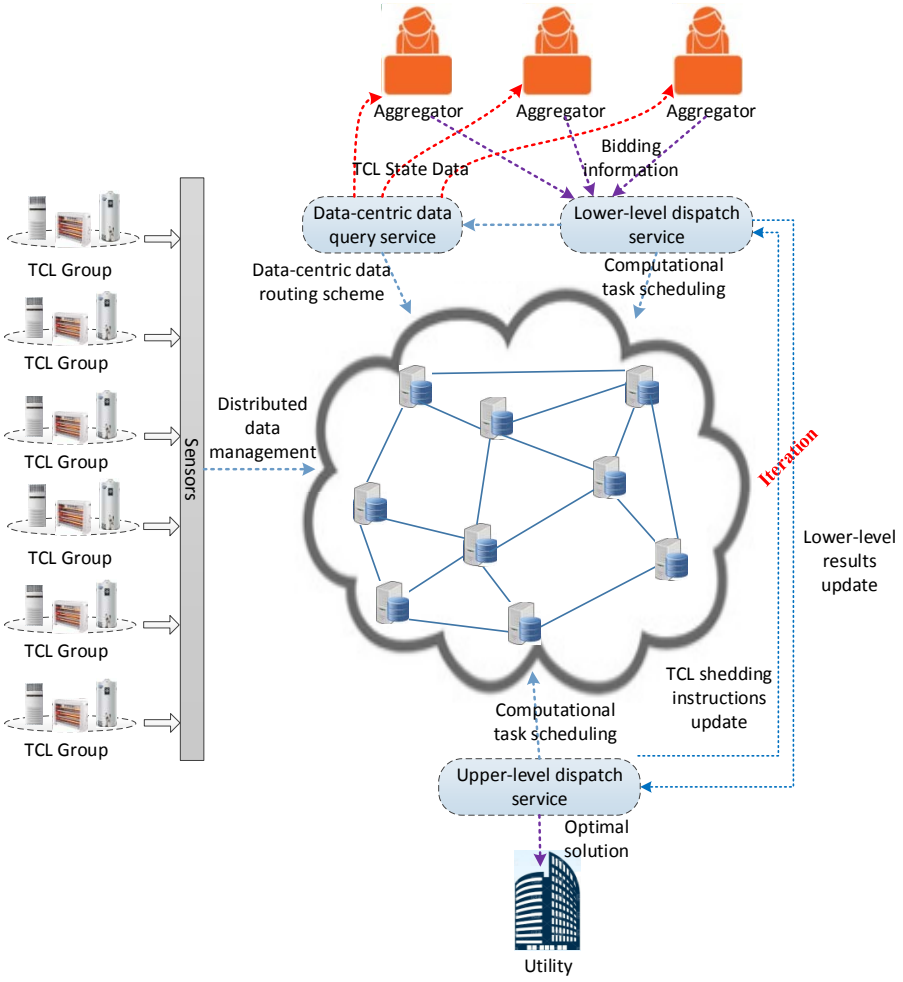

Figure 2-13. Cloud-based DLC architecture [174]

Based on the cloud-based information infrastructure, the cloud-enabled DLC architecture is proposed to overcome above drawbacks, shown in Figure 2-13. In the cloud-based architecture, the roles of the utility EMS and aggregators are weak, and the cloud acts as the collaboration intermediary. The EMSs of the TCL aggregators and the EMS of the utility interact with the cloud services. Firstly, the *Sensor and Actuator Network Layer* collects the state data of the managed TCLs, and deliver it to the TCL aggregators through the data query service, which is located in the *Abstracted Service Layer*. Based on the collected TCL data, the aggregators make the bids and send the bid information to the lower-level dispatch service. The lower-level dispatch service notifies the utility EMS about the bid information and then launches the distributed optimization process. In each iteration, the upper-level dispatch service notifies the lower-level dispatch service about the upper-level dispatch results, and the latter solves the lower-level dispatch model, and sends the updated lower-level dispatch results to the upper-level

dispatch service. The upper-level dispatch service then updates the upper-level dispatch results. When the optimization process converges, the web services notify the aggregator and the utility about the final dispatch results. Both of the lower-level and upper-level dispatch services are located in the *Abstracted Service Layer*. The cloud-based DLC architecture is distinguished with the centralized DLC architecture in the following aspects.

(1) Service-oriented computing. In the cloud-based architecture the aggregator agents communicate with the utility and the TCL database through the *Abstracted Service Layer* without knowing their host addresses. The mapping of the service interface and the underlying physical resources is managed by the *Firmware Layer*.

(2) Data-centric distributed data management. In the centralized DLC model, the TCL information is stored centralized in the database of the aggregator EMSs. In the cloud-based architecture, all the raw physical data (including demand side data, power network data, etc.), which is called *observations* [56], is stored distributed storage network. Users can define *events* to query the data. *Events* are referred to certain pre-defined constellations of observations. In our application, an *event* defined by the aggregators may include the model parameters of the TCLs (air conditioner, water heater, etc.), building parameters, etc. The data is stored and queried in a data-centric manner. That is, all the data is stored by name at the storage nodes. Queries of the data are based on a particular name rather than the address of the nodes. Certain data routing algorithms (e.g. the Greedy Perimeter Stateless Routing (GPST) algorithm [57]) is then applied in the dynamical scheduling layer to transfer the data to the query node.

(3) Computational network load control. The DLC computations are scheduled together with other computational tasks on the physical computational resources. Certain computational load routing schemes will be applied in the *Dynamical Scheduling Layer* to schedule the computational tasks among different resources.

5) Simulation Results

To prove the validity of the proposed DLC framework, we simulate 4 TCL aggregators. The air conditioner loads (ACLs) are considered. Each aggregator manages 200 ACL groups and each group includes 200 houses. The ACL model in [102] is used and the Monte-Carlo simulation strategy in [103] is performed to generate the realistic house scenarios. The differential evolutionary algorithm [104] is used to solve the lower-level dispatch model, and the AMPL solver [105] is applied on the upper-level dispatch model. The dispatch process finally converges after 24 iterations. Figure 2-14 shows the final dispatch results. The solid and dotted lines represent the instructed shed load and the scheduled shed

load profiles. It can be seen the aggregators effectively schedule the ON/OFF states of the TCL groups to follow the load shed instructions, with some minor deviations.

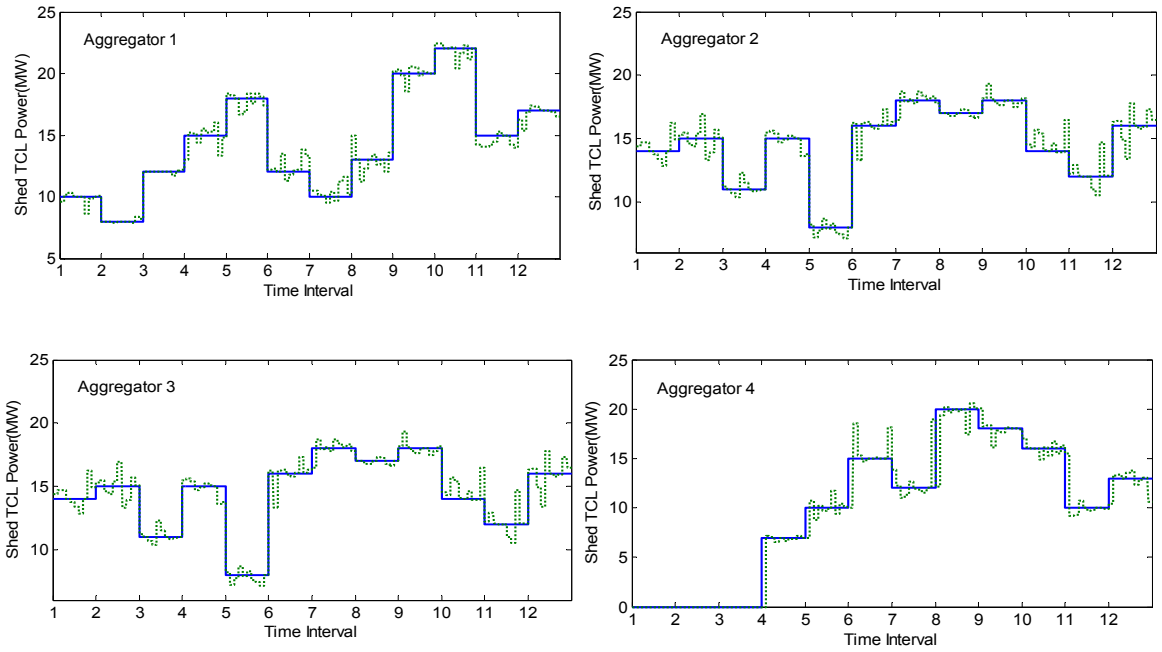

Figure 2-14. Day-ahead operational planning results of the aggregators

The convergence performance is significantly by the control parameter α. Figure 2-15 shows that with the increase of α, the dispatch deviation decreases. However, with larger α, more iteration times are needed to convergent. The choice of α is a compromise between dispatch deviation and execution time.

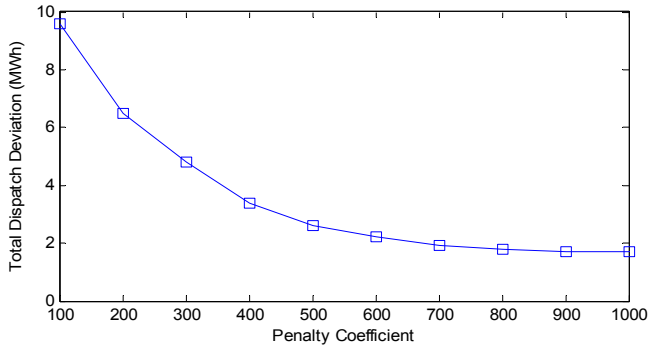

Figure 2-15. Sensitivity study of α

IV. CYBER SECURITY CONSIDERATIONS

Since the modern power systems have been becoming then complex cyber-physical systems, the cyber security issues of the power grids have been drawn increasingly attentions in recent years. As discussed below, with the support of some newly emerged cyber-attack defend technologies, the cloud-based information infrastructure is capable of securing the cyber security collaborative process to ensure the reliable DLC operation.

Here we consider 4 kinds of cyber-attacks as below, which have been proven to be the non-neglectful threatens for the modern industrial systems [106].

A. Compromised-Key Attach & Eavesdropping Attack

By using the compromised key, the attacker can gain access to the secure communication between the load aggregator and the cloud to interpret the private information such as the price and the dispatch capacity. Also, since such private data will be decrypted in the cloud before the computing, the attacker could eavesdrop the decrypted data.

As for these two kinds of attacks, there are some new technologies can be integrated into the cloud-based information infrastructure to secure the information communications. One possible option is to utilize the SMC technology, which allows the communication ends to operate the encrypted data without decrypting it. For example, in the previous collaborative DLC application scenario, the utility can do the calculations based on the encrypted price and capacity data directly. By this way, there is no need to transfer the private key from the load aggregator to the utility agent, and the private data security can be significantly enhanced. The other possible solution is to adopt the ‘crypto cloud computing structure’ [107], which is based on the Quantum Direct Key system [108]. In the crypto cloud computing structure, each entity encrypts data using his/her own private key. All elements in the system have their own keys, and all the events occurred in the cloud environment are also assigned a unique key. For instance, in the collaborative DLC application, the involved web services and all the DLC events (TCL data query, upper-level dispatch, lower-level dispatch, etc.) are assigned unique keys, which are hard to compromise by the attackers. In this way, the security and credibility of the exchanged information can be guaranteed.

B. Denial-of-Service (DoS) Attack

The attacker can inject a huge amount of data to the communication channel to overload the server. The DoS attack could happen in different levels of the cloud environment. It could inject the junk data to consume the bandwidth resources (the bandwidth attack); it could take advantage of the lacuna of the network protocols to overload the target server (the protocol attack); or it could sends a large number of HTTP requests to attack the web applications (the application attack). Taking the collaborative DLC application as an example, there is an iterative convergence process for the DLC dispatch, where the information is exchanged periodically between the servers where the DLC web services are hosted. Any kind of above 3 DoS attacks will significantly block or delay the iterative DLC process.

The DoS attack in the cloud environment could be well addressed by many cloud-based solutions. For example, one option is to use the cooperative intrusion detection system [109]. A intrusion detection system (IDS) is deployed in each cloud computing region which will cooperative with each other to mitigate the DoS attack in the network. The IDS compares the type of received data packet with that in its block table and if a match is found, the packet will be dropped. If no match is found, but detected as anomalous, then a alert is sent to other IDSs. Each IDS then exchange alerts with other IDS and uses the majority vote method to dice true and false alerts.

Another promising solution for defending the DoS attack is to use the cloud trace back (TCB) technique [110], which is deployed in the Web server and uses the distributed packet marking algorithm to identify the source of the DoS attack. Then, the Cloud Protector technology [110] can be used to filter these attack patterns in future.

Other technologies that can be used to enhance the robustness of the cloud-based infrastructure include the confidence based filtering approach [111], the filtering tree approach [112], the information based metrics method [113], etc.

C. Man-in-the-Middle Attack

In the man-in-the middle attack, the attacker could place himself between the two ends of a communication, and he/she could intercept or modify the communications. Thorough the man-in-the middle attack, the attacker might run power applications deliberately in the cloud without authorization. The cloud-based infrastructure can resist the man-in-the-middle attack through the authentication

mechanism. The core of the authentication is based on the File Allocation Table (FAT) [114], which has been already supported by all existing virtualized operating systems. The FAT contains the information of the operations that a user is going to do. By checking over the previous operations of the user, the cloud system can determine the validity and integrity of the new operation.

As an important type of the man-in-the-middle attack, the false data injection attack (FDIA) [115] can significantly disturb the operation of the power grid. In the FDIA, the attackers can intrude the communication channels to inject the false data. These injected data could lead to the wrong control actions and mistaken operation results by artificially altering the communications. For example, in the collaborative DLC application described above, the attacker could alter the price and load capacity data by launching the man-in-the-middle attack on the communication channels between the load aggregator agents and the utility agent, and this will affect the upper-level DLC dispatch results. The defense of the FDIA mainly lies in two levels. In the hardware level, the robustness of the physical sensors (such as the smart meters, PMUs, etc.) needs to be enhanced to make them more difficult to be intruded. In the application level, in addition to the cloud authentication mechanism, the false data detection techniques can be implemented and integrated in the cloud platform. For example, [116] proposed a defend method to protect a set of basic measurements to detect FDIAs; [117] proposed a defending strategy against FDIAs by dynamically changing the information structure of micro-grids; [118] proposed an adaptive CUSUM algorithm to defend against FDIA.

V. CHALLENGES AND LIMITATIONS

In despite of the merits, there are some technical challenges which need to be considered when practically develop the cloud-based information infrastructure for the future's power grid. In this section, we summarize some challenges which arise in different aspects.

A. Computational Load Scheduling

The cloud-enabled computational load scheduling algorithms for the future power system problems needs to be studied. Different power grid problems often have different computing response time requirements. For example, a long-term network planning task has low accomplishment time requirement; an operational planning problem often needs to be resolved in several minutes to several hours; a real-time dispatch and control task may has to be accomplished in several seconds. Furthermore, different applications may need to access different power resources, which would be

located in different locations and have different access authorities. Although the cloud-based information infrastructure can provide elastic and scalable computing capabilities to serve various power grid applications, the 'power grid-aware' computational load scheduling algorithms needs to be studied, which need to consider not only the performance of the computational resource network, but also the characteristics and performance requirements of the power grid applications.

B. Distributed Data Management

Different power applications may have different scale data requirements. For example, a distribution system planning application will only use the local system data to do optimization, and the control objectives are the local resources (feeders, transformers, substations, etc.); a wide-area control application may involve the large-scale data and control the resources distributed in the wide area. Therefore, the 'smart' data aggregation and replication algorithms in the cloud-based information infrastructure should be studied to aware of the power grid features (such as the topology of the power grid), so as to achieve the optimal data retrieving, routing & storage performance.

C. Hardware & Software Technique Obstacles

Although there have been many emerging technologies to support the implementation of the cloud-based information infrastructure, there are still some technique obstacles. On one hand, some promising technologies are still not mature enough to be adapted to wide range of power applications. For instance, although the SMC technique has been implemented to a certain extent and has been applied on some simple electricity price clearance calculations [119], the current SMC technology is still limited to perform complex numerical calculations [76]. This will restrict its applications, at least in the current stage. On the other hand, the availability of some power devices to support specific functions are limited. For example, some current smart grid devices may not support public key operations, which may lead to some security threats.

D. The Impact of the Operation of the Cloud Data Centre on Power Systems

With the development of the cloud computing, the cloud data centers has become the large power consumers. For example, Microsoft's data center in Quincy, WA, has 43,600 square meters of space and uses 4.8 kilometers of chiller piping, and 965 kilometers of electric wire. This data center totally consume 48 MW power, equal to 4,000 homes [120]. Such large power consuming will also in turn affect the power flow of the grid. Therefore, the cloud data centers can also be treated as a specific

kind of controllable load, and the proper computational load scheduling among different data centers can alter their energy demand, and finally make contribution to the effective operation of the power grid. Although the study of this issue can be found in the literature [121], it is still a less-examined topic in both of the industry and academic circle.

E. Other Limitations

Other limitations will also be considered in the practical deployment of the cloud-based information infrastructure for the power grids. One limitation is the security aspect. As a newly developed computing paradigm, although there have been many efforts made to enhance the security of the cloud environment, it security still has not been proved for the large industrial systems. Considering the number of the participants of the future's power grid is very large and the coordinated work flow of different power tasks would be very complex, how to promote the effective operation of the grid while keeping the data security and integrity will become a major concern.

Also, the operation of the cloud platform heavily relies on the Internet. Although the efficiency of the Internet is kept on improving, in many cases the bandwidth limitations or unstable network conditions would limits its applications on solving the scientific and engineering problems. Consider the local resources (such as the local HPC facilities) have the advantage of easy to access and deploy, for specific types of the power applications, the proper choice should be made on running the power applications on local resources or the cloud side.

Another limitation lies in the application development complexity. The whole cloud-based information infrastructure would be supported by different cloud vendors, and the cloud working environment provided by different vendors might be quite different. Furthermore, in some cases the development of the cloud-based application would require the expert knowledge in the domain of computer science, which would be more complicated than developing the applications on the local computing resources. Therefore, the power users might feel difficult to adapt themselves to the cloud development environments.

To sum up, due to some security, confidentiality and convenience considerations, not all power applications are suitable to be mitigated to the cloud side. To what extent the power applications need to be mitigated to the 'cloud' is an issue which needs to be investigated by different parties in the practical deployment.

VI. SUMMARY

This chapter gives the discussion of constructing the cloud-based information infrastructure for the next-generation power grid. Firstly, this chapter analyzes the limitations of the current information infrastructure of the power grid. Then, this chapter proposes a layered model of the cloud-based information infrastructure to deal with massive data manage and storage problem of the power grid. Different cyber-physical entities are decoupled and their roles are identified in the layered model. The implementation technologies of the proposed layered model is also discussed.

Followed by the proposed layered cloud-based information infrastructure model, this chapter discusses the benefits of the cloud computing technology to 4 categories of power applications, respectively. This chapter gives 3 specific cloud-based power applications, for the demonstration purpose.

The cyber security issues related to the cloud-based information infrastructure and some challenges and the technique obstacles for applying cloud computing technology on the next-generation smart grid are also discussed. To enhance the security level of smart grid, a new method of quantum cryptography based cyber-physical frame will be discussed in the following chapters. To begin with, a definition of critical points will be addressed in the next chapter.

Chapter 3. Algorithm for Critical Points Searching

As we have discussed in Chapter 1 and 2, cloud-based information infrastructure provides high performance of computing and the ability of large sets of data management, which will handle big continuously generated data of future smart grid, but cyber security issues related to the cloud-based information infrastructure cannot be neglected.

Higher requirements for secure data transmission for the next generation are urgent. In Chapters 3 and 4, a quantum cryptography based cyber-physical security technology will be proposed on critical points of smart grid to deal with cyber-attacks. By using it, the priority is to find the critical points (or trust nodes).

I. INTRODUCTION

[122][123]provided a mathematic constrained optimization model on how to place the trust nodes to sound and feasible locations for a power system with many constrained economic or physical conditions. In other words, the model is aiming to divide a utility's network optimally into several regions, which can use the trust nodes detect various abnormal cases within a small area in case of any malicious activities being launched, meanwhile, the model gives a rigorous method to measure whether all constraints have been satisfied. Sadly, solving the problem directly by some current fashionable tools even have still been time-consuming[122] since the mixed integer linear programming(MILP) problem is provably NP-Hard.

[124] trys to construct a multi-layer intrusion detection systems(IDSs) to defend attacks in the communication network of smart grid system. In the smart grid network, such two targets as static placement of trust nodes as well as dynamic routing among communicating nodes were considered to be optimized simultaneously. However, only a preliminary heuristic algorithm, say, Dijksra's algorithm was applied to solve the complicated problem so that the method would be still time-consuming as well, especially facing practical engineering problems.

Evolutionary algorithm is a powerful approach evolutionary computation in artificial intelligence domain. It often performs well on exploring solutions for different kinds of problems because it is not necessary to make any assumption about the underlying fitness landscape when solving solutions. For

NP-hard problems, evolutionary algorithm may not guarantee to obtain the final optima, but it is definitely to approximate out some satisfied solutions meeting certain criteria. Multi-objective evolutionary algorithm (MOEA) is a subset of evolutionary algorithm. It has supper capacity to reach tradeoff optima for several conflicted objectives than normal single-objective approaches have. During the past years, in the area of multi-objective evolutionary optimization, a new MOEA based on decomposition called MOEA/D has been attracting much attention via a series of big successes since proposed by Li and Zhang[125]. The main idea of MOEA/D can be generalized in short: the original multi-objective optimization problem (MOP) is divided into a set of scalar sub-problems through a group of uniformly distributed weight vectors. Due to searching directions guided by even distributed weights, the diversity of the Pareto optimal solutions is ensured. Simultaneously, MOEA/D also provides another new yet excellent framework, which is large different from non-dominated sorting (NSGAII)[126], to develop general algorithm for multi-objective optimization. All these motivate us to bridge MOEA/D to optimizing intrusion detection systems (IDSs) in the smart grid network.

II. BRIEF REVIEW

A. Three Layer Structure

Smart grid is an intelligent network developed by many technologies so that often to be analyzed by a model consisting of three-layer structures, i.e., it is divided into three different layers, home area network (HAN), neighborhood area network (NAN) and wide area network (WAN), which gives us a clear frame of smart grid, because each layer has its own duty. All these three layers work together, providing us a smart grid that monitor and optimize the operations of all functional units from power generation to all the end-customers. The physical and attacks may seriously violate the generation, transmission and distribution of power system, the vulnerabilities of smart grid also allow adversaries commit cyber-attacks.

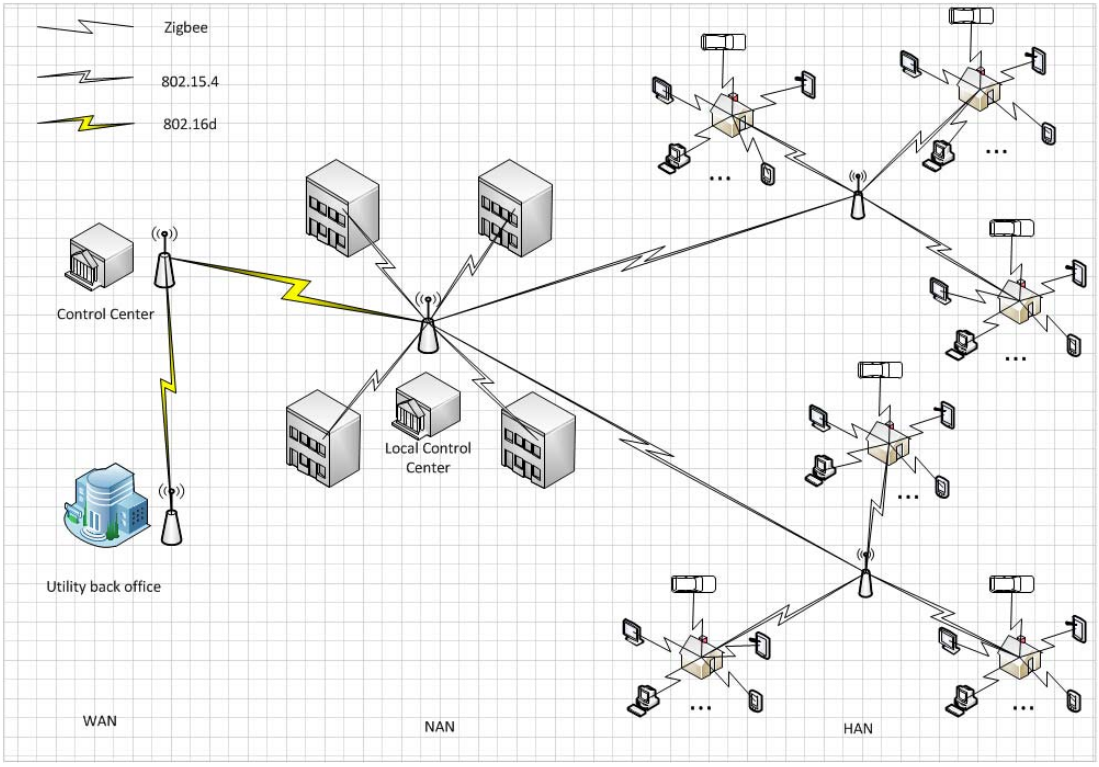

Figure 3-1. Three layer structure network

Generally, cyber-attacks can take place in any layers of smart grid. Vulnerable targets may include a series of components in advanced metering infrastructure (AMI), namely smart meters and access points in NAN, etc. Besides, cyber-attacks may also take advantage of accessibility through the HAN or NAN to attempt to remotely compromise, send fake data or control electronic resources. All of these would heavily disrupt power system, and our goals are determining the critical points in the network and using new technology on it to improve the security level of cyber-physical network.

B. Undirected Graph

A graph is a pair G = (V, E) of sets, the elements of E are 2-element subsets of V. To avoid notational ambiguities, we shall always assume tacitly that $V \cap E = \varnothing$. The elements of V are the vertices (or nodes, or points) of the graph G, the elements of E are its edges (or lines). The usual way to picture a graph is by drawing a dot for each vertices from an edge [127].

Giving any kind of network topologies, they can be abstracted into a graph. Considering the network for communications between two nodes is also bidirectional, so it always be put into an

undirected graph. For example, a three layer small network model which has 5 nodes in WAN, 20 nodes in NAN and 30 nodes in HAN can be abstracted as below:

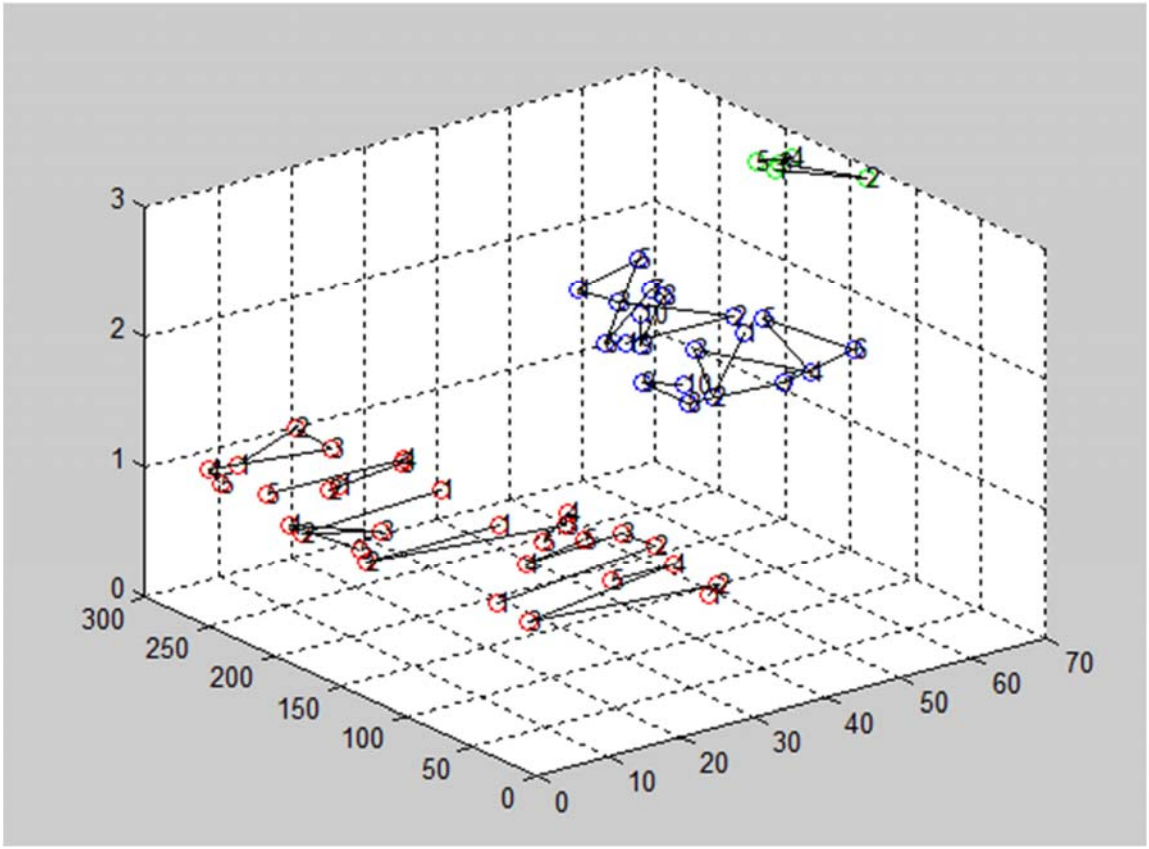

Figure 3-2. Three layer small network model

The optimization problem consists of an input network that represents a smart grid, the different terminals' connections (edges), and the each connection delays (weight).

D. NP-Hard Problem

To find the critical nodes by following certain constrains (multi-objective optimization) in this case is a NP-Hard Problem. NP-Hard (Non-deterministic Polynomial-time hard), means a set of problems that at least as hard as the hardest problems in NP. This NP-Hard conception is a computational complexity theory. In other words, a problem H is NP-hard when every problem L in NP can be reduced in polynomial time to H [128].That means, finding a polynomial algorithm to solve an NP-hard problem

would give polynomial algorithms for all the problems in NP, which is unlikely as many of them are considered as hard [129].

In our critical nodes case, first thing we need to do is calculate the degree on each edge. To do this, we should use communication methods and take several things into account, such as, power line carrier, radio, direct wired and fiber optic communications etc. Our main purpose is to divide the whole network into many domains.

III. MATHEMATICAL BACKGROUND

The state-of-the-art techniques include time-series methods such as ARIMA[130][131] and GARCH[132], and machine learning methods[133]. Among these techniques, machine learning models have shared the largest research attention mainly because of its strong nonlinear modeling capacity [134][135]. In the machine learning applications to electricity price prediction, there are generally two categories of learning algorithms as introduced below.

•The first is the conventional machine learning tools, for instance, ANN[136][137], SVM[134], etc. The best merit of such kind of approaches is that they can extract the nonlinear relationships out of the input and output dataset. They therefore have been developed and adopted widely in power engineering domain during past decades. However, the approaches fallen in this category are mainly to use some dull gradient-descent information to direct the training for their forecasting models, and they are often deemed as lacking efficient strategies to escape premature convergence or many local minima.

•The other is a novel approach proposed recently called Extreme learning machine (ELM)[138]. ELM and its variants have one common distinguished capacity, fast training speed. At the beginning, they initialize hidden nodes randomly and then obtain the output weights via Moore-Penrose pseudo inverse[138] method, i.e. the output weights vector is treated as one solution of a group of linear-like equations. For many ordinary regression or classification problems being in low dimensionality, this kind of method is obviously enough to obtain better results than those traditional ones in respect both of training speed and training accuracy.

However, as for high dimensional problems, the inputs need to be considered with more characters than the ordinary ones. As we observed in our previous works [139][140], ELM is sometimes difficult to find out a satisfied regression or classification results by once calculation, even though it can

calculate output weights fast. According to E-ELM [141], one random matrix of hidden weights is corresponding to a vector of out-put weights, besides that, better hidden weights and output weights can lead to a lower root mean square error, that is, a better regression or classification result. So the hidden weights can be combined into a single row solution of the objective function of ELM, the optimum can be obtained after evaluating the solution individual and comparing with other solutions among whole population. As for E-ELM, self-adaptive evolutionary extreme learning machine (SaE-ELM)[142] is a representative method, which can obtain output weights for a single hidden layer feed-forward network (SLFNs) with some promising features. However, in respect to training high dimensional data, SaE-ELM is also time-consuming in evolutionary iterations and seems a bit exhausted. For example, let the data is 100 dimensions and the number of the hidden layers is 10, the dimensionality of the solution individual will then reach 1000. Usually, dimensionality of the power market data or the data for electricity load forecasting is over 100. Hence, faster convergence and better quality of solution are two mandatory objectives should be considered.

As mentioned above, in conventional neural network, the gradient information provides some rapid exploring guides though often leading to local optima. This motivates us that gradient information perhaps can be properly used in E-ELM to provide some rational directions to accelerate the whole optimization procedure. But the complicated objective function of E-ELM is too difficult to mine the gradient information directly and the basic framework of ELM seems to have pushed the gradient approaches out of date. Therefore, a new simple model composing an approximate mapping to simulate the old functional relationship of E-ELM within a comparative small region is proposed. Based on the new model, a hybrid DE algorithm is developed to ensure that the new E-ELM not only obtains global optima, the weights, more reliably than those dull gradient methods, but also inherits the rational searching features simultaneously, that is, the new algorithm can approach global optimal region faster than pure stochastic tools while keeping high level quality of the solutions. Thus it can be seen that the reliability of greedy means and their variants becomes a less crucial problem, i.e., they are no more the patent of local optimum or premature convergence, on the contrary, their fast convergence becomes more attractive as long as with a well-design scheme .

A. Extreme Learning Machine (ELM) [138]

ELM has been shown many good performances on the generalized single-hidden layer feed-forward networks (SLFNs) since it was proposed. It has some differences from the traditional neural

networks on the hidden layer, e.g. random generation of its hidden nodes is the main feature of ELM. The basic working mechanism of ELM is briefly generalized as follows,

Given N training samples$\{(x_i, t_i)\}_{i=1}^{N}$which can be also described in matrix style$\{(P, T_{tar})\}$, where P is a $D \times N$ real matrix of input data and T_{tar} represents $N \times 1$ target vector. H is a $L \times D$ real matrix consisting of the hidden layer parameters generated randomly. β is a $L \times 1$ real vector of output weights. Their mathematical relationship can be expressed as Eq.(1)

$$f(H \cdot P + Bias)^{\mathrm{T}} \cdot \beta = T_{tar} \qquad (1)$$

where $Bias$ is a $L \times N$ real matrix and function $f(\cdot)$ is a kind of activation functions[135], for instance, a log-sigmoid function,

$$\sigma(t) = \frac{1}{1+e^{-c \cdot t}} \qquad (2)$$

where c is a slop parameter.

Usually, Eq.(1)can be presented in brief as Eq.(3)

$$\mathrm{H} \cdot \beta = T_{tar} \qquad (3)$$

where $\mathrm{H} = f(H \cdot P + Bias)^{\mathrm{T}}$is a $N \times L$matrix. EML uses Moore-Penrose pseudoinverse $\widehat{\mathrm{H}}^{\dagger}$ and target vector T_{tar} to obtain a least-square solution of such linear system as Eq.(3). That is, a least-square solution of output weight vector β can be analytically determined as Eq.(4)

$$\hat{\beta} = \widehat{\mathrm{H}}^{\dagger} \cdot T_{tar} \qquad (4)$$

where

$$\widehat{\mathrm{H}}^{\dagger} = \begin{cases} \mathrm{H}^{\mathrm{T}} \cdot \left(\frac{I}{C} + \mathrm{H} \cdot \mathrm{H}^{\mathrm{T}}\right)^{-1}, & N < L \\ \left(\frac{I}{C} + \mathrm{H}^{\mathrm{T}} \cdot \mathrm{H}\right)^{-1} \cdot \mathrm{H}^{\mathrm{T}}, & L < N \end{cases} \qquad (5)$$

More details can be referred to[138].

Instead of following traditional gradient descend approach, ELM minimizes training accuracy or the cost function Eq.(6) via the result gotten by Eq.(4).

$$RSME = \sqrt{mse(\mathrm{H} \cdot \hat{\beta} - T_{tar})} \qquad (6)$$

where $mse(\cdot)$ is the function to measure network performance as the mean of absolute errors.

B. Basic Differential Evolution Framework

Differential evolution (DE)[139] has been applied to many practical engineering problems since it was proposed in 1995. Furthermore, the variants of DEs with enhanced search performance have been introduced in literature [140][137]. Especially for multimodal optimization, researchers tend to combine DE with other evolutionary methods, sometimes called hybrid DEs, so as to promote whole performance of the algorithm.

In classical DE framework, the remarkably simple trial vector generation scheme is a main character distinguished from other EAs. It processes a scaled difference of vectors originating from a fixed-size population of decision vectors. Usually, three evolutionary operators are included that are mutation, crossover and selection respectively. During the g -th generation and in the basic DE mutation, a trial vector $u_{i,g}$ is produced by a crossover operation between old individual vector $x_{i,g}$ and a mutated vector $v_{i,g}=x_{r1,g}+F_i\cdot(x_{r2,g}-x_{r3,g})$, where $F_i>0$ is a scaling factor, $x_{r1,g},x_{r2,g},x_{r3,g}$ are three independent decision vectors selected randomly from the whole population $P=\{x_{1,g},x_{2,g},\ldots,x_{NP,g}\}$ in decision space. For each vector $x_{i,g}\in P$ in turn, there is a corresponding trial vector $u_{i,g}$ being generated. Each old vector $x_{i,g}$ in P will not be replaced unless its trial vector $u_{i,g}$ yields a better objective function value than itself. Thus $x_{i,g}$ is also called a target vector in literature. One can refer to [143] for more different crossover operators and more variants of DE in details.

C. SaE-ELM

Self-adaptive evolutionary extreme learning machine (SaE-ELM)[142] is upgraded from DE-LM[144] and E-ELM[141]. It chooses trial vector generation strategies and some relative control parameters adaptively. Their common place is to explore the network input weights and hidden node biases of ELM aiming to get optimum of the network output weights. When training data set $X_{D\times N}$, L hidden layers and an activation function $f(\cdot)$ are given, the individuals to be evolved during the g-th generation can be coded into as following vector[21],

$\theta_{k,g} = (h_{11}^g, \dots, h_{1D}^g, h_{21}^g, \dots, h_{2D}^g, \dots, h_{L1}^g, \dots, h_{LD}^g, b_1^g, \dots, b_L^g)$, where $1 \le k \le NP$, NP is the population size, $b_i^g, 1 \le i \le L$, represents the bias value for the i-th hidden layer in g generations.

Based on the coding format, the parameters like $H, Bias$ are obtained as follows,

$$H = \begin{bmatrix} h_{11}^g, \dots, h_{1D}^g \\ h_{21}^g, \dots, h_{2D}^g \\ \vdots \\ h_{L1}^g, \dots, h_{LD}^g \end{bmatrix}, P = X_{D\times N}, Bias = \begin{bmatrix} b_1^g \\ b_2^g \\ \vdots \\ b_L^g \end{bmatrix} \times J_{1\times N} \qquad (7)$$

where $J_{1\times N}$ is a one row and N columns matrix of ones. Then the corresponding fitness function is formulated as Eq.(8),

$$RSME = \sqrt{mse(f(H \cdot P_{test} + Bias)^{\mathrm{T}} \cdot \hat{\beta} - T_{test})} \qquad (8)$$

where P_{test} and T_{test} are testing data set and testing target vector respectively.

The main aim of such kind of algorithms is to explore an optimum of H from population consisted of $\theta_{k,g}$ $(1 \le k \le NP)$ during g_{max} generations. The individuals which can survive from g generations to the next must satisfy Eq.(9).

$$\theta_{k,g+1} = \begin{cases} u_{k,g}, & RMSE_{\theta_{k,g}} - RMSE_{\theta_{k,g+1}} > \varepsilon \cdot RMSE_{\theta_{k,g}} \\ u_{k,g}, & |RMSE_{\theta_{k,g}} - RMSE_{\theta_{k,g+1}}| < \varepsilon \cdot RMSE_{\theta_{k,g}} \\ & and \ \left\|\beta_{u_{k,g+1}}\right\| < \left\|\beta_{u_{k,g}}\right\| \\ \theta_{k,g}, & Otherwise \end{cases} \qquad (9)$$

IV. APPROXIMATION MODEL

Sometimes traditional optimization approaches are certified very useful for evolutionary exploring as long as they can be manipulated properly. However, in many situations, traditional optimization means cannot be adopted directly due to the complicated functional relationship. These stimulate a motivation to employee simpler approximation models to replace the original fitness function. As Figure 3-3 shown, in this section a simple first-order approximation model is proposed in order to imitate the compound mapping between variable data and their objective function. Perhaps, such kind of functional relationship based on the approximation model is not very accurate to replace the original one over whole hyper-plane, but within a limited region it can absolutely satisfy those practical demands[145].

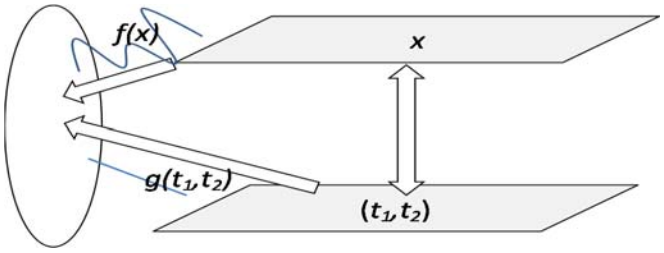

Figure 3-3. Principle of the approximation model

A. First-order Approximation Model

Without loss of generality, a decision space can be formulated as a hyper-plane by one point attached with two vectors. Let $x \in \mathbb{R}^n$ is an arbitrary point in decision space $\mathbb{R}^n$ or the point can be denoted as a decision vector $(x_1, x_2, \ldots, x_n)^{\mathrm{T}}$, L is the hyper-plane, suppose $x^0 \neq x^1 \neq x^2$ are three distinct points selected randomly among $\mathbb{R}^n$, then any arbitrary point $x \in L$ can be formulated as such style as Eq. (10)

$$x = x^0 + t_1 \cdot (x^1 - x^0) + t_2 \cdot (x^2 - x^0) \qquad (10)$$

where t_1, t_2 are two independent real variables.

According to Eq. (10), any $x \in L$is linear corresponding to the variable vector(t_1, t_2) because rest parameters are constants, i.e., $x \Leftrightarrow (t_1, t_2)$, if and only if three arbitrary yet independent points $x^0 \neq x^1 \neq x^2$ have been fixed. In other words, if $x^0 \neq x^1 \neq x^2$are located, any $x \in L$ can be evaluated based on variable vector (t_1, t_2) and Eq.(10). Therefore, when decision vector x approaches its optimum, x^*, there must exist a corresponding variable vector $(t_1^*, t_2^*) \Leftrightarrow x^*$, i.e.,

$$x^* = x^0 + t_1^* \cdot (x^1 - x^0) + t_2^* \cdot (x^2 - x^0) \qquad (11)$$

Likewise, for any pair of fitness function $f(x)$and its variable x, there has another pair of image $g(\cdot)$and its variable vector(t_1, t_2). Their common place is $g(t_1, t_2) = f(x)$, while the difference is the functional relationship of $g(\cdot)$ is simpler than the one of $f(\cdot)$. Fig.1 shows the principle of approximation model.

The conversion relationship between $g(\cdot)$ and $f(\cdot)$ is defined as Eq.(12)

$$g(t_1, t_2) = f(x) = g^0 + t_1 \cdot (g^1 - g^0) + t_2 \cdot (g^2 - g^0) \qquad (12)$$

where g^0, g^1, g^2, can be dealt with as constants if $x^0 \neq x^1 \neq x^2$ have been fixed as mentioned above.

In order to obtain the constants, g^0, g^1, g^2in a simple way, some special points are considered here. Assume (t_1, t_2) is substituted by vectors, (0,0), (1,0) ,(0,1) respectively, then $g^0 = f(x_0)$, $g^1 = f(x_1)$, $g^2 = f(x_2)$ can be easily extracted out via Eq.(12) and Eq.(10). Eq. (12) hereby provides an approximation equation as well to replace the original fitness function since $g(t_1, t_2) = f(x)$. So, nobody would like to care about how the complicated functional relationship between the decision variable $x \in \mathbb{R}^n$ and its original image$f(x)$ is, as long as the new mapping between $g(\cdot)$ and (t_1, t_2) is enough simpler.

B. Direction to Optimum

As pointed out before, Eq. (12) also provides a linear functional relationship between variable vector (t_1, t_2) and its image $g(t_1, t_2)$. Through conventional optimization theories, $g(t_1, t_2)$ at point (t_1, t_2) has a vector of first partial derivatives, or gradient vector $\nabla g(t_1, t_2) = ((g^1 - g^0), (g^2 - g^0))$. Hence, the local minimum optimum of (t_1^*, t_2^*) is most probably being placed in the opposite direction of $\nabla g(t_1, t_2)$,

$$(t_1^*, t_2^*) = (0,0) - \alpha \cdot \nabla g(t_1, t_2) = -\alpha \cdot \nabla g(t_1, t_2) \qquad (13)$$

where α is a step parameter. In one word, any three distinct decision variables,$x^0 \neq x^1 \neq x^2$, can deduce out the local optimum x^* via Eq.(11-13) , which can be expressed as Eq. (14),

$$x^* = x^0 - \alpha \cdot [(g^1 - g^0) \cdot (x^1 - x^0) + (g^2 - g^0) \cdot (x^2 - x^0)] \qquad (14)$$

V. PROPOSED ALGORITHM

In general, no method is flawless, neither is the new rational approximation model. Aiming to obtain a tradeoff between global exploration and local exploitation, another DE mutation strategies, 'DE/current-to-best/1'[146], is enrolled as well to construct a hybrid rational and self-adaptive mutation strategy named RSM mutation just as shown in Figure 3-4.

function RSM-Trial()
input: $x_{r0,g} \neq x_{r1,g} \neq \hat{x}_{r2,g}, x_{i,g}$, $x_{best,g}^{P}$ (one of the P best individuals in current population, P=5 in this paper)
output: two trial vectors $u_{i,g}^{1}, u_{i,g}^{2}$
$g^0 = f(x_{r0,g}); g^1 = f(x_{r1,g}); g^2 = f(\hat{x}_{r2,g})$;
$t_1 = -(g^1 - g^0)$; $t_2 = -(g^2 - g^0)$;
$s = Step_{i,g}/\sqrt{t_1^2 + t_2^2}$;
$v_{i,g}^{1} = x_{r0,g} + s \cdot [t_1 \cdot (x_{r1,g} - x_{r0,g}) + t_2 \cdot (\hat{x}_{r2,g} - x_{r0,g})]$;
$v_{i,g}^{2} = x_{r0,g} + F_i \cdot (x_{best,g}^{P} - x_{i,g}) + F_i \cdot (x_{r0,g} - x_{r1,g})$;
for j =1 to D
for k =1 to 2
if($j = k_{rand}$) or $rand(0,1)$ <CR_i^k
$u_{j,i,g}^{k}$=$v_{j,i,g}^{k}$
else
$u_{j,i,g}^{k}$=$x_{j,i,g}^{k}$
end if
end for
end for
end func

Figure 3-4. Pseudo-code of producing hybrid trial vectors

A. Historical Pool

From experimental results, fitness values evaluated by the new approximation model are very sensitive to the shape formed by three input individuals $x_{r0,g}$, $x_{r1,g}$ and $x_{r2,g}$. The basic idea is to avoid excessive similarity between the candidates. Learn from JADE[26], RSM mutation applies a historical pool to temporarily reserve a part of individuals sifted out from the population. Each time, one of three distinct individual is picked out the union of current population and the historical pool, hereby denoted by $\hat{x}_{r2,g}$, while the others $x_{r0,g}$, $x_{r1,g}$ are still selected from the current population. The size of the historical pool is set to a quarter of the population and the initial state is empty. After being full, the pool permits the individual perished from current population to replace the worst one if the perished one is better.

B. Self-Adaptive Parameters

Motivated by [147][148], in the new algorithm many control parameters are extended into solution individuals for controlling self-adaptively. The parameters are evolved simultaneously whilst the classical population of solutions is being processed in evolution procedure.

In general, the better control parameter value is corresponding to the optimal trial vector. Therefore the proposed algorithm utilizes the statistical results of recent successful parameters to guide the production of parameters for next generation.

Main parameters for self-adaptive control, such as $Step_{i,g} \in [0,2]$, $CR_i^1, CR_i^2 \in [0,0.9]$ and $F_{i,g} \in [0.1,1.0]$, are initialized within their definition domain. The successful parameters survive to the next generation, while the unsuccessful ones are replaced by a normal distribution of the mean$P_{m,g}$ and standard deviation $sigma$ as shown in Eq. (15).

$$P_{i,g} = P_{m,g} + sigma \cdot randn_{i,g} \qquad (15)$$

where $P_{i,g}$ represents the variable of parameters for the i-th individual in g generation. The sigma of each parameter equals to $\min(|P_{m,g} - P_{Ub,g,}|, |P_{m,g} - P_{Lb,g}|)$. The mean values are initialized as follows, $Step_{m,1} = 1.1$, $F_{m,1} = 0.6, CR_i^k = 0.6$,$(k = 1,2)$. Parameter $Step_{i,g}$ controls the incremental degree of the mutation shown in Figure 3-4.

$v_{i,g}^1 = x_{r0,g} + s \cdot \left[t_1 \cdot \left(x_{r1,g} - x_{r0,g}\right) + t_2 \cdot \left(\hat{x}_{r2,g} - x_{r0,g}\right)\right]$, where $s = Step_{i,g}/\sqrt{t_1^2 + t_2^2}$. At the beginning of whole evolving procedure, $Step_i \geq 1$ helps population converge to optimum fast, while $Step_i < 1$ is good at effective exploitation, especially for solutions approaching to the optimum.

C. Hybrid Strategy for Trial Vector

In the procedure of selection, as shown in Figure 3-5, if two new trail vectors satisfies

Case 1: $f(x_{i,g}) < f(u_{i,g}^1) < f(u_{i,g}^2)$

Both two trail vectors are successful trail ones , i.e., success(i,1)=1, success(i,2)=1, all their parameters can be kept to the next generation.

Case 2: $f(u_{i,g}^1) < f(x_{i,g}) < f(u_{i,g}^2)$

$u_{i,g}^1$ is named as a successful trail vector and success(i,1)is set to 1.

Case 3: $f(u_{i,g}^1) < f(u_{i,g}^2) < f(x_{i,g})$

This case means all the parameters need to be adjusted. As similar as above, the converse is also followed the rules.

At end of each generation, the mean of each parameter is adjusted by Eq. (16)

$$P_{i,g+1} = 0.85 \cdot P_{m,g} + 0.15 \cdot mean(P_{success,g}) \qquad (16)$$

where mean(.) is a function of arithmetic mean.

D. RSM-DE algorithm

The main body of RSM-DE algorithm:

Input: *NP*: the size of the population;

Maxgen: the number of the maximum iteration;

Fitness function;

D: The dimension of decision space.

Output: Optima of the fitness function.

Step 1 Initialization

Create a random initial population$\{x_{i,0} | i = 1, \dots, NP\}$. Initialize parameters within their definition regions.

For $g = 1, \dots, Maxgen$, do

Step 2 Evolution Items

For $i = 1, \dots, NP$ do

Step 2.1 New Parameters Generating: Unsuccessful parameters are refreshed based on Eq.(15).

Step 2.2 Mating: One of the P best individuals and other three independent individuals, $x^P_{best,g}, x_{r0,g} \neq x_{r1,g} \neq \hat{x}_{r2,g}$, are picked out. $\hat{x}_{r2,g}$ is from the union of current population plus historical pool and $x^P_{best,g}$ is one out of from current population, *P=5*.

Step 2.3 Call Function RSM-Trial(): To produce two trail vectors by two strategies respectively.

Step 2.4 Call Function Selection(): To select successful trail vectors and parameters into the next generation.

Step 2.5 Renew Historical Pool: If the historical pool is not full then the eliminated individuals are pushed into the pool, otherwise the worst one in the pool is replaced when the eliminated on is better.

Step 2.6 Summarize the Statistical Result of Successful Trail Vectors: To evaluate the arithmetical mean value of each parameter by Eq. (16).

Step 3 Stopping criteria

When stopping criterion is satisfied, the algorithm stops here and outputs corresponding results. Otherwise, goes to Step 2.

E. RSM-DE-ELM

Given a set of training data, a set of testing data, a candidate range for L hidden layers and an objective function g(·), RSM-DE-ELM algorithm is summarized as following Figure 3-5. $RSM\_DE\_ELM(\cdot)$ represents a procedure to optimize ELM based on the RSM-DE algorithm. It returns the optimum of the net. $[L_1, L_2]$ is the candidate range and $Train, Test$ denote training set, testing set respectively.

```
function Optimal_Layer()
input: [L1,L2],Train,Test
output: Optimum of Lbest,Fitnessmin
m1 = RSM_DE_ELM(Train,Test,L1) ;
m2 = RSM_DE_ELM(Train,Test,L2) ;
while(L1!=round((L1+L2)/2+0.1) or
L1!=round((L1+L2)/2-0.1))
    m3 = RSM_DE_ELM(Train,Test,round((L2 + L1)/2 ));
if(m1>m2)
swap(m1,m2), swap(L1,L2);
endif
m2 = m3;   L2 = round((L1 + L2)/2);
if(m1>m2)
swap(m1,m2); swap(L1,L2);
endif
endwhile
Lbest = L1; Fitnessmin = m1;
End func
```

Figure 3-5. Pseudo-code of RSM-DE-ELM

VI. CASE STUDY

In this section, the proposed algorithm is applied to search critical points in a small network model (like Figure 3-2), which including 55 points. Its performance is also compared against other state-of-the-art algorithms.

A. Optimization Algorithm Description

Consider the small network model is a three-layer structure represented by three simple graphs G1, G2, G3. Each graph consists of a set $V(G_i)$ of nodes, a set of $E(G_i)$ of edges, a set of $W(G_i)$ of

weights(network delay etc.). An arbitrary node, an arbitrary edge and an arbitrary are marked as v, e and w. n_{ij} is the number of nodes in each graph G_i. We then have $v \in V(G_i)$, $e \in E(G_i)$ and $w \in W(G_i)$.

In order to enhance the security level of the network (smart grid or communication network), we divide each layer of the model into several domains to isolate the attacks or malfunctions within a certain area. The aim of this compartmentalization is to maintain the damage in each domain without affecting other parts of network. [122][124] give the different optimization strategies to solve the similar problems as our critical points searching problem. Both of them finalize the problem as a multi-objective optimization problem, which can be improved by using the algorithm we proposed in this chapter.

B. Experimental Results

For the second layer in a three-layer structure network (like Figure 3-2), consists of 20 nodes. The nodes are connected by edges as Figure 3-6, each edge has a weight which represents the distance and/or delay between nodes. Due to different traffic background, transmission distance and responding time of different transmission types, the delays of edges are various and are calculated outside the model. By using the self-adaptive DE frame discussed above following constrains described in [122], the result of critical points was marked in Figure 3-7.

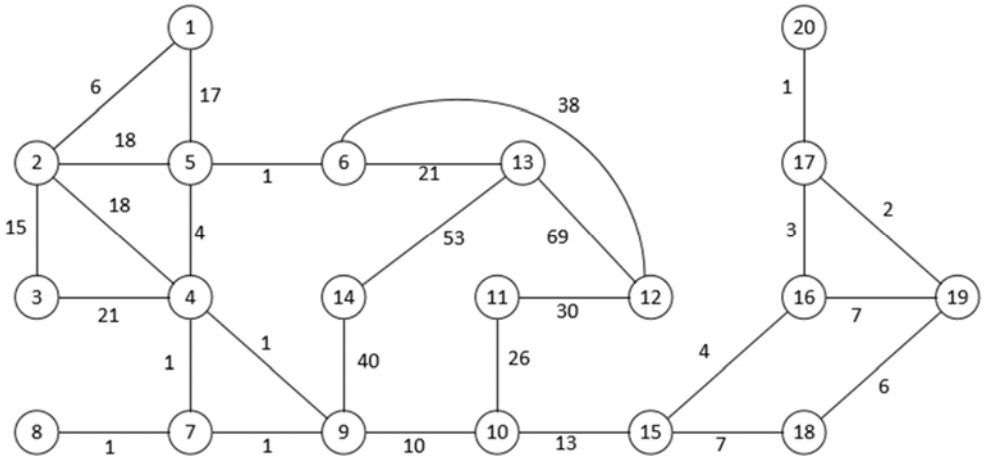

Figure 3-6. Layer 2 nodes connection graph

This optimization includes many constrains including the timing constrains, minimum number in each domain, the number of critical points and so forth. The results are different when we use different inputs.

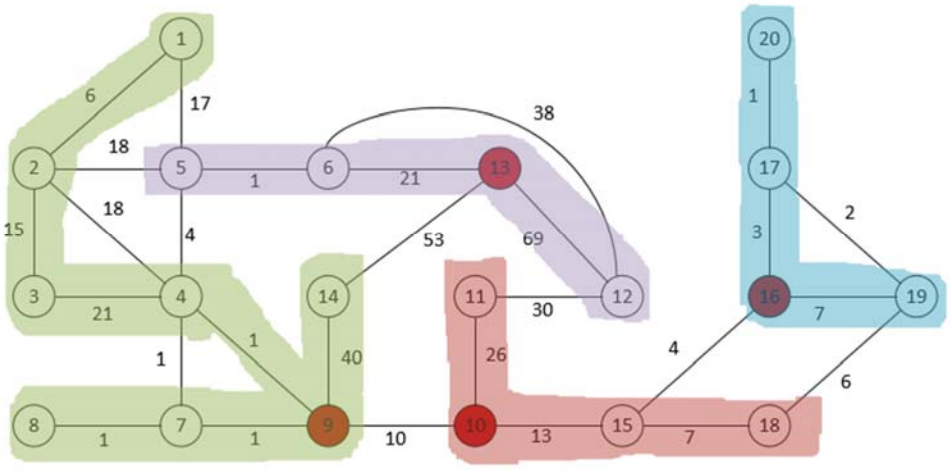

Figure 3-7. Result of domain division and critical points setting from Figure 3-6

Figure 3-7 gives us 4 critical points and the minimum number of each domain is 4.

VII. SUMMARY

A self-adaptive DE frame is proposed to solve the multi-objective optimization problem. A case study of critical points searching is presented in this chapter. Experimental results illustrate some mathematical auxiliary guides for evolving optima can bring optimization procedure more reliable performances than stochastic strategies do, as long as the design is a slight proper.

To make sure the stability and reliability of smart grid, a secure communication channel will be added between critical points for high level confidential information to be transmitted. A quantum cryptography based infrastructure will be described and potential applications will be proposed in Chapter 4.

Chapter 4. Quantum Cryptography

I. INTRODUCTION

The smart grid involves the interconnection among different types of networks, where the communication systems of a large number of small-scale networks are interconnected to form an integrated communication infrastructure covering large geographic areas [149]. Due to its heavy reliance on the cyber infrastructure for sensing and control, the smart grid will be exposed to new risks from computer network vulnerabilities as well as inherit existing risks from physical vulnerabilities in the power grid. Therefore, the smart grid today should have the ability of preventing cyber intrusions, which triggers the research area of cyber-physical security of the smart grid [150].

In the literature, there have some efforts been made to address the cyber-physical security of the smart grid, both in system architecture and analytical methods. [1] modeled the load redistribution attack behavior of the cyber attackers. It also analyzed its impact on the power system and discussed the protection strategies; [151] gave a comprehensive discussion on the smart grid cyber security requirements; [152] compared different SCADA cyber security standards and guidelines; [6], [153] proposed a cloud computing based information infrastructure to aggregate the big data in smart grid; [154] proposed a cloud-based bargaining model for the demand response to enhance the security and robustness of the communication process between the load aggregators and the utility; [155] modeled the false data injection attacks in power systems and analyzed their impacts on the power grids; [156] proposed a data-centric information platform to manage the information flow in the smart grid in a secure manner.

In the smart grid, tons of data are collected every day by the sensor infrastructure, and a large number of control instructions are transmitted. The information flows in the smart grid communication system always become a tempting target for cyber attackers. Once the sensitive information was eavesdropped by advisory, it might cause serious consequences, such as large-scale blackouts. Therefore, it is essential to ensure all data and instructions can be sent to their destinations effectively and precisely without any eavesdropping. The communication infrastructure of the current grid is potentially vulnerable to the eavesdroppers.

II. STATE-OF-THE-ART

A. Limitations of the Current Communication Infrastructure of the Smart Grid

The aim of the data cryptography is to design cryptography algorithms which are impossible or hard to break in practice by any adversary. So they are designed based on computational hardness assumptions. Modern cryptography techniques can be classified into two classes: public-key cryptography (asymmetric cryptography) and private-key cryptography (symmetric cryptography). The current communication infrastructure of the smart grid is based on the RSA architecture [157], which is the most widely used public-key cryptosystem. The RSA architecture is heavily based on the mathematical theory and computer science practice. The core of RSA is the hardness of factoring large numbers. The factoring problem has been studied for hundreds of years, but no efficient algorithm be found by now. The factoring assumption is truly hard, thus the RSA algorithms are considered to be safe for traditional computers.

However, the RSA architecture has been facing the challenges since the emergence of the quantum computing. In 1994, in his seminar paper, Peter Shor proved that quantum computers can make discrete logarithm operation [158], and the speed is far better than the traditional computer. Since Shor's algorithm shows that a quantum computer can crack RSA algorithm, the field of quantum computing has quickly drawn the world wide attentions. Theoretically, if the quantum computer can be constructed, then the RSA architecture will lose effectiveness.

B. Development of the Quantum Computer

In the latest years, the worldwide industrial and academic efforts have brought the quantum computer from theory to practice gradually.

In 2011, some researchers proved that a quantum computer can be made with a Von Neumann architecture [159]. In 2012, a research group in Australia made a great breakthrough by creating the first “quantum bit” based on a single atom in silicon [160]. It can be expected that such big progresses will bring the quantum computing into not only modern computers, but also laptops and mobile phones in a foreseeable future.

In the industry, the first commercial quantum computer named “D-Wave One” was launched by the D-Wave company in 2011. Afterwards, they have smoothly doubled the number of qubits each year,

and in 2013 they published the 512-qubit D-Wave Two system. Now D-Wave systems are being used to solve some pilot researches. For example, the National Aeronautics and Space Administration (NASA) of the U.S has been using the D-Wave One system to do the deep space exploration [161]. Google also plans to been using the quantum computer to do the big data mining [162].

With the potential risks of the current cryptography technologies and the development of the quantum computer, it is necessary to adopt a more robust cryptography technology to enhance the cyber-physical security of the smart grid. The quantum cryptography provides an ideal solution.

C. Development of the Quantum Cryptography

Since the first apparatus was set up and a remarkable experiment of point-to-point quantum key distribution (QKD) over short distance was performed successfully in 1989, quantum cryptography was no longer a theoretical method. After that, progress towards this technique has grown rapidly.

In the last decades, many important experiments have been conducted by the institutions and research groups all over the world. The first experimental quantum cryptography was performed in 1989 at the IBM Thomas J. Watson Research Centre, where the researcher established a 30cm long quantum channel [163]. In 1996, a group of the University of Geneva accomplished a quantum cryptography experiment. By using the fiber under Lake Geneva, they extended the distance to 23km [164]. After that, many experiments were further performed, such as the quantum cryptography on multiuser optical fiber networks by Townsend in Ireland [165], etc.

Some significant breakthroughs have also been achieved by the industrial companies. Toshiba has designed a quantum key distribution system to deliver keys through a fiber optics based network. It achieves the long-distance keys distribution aim and allows a standard fiber link to generate 100 256-bit keys in every second. Besides, it has been proven to be secure for all types of eavesdropping attacks [166]. The same efforts have also been made by IBM [167]. To bring quantum cryptography to reality, IBM developed its own quantum cryptosystem by using the standard telecommunication fibers, lasers and devices. In 2005, a fortnight-long, continuous quantum cryptograph system was designed by NEC [168]. It was successfully operated over a 16-km-long commercial optical network.

To sum up, the great successes of these breakthroughs show that it is meaningful and feasible to introduce the quantum cryptography into the smart grid operation in the near future.

III. QUANTUM CRYPTOGRAPHY

Just as the traditional computers operate the bit as the basic unit, the basic unit in the quantum computing is the quantum bit, or called 'qubit'. In the traditional communication, the bits are used to encode the information; in the quantum communication, the information is encoded as qubits. The Heisenberg's uncertainty principle is the fundamental of the quantum cryptography [164]. It declares that the more precisely the position of a particle is determined, the less precisely its momentum can be known, and vice versa. Therefore, it is impossible to assign exact simultaneous values to the position and momentum of a physical system simultaneously. These quantities can only be determined with some characteristic uncertainty, and any eavesdropping behavior will change the state of the qubits and disrupt the integrity of the transferred information.

Generally, there are two ways for an eavesdropper to intercept the keys: one is to measure the qubits during transmission and get the information directly. Since any kind of measurement will change the state of a quantum, the sender and receiver are easily to know whether the qubits are safe after their short communication. Another way to eavesdrop is to copy all the qubits (which is called quantum cloning) without measurement and send the original qubits to the receiver. In this way, the sender and receiver will not know the existence of the eavesdropper. However, quantum cloning is forbidden by the laws of quantum mechanics by the no cloning theorem, which means it is impossible to copy any quantum bit [169].

A. Photon Polarization Basis of the Quantum Cryptography

The first QKD protocol was proposed by Bennett and Brassard in 1984, which is called the BB84 protocol. Although several protocols (such as two-state protocol, six-state protocol, Ekert91 protocol, differential phase shift protocol, etc.) have been proposed in recent years, BB84 protocol is still the most popular protocol. The BB84 protocol is based on the polarization of photons. In the quantum computing, the possible values a qubit can have multiple values, which are referred to the basis. In the BB84 protocol, like the digital bits, a qubit has two possible values: 0 and 1. Table 4-1 illustrates the two different basis defined: horizontal-vertical basis (basis 1) and diagonal basis (basis 2).

Table 4-1. Basis in quantum key distribution

Basis	*0*	*1*
Horizontal-Vertical (0° and 90°)	*Vertical(90°)*	*Horizontal(0°)*
Diagonal directions (45° and 135°)	*45°*	*135°*

Key distribution is an essential part for both private-key cryptography and public-key cryptography. In private-key cryptography, both two parties which are participating information transmission need a shared key to encrypt and decrypt data. While in public-key cryptography, the distribution of public keys always be done by a public-key sever. The key distribution in the quantum cryptography is based on the polarizing of the light. At the start of the key distribution process, the light is polarized as one of the four directions (0°, 45°, 90° and 135°). On the horizontal-vertical basis, the vertical (0 degrees) polarization stands for value 0; the horizontal (90 degrees) polarization represents value 1. Similarly, on the diagonal basis, the 45° polarization means value 0, and 135° polarization signifies value 1.

B. Quantum Channel

The core of quantum cryptography is to generate keys to encrypt and decode information. BB84 protocol uses two fundamentally different communication channels to accomplish key distribution and information transmission: a classic channel and a quantum channel. The classical channel allows sender and receiver to send individual bits of information back and forth. The quantum channel behaves quite differently. Instead of transferring bits, the quantum channel transfers qubits.

In the sender side, the qubits can be generated by either of the two kinds of basis. These qubits can only be measured correctly by the same basis in the receiver side. For example, the horizontal-vertical basis can be used to read photons with 0 degree and 90 degrees, and gives the correct information (0 or 1) for receiver. But photons with diagonal directions are impossible to be read by the horizontal-vertical basis, so the receiver will get a value (0 or 1) randomly under the basis horizontal-vertical basis.

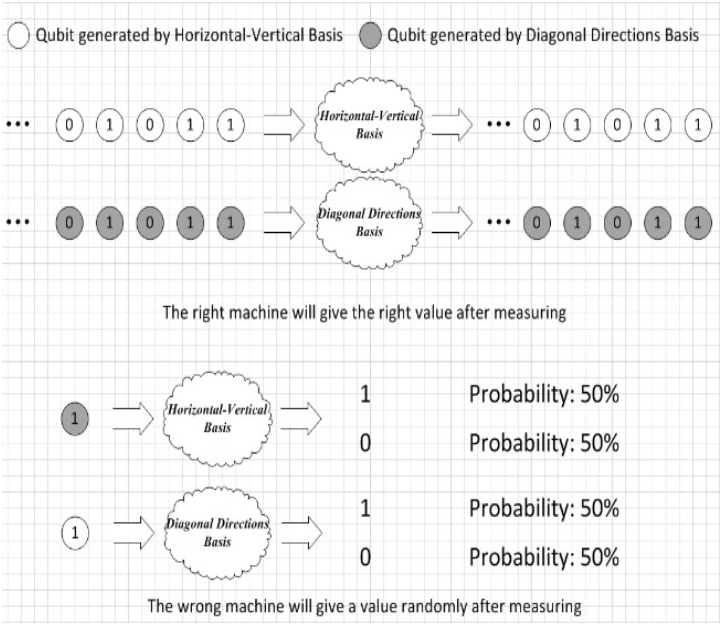

Figure 4-1. Quantum key distribution measurement

C. Quantum Key Distribution

The quantum key distribution begins with a sender sending a very large number of qubits to receiver over a quantum channel. Receiver records all the output (qubits) and measures each of them with two kinds of basis. Since the receiver does not know which process is used by the sender to generate the qubits, he or she will measure each qubit randomly. Generally the receiver has 50% success rate to choose the right basis to measure a qubit and get the right output. Otherwise, he or she will guess the wrong basis which gives a random guess on 1 or 0. In other words, even choosing a wrong basis, the receiver still has 50% chance to get the true values. Therefore, the total probability of getting incorrect values after measurements is 25% (50%*50%) on average. The percentage of correct outputs will be approximately 75% after the quantum communication, if there is no eavesdropping anywhere in the quantum channel. After measuring, the state of this specified qubit will be changed. If there is any eavesdropper intercepting the quantum bits before receiver, he or she must also make the random guess about which basis is the right one for measuring. Therefore, the eavesdropper also has 50% success rate to decode the qubits correctly.

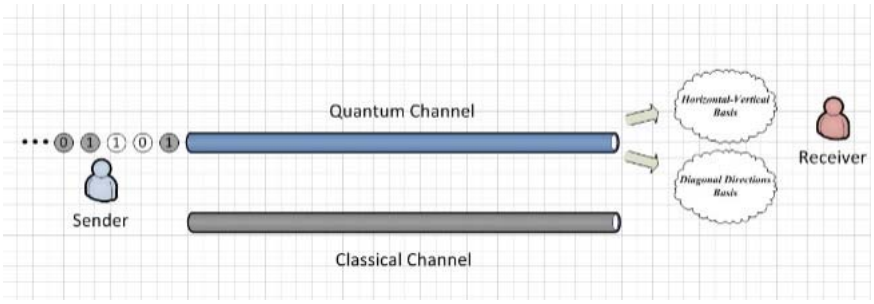

Figure 4-2. Quantum bits transmitted through quantum channel

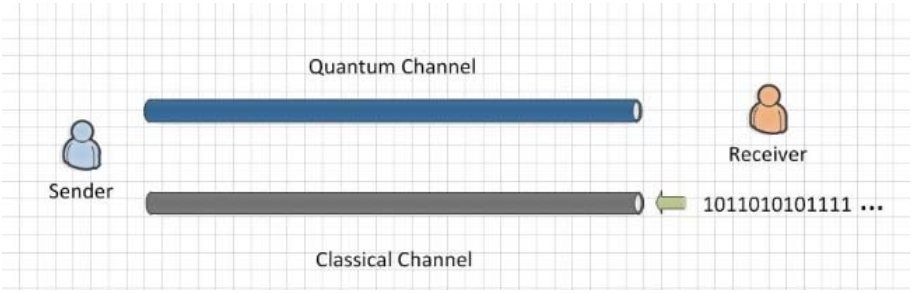

Figure 4-3. Communication through classical channel after qubits measurement

After the transmission of the qubits, the classical channel is turned on to do the eavesdropper detection. Firstly, the receiver sends a sequence of bits by the classical channel to tell the sender what basis he or she used to decode each qubit. Since the receiver only has 50% success rate to decode the qubits correctly, after receiving all bits from the receiver, the sender crosses reference his or her private records and sends a string of bits to tell the receiver which bits the receiver should measure correctly. Then both of the receiver and the sender discard the bits which were measured by wrong basis.

By receiving the response from the sender, the receiver chooses a subset of bits and compares them with the bits sent by the sender. If the bits have an accuracy of 100%, the communication was secure. Then both of them can use the remaining bits to form a secure key that is known only by them and encrypt further communication. If the bits have an accuracy rate under 100%, then they will be informed that an eavesdropper exists in somewhere of the channel.

In this way, a perfectly secure key can be generated that is known by nobody else except them.

D. Case Demonstration

In this section, we use a simulation program to demonstrate the quantum cryptography process.

1) Quantum Channel Communication

Firstly, the sender records the entire basis he or she used as alphabet. Then the receiver records the entire basis he or she randomly guessed as an alphabet, too. The procedure is shown as follows:

Stage 1: Quantum channel: Quantum Bits Communication

>>Qubits sent from sender represent:

>>1000110011001100100000110001010100011000010010100010110000100001100111110100100101101010100011101…

>>Qubits received by receiver represent:

>>1110001110111000111000000000011010011011110011111010100001100010010001100101010001100101000111101…

The bits received by the receiver are different from those sent by the sender, because the alphabets they use are different. Similarly, the random guess will also be made by the potential eavesdroppers, qubits an eavesdropper may get are shown as below:

>> Qubits received by eavesdropper represent:

>>1001101100011000110000010001010100011001010011110010110101100011100101111100110001110101001001110 0…

After this, the stage 1 of the QKD is completed. Quantum channel can be closed.

2) Cross Reference

In stage 1, the quantum bits are transmitted in the quantum channels. In stage 2, two participants communicate through the classical channel and cross reference some basis they used.

Stage 2: Classical channel: Cross Reference Basis

>> Sender's basis:

>>0111100010001001001010111101011001011111110000100011110010000110011100010110110110011101100010101…

>>Receiver's basis:

>>1001111011110011111001010011010111111000011110011010011011010111000010000000101100100010100000001101…

>>Eavesdropper's basis:

>>01100111010111110100100010000110011011101101110100111001110010001111101111101000010111100110111100…

We list all three alphabets (basis) here. But in practice, the alphabets will never be illustrated as above.

3) Calculation

After the communication, the sender and receiver know which bits they should end up with the same value. The quantum key distribution enters the final stage.

Stage 3: Calculating Error Rate

>> The length of key is: 92

>>The number of test key is: 39

>>The number of error bits is: 15

>>The error rate is 0.384615

>>Eavesdropper is detected!

>>Quantum key distribution failed!

If there is any eavesdropper, the results will be shown as above, and the quantum key distribution for this time will fail. The key may not safe. If there is no eavesdropper, the results would be as follows:

>> The length of key is: 90

>>The number of test key is: 42

>>The number of error bits is: 0

>>The error rate is: 0

>>Quantum key distribution is successful!

>>The final key for sender is:

>>0100000000001000101010111011101111…

>>The final key for receiver is:

>>0100000000001000101010111011101111…

IV. POTENTIAL APPLICATIONS IN SMART GRIDS

The quantum based cryptography can re-build the communication infrastructure of the smart grid and enhance the robustness of the grid operations. A large number of power grid applications can be developed on the quantum based cryptograph technology.

A. Power Market Operation

The power market in a smart grid is a highly deregulated environment where various parties are communicated and collaborated. Parties of the power market exchange their relevant data to enable the joint decision-making process. For example, generation companies will submit their bids to the Independent System Operator (ISO).

There is strong incentive of ensuring the data security and integrity during the communications. On one hand, the data involved in the communication might be the private data of the power market participants, and they would not want to disclose it to a third party. For example, the bids submitted by the generation companies might include the generation capacity and the bidding prices, which could be regarded as the private data of the generation company. If one of the generation company could eavesdrop the bidding information of the other companies, then it might raise the electricity price of the power market deliberately by using a certain of improper bidding strategy. Another case could be that if a cyber-attacker eavesdropped bidding data of the generation companies, it could obtain improper benefits from the power market by trading the option.

By employing the quantum based cryptograph technology, the data security of the power market can be enhanced from the infrastructure level and the operation of the power market can be ultimate robust since there is no opportunity for the cyber attackers to eavesdrop the confidential data of the market parties.

B. Demand Side Management

With the wide deployment of the smart meters and the distributed generation, the distribution system of a smart grid will continuously generates a huge number of data. How to aggregate and manage the big data in an efficient and secure manager will be a big challenge of the demand side management.

An important area of the demand side management is the microgrid operation and control. A microgrid can aggregate the distributed resources such as renewable energy sources, interruptible loads, battery energy storage systems, etc. The microgrids can also act as the generation companies to participant in the power market, which are often referred to the virtual power plants (VPPs) [170]. The operation of the microgrids heavily rely on the forecast of the sustainable energy (such as wind and solar), which is often based on the real-time wind or solar data collected by the sensors. By knowing the installed power of the microgrids, a cyber-attacker can easily estimate the generation capacity of the VPPs by eavesdropping the transferred sustainable energy data. Furthermore, a cyber-attacker may distort the sustainable energy data collected by the sensors by injecting some false data to mislead the day-ahead scheduling of the microgrids.

Another critical aspect of the demand side management in a smart grid is the load control. There are often two approaches: the demand response (DR) [171] and the direct load control (DLC) [172]. In the DR, the end customers will respond the incentive mechanisms provided by the utility actively to adjust the energy consuming pattern. In the DLC, the utility will control the end loads actively to achieve some objective, such as re-shaping the system load profile, while minimizing the disruption of the end users. In either approach, the end users need to communicate with the utility to exchange some private information (such as the load information, customers' personal information, the incentive price, etc.). Since there will be a large number of end users involving in the communications, obviously the data security and integrity will be the primary requirements.

Based on above analysis, it can be expected that the quantum based cryptograph technology can be employed to effectively ensure the communication security and integrity of the demand side management in the infrastructure level.

C. Wide Area Control of the Power Grid

Along with the development of the smart grid and the rapid development of the new measurement technology, such as PMUs and the AMI, the wide area control of the power grids are facing higher risks from the cyber attackers.

A cyber-attacker may attack the control loops of the power grid to disturb the wide area control and operation of the grid. For example, the grid's state estimation is an important part of the operation of the power grid. Many applications, such as the contingency analysis and control, are based on this

estimated grid state. There have been many studies [155], [173] show that a cyber-attacker can eavesdrop the data transferred from the sensors and then inject some false data to escape from the detections of the attack detection devices. These false data injection will lead to inaccurate grid state estimation and finally result in the incorrect control actions.

Another example is that a cyber-attacker can get the system load level by eavesdropping the communication channels between the control center and the sensors, and then distort the load data. This will force the control center to make incorrect economic dispatch strategies. The improper dispatch strategies will finally lead to imbalance of the generation power and load, threaten the grid stability, and incur some extra costs to the utility.

V. SUMMARY

In this chapter, the feasibility of applying the quantum cryptography to enhance the cyber-physical security of future smart grid is discussed. By introducing quantum key distribution, secure keys can be generated and used to encrypt and decrypt data, thus the confidentiality of data can be well maintained during transmission. Based on this, this chapter highlights some potential applications of the quantum cryptography technology on cloud-based smart grid. This chapter gives some general discussion about how the quantum cryptography can enhance the data security and integrity of the power market operation, demand side management, and grid wide area control. Works on a quantum cryptography based secure collaborative framework for the direct load control in the smart grid is currently under development.

Chapter 5. Conclusions and Future Work

I. CONCLUSIONS

Our world has entered the new phase of development, technologies (such as artificial intelligence, sensors, robotics etc.) are following exponential growth. Successful applications and new approaches have been applied to enhance the performance of smart grid. As the world's largest cyber-physical system, there is reason to believe that the future smart grid must be more powerful, efficient and reliable to meet the requirements of the future society.

Technology has been changing every detail of our lives. In the future, we will live in a world that is fully connected. It will also bring new functions to the future grid. Tons of data will be collected, transmitted, managed and studied to monitor and control the grid's operation. The integrity and security of data is foundation of a reliable power grid.

This research emphases the importance of the big data opportunity for future smart grid and gives new approaches to handle the big data transmission, storage and management problems. It also proposes a quantum cryptography based technology infrastructure to enhance the security level of future smart grid.

The contribution of this thesis can be summarized as follow:

- Summarize new emerging technologies which can be used in big data analysis and give potential case scenarios in smart grid.
- Critical points searching: a definition of critical points searching is proposed, and a method is designed to find the critical points.
- Quantum cryptography based cyber-physical infrastructure is designed for secure data transmission.

II. FUTURE WORK

Future work should include the development of quantum cryptography based secure collaborative framework, a completed application for critical points searching should be developed to simplify the process of getting network topologies and shorten the optimization span. More potential

scenarios which are suitable for cloud computing frame should be explored. Technical limitations of big data management by using cloud based frame should be gradually eliminated.

Reference

[1] Y. Yuan, Z. Li, K. Ren, “Quantitative analysis of load redistribution attacks in power systems,” IEEE Transactions on Parallel and Distributed System, vol. 23, no. 9, Sep. 2012.

[2] W. Meng, R. Ma, H. Chen, “Smart grid neighborhood area networks: a survey,” Network, IEEE vol. 28, no. 1, pp. 24-32, 2014.

[3] S.M. Amin and B.F. Wollenberg, “Toward a smart grid: power delivery for the 21st century,” IEEE Power and Energy Magazine, vol. 3, no. 5, pp. 34-41, Sep. 2005.

[4] J. Giri, D. Sun, and R. Avila-Rosales, “A more intelligent grid,” IEEE Power and Energy Magazine, vol. 7, no. 2, pp. 34-40, 2009.

[5] Y. Liu and P. Ning, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 13, May. 2011.

[6] F. Luo, Z.Y. Dong, Y. Chen, Y. Xu, K. Meng, and K.P. Wong, “Hybrid Cloud Computing Platform: The Next Generation IT Backbone for Smart Grid”, Proc. IEEE PES General Meeting, San Diego, California, USA, Jul. 2012.

[7] H. Kim, Y. Kim, K. Yang, and M. Thottan, “Cloud-based demand response for smart grid: architecture and distributed algorithms,” Proc. International Conference on Smart Grid Communications, 2011.

[8] Y. Kim, M. Thottan, V. Kolesnikov, and L. Wonsuck, “A secure decentralized data-centric information infrastructure for smart grid,” IEEE Communications Magazine, vol. 48, no. 11, pp. 58-65, 2010.

[9] I. Foster, Y. Zhao, and I. Raicu, etc, “Cloud computing and grid computing 360-degree compared,” Grid Computing Environments Workshop, Austin, pp. 1-10, 2008.

[10] R. Buyya, J. Broberg, and A. Goscinski, Cloud Computing: Principles and Paradigms. Wiley, Feb. 2011.

[11] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, “Recent advances in homomorphic encryption: a possible future for signal processing in the encrypted domain,” IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 108-117, Mar. 2013.

Reference

[12] R. Pibernik, Y. Zhang, F. Kerschbaum, and A. Schropfer, “Secure collaborative supply chain planning and inverse optimization—the JELS model,” European Journal of Operational Research, vol. 208, no. 1, pp. 75-85, Jan. 2011.

[13] J. Dean and S. Ghemawat, “MapReduce: simplified data processing on large clusters,” Communications of the ACM, vol. 51, no. 1, pp. 107-113, Jan. 2008.

[14] S. Ratnasamy, B. Karp, S. Shenker, “Data-centric storage in sensornets with GHT: a geographic hash table,” Mobile Networks and Applications, vol. 8, no. 4, pp. 427-442, Aug. 2003.

[15] B. Karp and H. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” Proc. 6th Annual International Conference on Mobile Computing and Networking, 2000.

[16] S4: Distributed Stream Computing Platform [online], Available: http://incubator.apache.org/s4/

[17] Storm: Distributed and Fault-Tolerance Real Time Computation [online], Available: https://storm.apache.org/

[18] StreamBase [online], Available: http://www.streambase.com/

[19] R. Cheng, D. Kalashnikov, and S. Prabhakar, “Evaluating probabilistic queries over imprecise data,” in Proc. ACM SIGMOD, 2003.

[20] J. Chen and R. Cheng, “Efficient evaluation of imprecise location-dependent queries,” in Proc. IEEE 23rd International Conference on Data Engineering, 2007.

[21] M. Chau, R. Cheng, B. Kao, and J. Ng, “Uncertain data mining: an example in clustering location data,” Lecture Notes in Computer Science, vol. 3918, pp. 199-204, 2006.

[22] W. Ngai, B. Kao, C. Chui, R. Cheng, M. Chao, and K. Yip, “Efficient clustering of uncertain data,” in Proc. 6th International Conference on Data Mining, 2006.

[23] S. Tsang, B. Kao, K. Yip, W. Ho, and S. Lee, “Decision trees for uncertain data,” IEEE Transactions on knowledge and data engineering, vol. 23, no. 1, pp. 64-78, Jan. 2011.

[24] D. Ming, P. Meira, X. Wilsun, and C.Y. Chung, “Non-intrusive signature extraction for major residential loads,” IEEE Transactions on Smart Grid, vol. 4, pp. 1421-1430, 2013.

Reference

[25] A. Reinhardt, P. Baumann, D. Burgstahler, M. Hollick, H. Chonov, M. Werner, and R. Steinmets, “On the accuracy of appliance identification based on distributed load metering data,” Sustainable Internet and ICT for Sustainability, 2012.

[26] Energy Australia [online], Available: http://www.energyaustralia.com.au/

[27] B. Ramanathan and V. Vittal, “A framework for evaluation of advanced direct load control with minimum disruption,” IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1681-1688, Nov. 2008.

[28] G. Chalkiadakis, V. Robu, R. Kota, A. Rogers, and N. Jennings, “Cooperatives of distributed energy resources for efficient virtual power plants,” in Proc. 10th International Conference on Autonomous Agents and Multi-agent Systems, 2011.

[29] A vision for the modern grid, [online].

Available:http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Whitepaper_The%20Modern%20Grid%20Vision_APPROVED_2009_06_18.pdf

[30] S.M. Amin and B.F. Wollenberg, “Toward a smarg grid: power delivery for the 21st century,” IEEE Power and Energy Magazine, vol. 3, no. 5, pp. 34-41, Sep. 2005.

[31] H. Farhangi, “The path of the smart grid,” IEEE Power and Energy Magazine., vol. 8, no. 1, pp. 18-28, Jan. 2010.

[32] J. Giri, D. Sun, and R. Avila-Rosales, “A more intelligent grid,” IEEE Power and Energy Magazine, vol. 7, no. 2, pp. 34-40, 2009.

[33] F. Luo, Z.Y. Dong, Y. Chen, E. Pozorski, J. Qiu, Y. Zheng, Y. Xu and K. Meng, “Constructing the power cloud data center to deliver multi-layer services for smart grid,” Proc. The 9th International Conference on Power System Control, Operations and Management (APSCOM), Hong Kong, 2012.

[34] B. Bitzer and E. Gebretsadik, “Cloud computing framework for smart grid applications,” Proc. Power Engineering Conference, 2013.

[35] A. Mohsenian-Rad and A. Leon-Garcia, “Coordination of cloud computing and smart power grids,” Proc. The 1st International Conference on Smart Grid Communications, 2010.

Reference

[36] S. Rusitschka, K. Eger, and C. Gerdes, “Smart grid data cloud: a model for utilizing cloud computing in the smart grid domain,” Proc. The 1st International Conference on Smart Grid Communications, 2010.

[37] H. Kim, Y. Kim, K. Yang, and M. Thottan, “Cloud-based demand response for smart grid: architecture and distributed algorithms,” Proc. International Conference on Smart Grid Communications, 2011.

[38] I. Foster, Y. Zhao, and I. Raicu, etc, “Cloud computing and grid computing 360-degree compared,” Grid Computing Environments Workshop, Austin, pp. 1-10, 2008.

[39] R. Buyya, J. Broberg, and A. Goscinski, Cloud Comptuing: Princi-ples and Paradigms. Wiley, Feb. 2011.

[40] OSI Model, available at: http://vlsm-calc.net/models.php

[41] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” Advances in Cryptology-EUROCRYPT, vol. 2045, pp. 453-474, 2001.

[42] D. Bleichenbacher, “Chosen cipertext attacks against protocols based on the RSA encryption standard PKCS #1,” Lecture Notes in Computer Science, vol. 1462, no. 1998, pp. 1-12, 2006.

[43] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," Journal of Cryptology vol.5, no. 1, pp. 3-28, Jan. 1992.

[44] Cloud Scheduler, [Online]. Available: www.cloudscheduler.org/

[45] S. Selvarani and G.S. Sadhasivam, “Improved cost-based algorithm for task scheduling in cloud computing,” Proc. International Conference on Computational Intelligence and Computing Research (CCIC), 23010.

[46] J. Tsai, J. Fang, and J. Chou, “Optimized task scheduling and re-source allocation on cloud computing environment using improved differential evolution algorithm,” Computers and Operations Research, vol. 40, no. 12, pp. 3045-3055, Dec, 2013.

[47] Y. Fang, F. Wang, and J. Ge, “A task scheduling algorithm based on load balancing in cloud computing,” Lecture Notes in Computer Science, vol. 6318, pp. 271-277, 2010.

[48] K. Li, G. Xu, G. Zhao, Y. Dong, and D. Wang, “Cloud task scheduling based on load balancing ant colony optimization,” Proc. 6th Annual Chinagrid Conference, 2011.

Reference

[49] Q. Cao, Z. Wei, and W. Gong, “An optimized algorithm for task scheduling based on activity based costing in cloud computing,” Proc, 3rd International Conference on Bioinformatics and Bio-medical Engineering, 2009.

[50] D. Ergu, G. Kou, Y. Peng, and Y. Shi, “The analytic hierarchy process: task scheduling and resource allocation in cloud computing environment,” The Journal Supercomputing, vol. 64, no. 3, pp. 835-848, May. 2013.

[51] Brocade Vyatta Virtual Router, [Online]. Available: http://www.brocade.com/products/all/network-functions-virtualization/product-details/5400-vrouter/index.page

[52] HP VSR1000 Virtual Services Router Series, [Online].

Available:http://h17007.www1.hp.com/us/en/networking/products/routers/HP_VSR1000_Virtual_Services_Router_Series/index.aspx

[53] S. Ghemawat, H. Gobioff, and S. Leung, “The Google file sys-tem,” Proc. 19th ACM Symposium on Operating Systems Principles, 2003.

[54] Q. Wei, B. Veeravalli, B. Gong, L. Zeng, and D. Feng, “CDRM: A cost-effective dynamic replication management scheme for cloud storage cluster,” Proc. 2010 IEEE International Conference on Cluster Computing, 2010.

[55] D. Sun, G. Chang, S. Gao, L. Jin, and X. Wang, “Modeling a dynamic data replication strategy to increase system availability in cloud computing environments,” Journal of Computer Science and Technology, vol. 27, no. 2, pp. 256-272, May. 2012.

[56] S. Ratnasamy, B. Karp, S. Shenker, “Data-centric storage in sensornets with GHT: a geographic hash table,” Mobile Networks and Applications, vol. 8, no. 4, pp. 427-442, Aug. 2003.

[57] B. Karp and H. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” Proc. 6th Annual International Conference on Mobile Computing and Networking, 2000.

[58] Dell Virtualization Management Solutions, [Online].

Available: http://software.dell.com/solutions/virtualization-management/

[59] RightScale, [Online]. Available: www.rightscale.com/

Reference

[60] VMWare Workstation, [Online]. Available: www.vmware.com/cn/products/workstation

[61] Google Cloud SQL, [Online]. Available: http://cloud.google.com/sql/

[62] Amazon EC2, [Online]. Available: http://cloud.google.com/sql/

[63] CloudFuzion, [Online]. Available: http://www.cloudfuzion.com/

[64] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters," Communications of the ACM, vol. 51, no. 1, pp. 107-113, Jan. 2008.

[65] Apache Hadoop, [Online]. Available: http://hadoop.apache.org/

[66] CloudBroker, [Online]. Available: http://cloudbroker.com/

[67] Cloudyn, [Online]. Available: http://www.cloudyn.com/

[68] Cloud Cruiser, [Online]. Available: http://www.cloudcruiser.com/

[69] Apache Storm, [Online]. Available: http://storm.apache.org/

[70] S4: Distributed Stream Computing Platform, [Online]. Available: http://incubator.apache.org/s4/

[71] StreamBase, [Online]. Available: http://www.streambase.com/

[72] R. Pibernik, Y. Zhang, F. Kerschbaum, and A. Schropfer, "Secure collaborative supply chain planning and inverse optimization—the JELS model," European Journal of Operational Research, vol. 208, no. 1, pp. 75-85, Jan. 2011.

[73] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: a possible future for signal processing in the encrypted domain," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 108-117, Mar. 2013.

[74] F. Luo, J. Zhao, J. Qiu, I. Foster, Y. Peng, and Z.Y. Dong, "Assessing the transmission expansion cost with distributed generation: An Australia case study," IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1892-1904, 2014.

[75] K. Meng, Z.Y. Dong, K.P. Wong, Y. Xu, and F. Luo, "Speed-up the computing efficiency of power system simulator for engineering based power system transient stability simulations," IET Generation, Transmission, and Distribution, vol. 4, no. 5, pp. 652-661, May. 2010.

Reference

[76] Yan Xu, Z.Y. Dong, Fengji Luo, Rui Zhang, and KitPo Wong, “Parallel-differential evolution approach for optimal event-driven load shedding against voltage collapse in power systems, ” IET Generation, Transmission and Distribution, vol. 8, no. 4, pp. 651-660, 2014.

[77] C.Y. Chung, H. Yu, and K.P. Wong, “An advanced quantum-inspired evolutionary algorithm for unit commitment,” IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1627-1636, Nov. 2008.

[78] Y. Zheng, Z.Y. Dong, F. Luo, K. Meng, J. Qiu, and K.P. Wong, “Optimal application of energy storage system for risk mitigation of DISCOs with high renewable penetrations,” IEEE Transactions on Power Systems, vol. 29, no. 1, pp. 212-220, 2014.

[79] J. Shu, W. Xue, and W.M. Zheng, “A parallel transient stability simulation for power systems,” IEEE Trans. Power Syst., vol. 20, no. 4, pp. 1709-1717, Nov. 2005.

[80] Google Cloud Datastore, [Online]. Available: http://cloud.google.com/datastore/?hl=zh-tw

[81] F. Luo, Z.Y. Dong, J. Zhao, X. Zhang, W. Kong, and Y. Chen, “Enabling the big data analysis in the smart grid, ” in Proc. IEEE PES General Meeting, 2015, to be published.

[82] C. Jensen and M. EI-Sharkawi, “Power system security assessment using neural networks: Feature selection using Fisher dis-crimination,” IEEE Transactions on Power Systems, vol. 15, no. 4, pp. 757-763, Nov. 2001.

[83] Data Analysis Australia, [Online]. Available: http://www.daa.com.au/home/

[84] T. Huang, X. Wang, L. Li, L. Zhou, and G. Yao, “Ultra-short term prediction of wind power based on multiple model extreme learning machine,” Advances in Neural Networks, vol. 6677, pp. 539-547, 2011.

[85] Y. Chen, Z.Y. Dong, K. Meng, F. Luo, W. Yao, and J. Qiu, “A novel technique for the optimal design of offshore wind farm electrical layout,” Journal of Modern Power Systems and Clean Energy, vol. 1, no. 3, pp. 258-263, 2013.

[86] F. Luo, K. Meng, Z.Y. Dong, Y. Zheng, Y. Chen, and K.P. Wong, “Coordinated operational planning for wind farm with battery energy storage system,” IEEE Transactions on Sustainable Energy, vol. 6, no. 1, pp. 253-262, 2015.

[87] M. Zeifman and K. Roth, “Non-intrusive appliance load monitoring: Review and outlook,” IEEE Transactions on Consumer Electronics, 2011.

Reference

[88] J. Zhao, Y. Xu, F. Luo, Z.Y. Dong, and Y. Peng, “Power system fault diagnosis based on history driven differential evolution and stochastic time domain simulation,” Information Sciences, vol. 275, pp. 13-29, 2014.

[89] J. Mjelde and D. Bessler, “Market integration among electricity markets and their major fuel source markets,” Energy Econ., vol. 31, no. 3, pp. 482-491, 2009.

[90] W. Yao, J. Zhao, F. Wen, Y. Xue, and G. Ledwich, “A hierarchical decomposition approach for coordinated dispatch of plug-in electric vehicles,” IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 2768-2778, 2013.

[91] H. Yang, D. Yi, J. Zhao, F. Luo, and Z.Y. Dong, “Distributed optimal dispatch of virtual power plant based on ELM transformation,” Journal of Industrial and Management Optimization, vol. 10, no. 4, pp. 1297-1318, 2014.

[92] Z. Zhou, F. Zhao, and J. Wang, “Agent-based electricity market simulation with demand response from commercial buildings,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 580-588, 2011.

[93] W, Wu, W. Qiu, K. Rustom, T. Kasparis, and I. Batarseh, “DSP-based multiple peak power tracking for expandable power system,” in Proc. IEEE IECON 22nd Int. Conf. Ind. Electron., Contr. Instrum., 1705-1710, 1996.

[94] T. Nagata, and H. Sasaki, “A multi-agent approach to power sys-tem restoration,” IEEE Transactions on Power Systems, vol. 17, no. 2, pp. 457-462, 2002.

[95] L. Lobos, and J. Rezmer, “Real-time determination of power sys-tem frequency,” IEEE Transactions on Instrumentation and Measurement, vol. 46, no. 4, pp. 877-881, Aug. 1997.

[96] F. Oldewurtel, A. Parisio, C. Jones, D. Gyalistras, M. Gweder, V. Stauch, B. Lehmann, and M. Morari, “Use of model predictive control and weather forecasts for energy efficient building climate control,” Energy and Buildings, vol. 45, pp. 15-27, Feb. 2012.

[97] Google Application Engine, [Online]. Available: http://code.google.com/intl/zh-CN/appengine/.

[98] D. Sanderson, Programming Google App Engine. O’Reilly, Nov. 2009.

Reference

[99] Y. Xu, Z.Y. Dong, L. Guan, R. Zhang, K.P. Wong and F. Luo, “Preventive dynamic security control of power systems based on pattern discovery technique”, IEEE Trans. Power Syst., vol. 27, no. 3, pp. 1236-1244, Aug 2012.

[100] F. Luo, Z.Y. Dong, Y. Xu, G. Chen, Y. Chen, K. Meng, and K.P. Wong, “Advanced pattern discovery based fuzzy classification method for power system dynamic security assessment,” IEEE Transactions on Industrial Informatics, vol. 11, no. 2, pp. 416-426, Apr. 2015.

[101] M. Sikonja and I. Kononenko, “Theoretical and empirical analysis of RelieF and RRelieF,” Machine Learning, vol. 53, no. 1, pp. 23-69, 2003.

[102] B. Ramanathan and V. Vittal, “A framework for evaluation of advanced direct load control with minimum disruption,” IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1681-1688, Nov. 2008.

[103] F. Luo, J. Zhao, Z.Y. Dong, X.J. Tong, Y. Chen, H. Yang, and H. Zhang, “Optimal dispatch of air conditioner loads in southern China region by direct load control,” IEEE Transactions on Smart Grid, early access.

[104] R. Storn and K. Price. “Differential evolution-A simple and efficient heuristic for global optimization over continuous spaces,” Journal of Global Optimization, vol. 11, no. 4, pp. 341-359 Dec. 1997.

[105] AMPL. Available at: http://ampl.com/

[106] P. Gunjal and S. Tamhankar, “Review of attack detection scheme for cyber physical security system,” International Journal of Computer Science and Mobile Computing, vol. 2, no. 12, pp. 401-405, Dec. 2013.

[107] Crypto Cloud Computing, [Online]. Available: http://research.microsoft.com/en-us/projects/cryptocloud/

[108] Quantum Direct Communication, [Online]. Available: http://cdn.intechopen.com/pdfs-wm/9861.pdf

[109] C. Lo, C. Huang, and J. Ku, “A cooperative intrusion detection system framework for cloud computing networks,” in Proc. 39th International Conference on Parallel Processing Workshops, 2010.

Reference

[110] K. Suresh and K. Prasad, “Security issues and security algorithms in cloud computing,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 10, 2012.

[111] W. Dou, Q. Chen, J. Chen, “A confidence-based filtering method for DDoS attack defense in cloud environment,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1838-1850, Sep. 2013.

[112] F. Lin, W. Zeng, Y. Jiang, J. Li, and L. Qi, “A group tracing and filtering tree for REST DDoS in cloud,” International Journal of Digital Content Technology and its Applications, vol. 4, no. 9, pp. 212-224, 2010.

[113] X. Yang, L. Ke, and W. Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics,” IEEE Trans. on Information Forensics and Security, vol. 6, no. 2, pp. 426-437, 2011.

[114] File Allocation Table, [Online]. Available: http://www.techopedia.com/definition/1369/file-allocation-table-fat

[115] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in Proc. Preprints of the 1st Workshop on Secure Control Systems, 2010.

[116] R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[117] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM), pp. 393-396, 2012.

[118] Y. Huang, H. Li, K.A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in Proc. IEEE 45th Annual Conference on Information Sciences and Systems (CISS), pp. 1-6, 2011.

[119] C. Thomas, T. Cui, and F. Franchetti, “Privacy preserving smart metering system based retail level electricity market,” Proc. Power and Energy Society General Meeting, 2013.

[120] A. Mohsenian-Rad and A. Leon-Garcia, “Distributed Inter-net-based load altering attacks against smart power grids,” IEEE Transactions on Smart Grid, vol. 2, no. 4, Dec. 2011.

Reference

[121] A. Mohsenian-Rad and A. Leon-Garcia, “Coordination of cloud computing and smart power grids,” Proc. 1st International Conference on Smart Grid Communications, 2010.

[122] J. M. C. Gonzalez, K. M. Hopkinson, G. H. Greve, M. D. Compton, J. Wilhelm, S. H. Kurkowski, and R. W. Thomas, “Optimization of trust system placement for power grid security and compartmentalization,” IEEE Trans. Power Syst., vol. 26, no. 2, pp. 550–563, 2011.

[123] R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: Requirements and architectural directions,” in Proc. 1st IEEE Int. Conf. Smart Grid Commun., Oct. 2010, pp. 350–355.

[124] Y. Zhang, L. Wang, W. Sun, R. C. Green, II, and M. Alam, “Distributed intrusion detection system in a multi-layer network architecture of smart grids,” IEEE Trans. SmartGrid, vol. 2, no. 4, pp. 796–808, 2011.

[125] Zhang Q, Li H. “MOEA/D: A multi-objective evolutionary algorithm based on decomposition,” IEEE Trans. on Evolutionary Computation, vol. 11, no. 6, pp. 712-731, 2007.

[126] Li H, Zhang Q. “Multi-objective optimization problems with complicated Pareto sets, MOEA/D and NSGA-II,” IEEE Trans. on Evolutionary Computation, vol. 13, no. 2, pp. 284-302, 2009.

[127] Diestel, Reinhard.”Graph Theory”. Edition 4. Springer. p. 2 ISBN: 9783642142789 P.

[128] Leeuwen, Jan van, ed. (1998). “Handbook of Theoretical Computer Science”. vol. A, Algorithms and complexity. Amsterdam: Elsevier. ISBN 0262720140. OCLC 247934368.

[129] Daniel Pierre Bovet; Pierluigi Crescenzi. “Introduction to the Theory of Complexity”. Prentice Hall. p. 69. ISBN 0-13-915380-2.

[130] J. Contreras, R. Espinola, F.J. Nogales, and A.J. Conejo, “ARIMA models to predict next-day electricity prices,” IEEE Trans. Power Syst., vol. 18, no. 3, pp. 1014-1020, Aug. 2003.

[131] A.J. Conejo, M.A. Plazas, R. Espinola, and A.B. Molina, “Day-ahead electricity price forecasting using the wavelet transform and ARIMA models,” IEEE Trans. Power Syst., vol. 20, no. 2, pp. 1035-1042, May 2005.

[132] R.C. Garcia, J. Contreras, M.V. Akkeren, and J.B.C. Garcia, “A GARCH forecasting model to predict day-ahead electricity prices,” IEEE Trans. Power Syst., vol. 20, no. 2, pp. 867-874, May 2005.

Reference

[133] G. Li, C.C. Liu, C. Mattson, and J. Lawarree, “Day-ahead electricity price forecasting in a grid environment,” IEEE Trans. Power Syst., vol. 22, no. 1, pp. 266-274, Feb. 2007.

[134] C. M. Bishop and others, Pattern recognition and machine learning, vol. 1. Springer New York, 2006.

[135] D. E. Goldberg and J. H. Holland, “Genetic algorithms and machine learning,” Machine learning, vol. 3, no. 2, pp. 95–99, 1988.

[136] Y. Xu, Z.Y. Dong, Z. Xu, K. Meng, and K.P. Wong, “An intelligent dynamic security assessment framework for power systems with wind power,” IEEE Trans. Industrial Informatics, vol. 8, no. 4, pp. 995-1003, Nov. 2012.

[137] K. Meng, Z.Y. Dong, and K.P. Wong, “Self-adaptive RBF neural network for short-term electricity price forecasting,” IET Gen. Trans. & Dist., vol. 3, no. 4, pp. 325-335, Apr. 2009.

[138] M.-B. Li, G.-B. Huang, P. Saratchandran, and N. Sundararajan, “Fully Complex Extreme Learning Machine,” Neurocomputing, vol. 68, pp. 306-314, 2005.

[139] X. Chen, Z.Y. Dong, K. Meng, Y. Xu, K.P. Wong, and H.W. Ngan, “Electricity price forecasting with extreme learning machine and bootstrapping,” IEEE Trans. Power Systems, vol. 27, no. 4, pp. 2055-2062, Nov. 2012.

[140] C. Wan, Z. Xu, P. Pinson, Z. Y. Dong, and K. P. Wong, ‘A Hybrid Artificial Neural Net-work Approach for Probabilistic Forecasting of Electricity Price’, IEEE Trans. Smart Grid, vol.5, no.1, pp. 463-470, Jan2014.

[141] Q.-Y. Zhu, A. K. Qin, P. N. Suganthan, and G.-B. Huang, “Evolutionary extreme learning machine,” Pattern recognition, vol. 38, no. 10, pp. 1759–1763, 2005.

[142] J. Cao, Z. Lin, and G.-B. Huang, “Self-adaptive evolutionary extreme learning machine,” Neural Processing Letters, vol. 36, pp. 285-305, 2012.

[143] N.M. Pindoriya, S.N. Singh, and S.K. Singh, “An adaptive wavelet neural network-based energy price forecasting in electricity markets,” IEEE Trans. Power Syst., vol. 23, no. 3, pp. 1423-1432, Aug. 2008.

[144] B. Subudhi and D. Jena, “Differential evolution and Levenberg Marquardt trained neural network scheme for nonlinear system identification,” Neural Processing Letters, vol. 27, no. 3, pp. 285–296, 2008.

Reference

[145] D. C. Montgomery, Design and analysis of experiments. Wiley.com, 2006, p405.

[146] S. Das and P. N. Suganthan, “Differential evolution: A survey of the state-of-the-art,” Evolutionary Computation, IEEE Transactions on, vol. 15, no. 1, pp. 4–31, 2011.

[147] J. Zhang and A. C. Sanderson, “JADE: adaptive differential evolution with optional external archive,” Evolutionary Computation, IEEE Transactions on, vol. 13, no. 5, pp. 945–958, 2009.

[148] A. K. Qin and P. N. Suganthan, “Self-adaptive differential evolution algorithm for numerical optimization,” in Evolutionary Computation, 2005. The 2005 IEEE Congress on, 2005, vol. 2, pp. 1785–1791.

[149] E. Ancillotti, R. Bruno, and M. Conti, “The role of the RPL routing protocol for smart grid communications,” IEEE Communication Magazine, vol. 51, no. 1, pp. 75-83, Jan. 2013.

[150] G. Sorebo and M. Echols, Smart grid security: an end-to-end view of security in new electrical grid, New York: Taylor and Francis, 2012.

[151] E. Pallotti and F. Mangiatordi, “Smart grid cyber security requirements,” in Proc. International Conference on Environment and Electrical Engineering (EEEIC), May. 2011.

[152] T. Sommestad, G. Ericsson, and J. Nordlander, “SCADA system cyber security---a comparison of standards,” in Proc. IEEE PES General Meeting, Jul. 2010.

[153] B. Bitzer and E. Gebretsadik, “Cloud computing framework for smart grid applications,” in Proc. Power Engineering Conference, 2013.

[154] H. Kim, Y. Kim, K. Yang, and M. Thottan, “Cloud-based demand response for smart grid: architecture and distributed algorithms,” in Proc. IEEE International Conference on Smart Grid Communications, Oct. 2011.

[155] Y. Liu and P. Ning, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 13, May. 2011.

[156] Y. Kim, M. Thottan, V. Kolesnikov, and L. Wonsuck, “A secure decentralized data-centric information infrastructure for smart grid,” IEEE Communication Magazine, vol. 48, no. 11, pp. 58-65, Nov. 2010.

Reference

[157] Mostafa M. Fouda, Z.M. Fadlullah, N. Kato, Rongxing Lu, Xuemin Shen, "A lightweight message authentication scheme for smart grid communications." IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Aug. 2011.

[158] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Foundations of Computer Science, in Proc. IEEE 35th Annual Symposium, 1994.

[159] Matteo Mariantoni, H. Wang, T. Yamamoto, M. Neeley, Radoslaw C. Bialczak, Y. Chen, M. Lenander, Erik Lucero, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, Y. Yin, J. Zhao, A. N. Korotkov, A. N. Cleland, John M. Martinis, "Implementing the quantum von Neumann architecture with superconducting circuits," Science, vol. 334, no. 6052 pp. 61-65, Oct. 2011.

[160] Jarryd J. Pla, Kuan Y. Tan et al, “A single-atom electron spin qubit in silicon,” Nature, vol. 489, no.7417, pp. 541-545, Sept. 2012.

[161] Quantum Artificial Intelligent Laboratory of NASA [online].

Available: http://www.nas.nasa.gov/quantum/

[162] MIT Technology Review [online].

Available:http://www.technologyreview.com/news/530516/google-launches-effort-to-build-its-own-quantum-computer/

[163] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, John Smolin, "Experimental quantum cryptography," Journal of Cryptology vol.5, no. 1, pp. 3-28, Jan. 1992.

[164] Muller, A., H. Zbinden, and N. Gisin. "Quantum cryptography over 23 km in installed under-lake telecom fibre," EPL (Europhysics Letters) vol. 33, no. 5, pp. 335, Feb. 1996.

[165] Paul D. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature, vol. 385, no. 6611, pp. 47-49, Jan. 1997.

[166] Toshiba Quantum Key Distribution System [online].
Available:http://www.toshibaeurope.com/research/crl/qig/quantumkeyserver.html

[167] IBM Research Project [online].

Available:http://www.almaden.ibm.com/st/past_projects/quantum_information/qcrypt/

Reference

[168] NEC Succeeds in World's Fastest Continuous Quantum Cryptography Key Generation over Fortnight Period [online].

Available:http://www.nec.co.jp/press/en/0505/3101.html

[169] Göran Lindblad, "A general no-cloning theorem," Letters in Mathematical Physics, vol. 47, no. 2, pp. 189-196, Jan. 1999.

[170] D. Pudjianto, C. Ramsay, and G. Strbac, “Virtual power plant and system integration of distributed energy resources,” IET Renewable Power Generation, vol. 1, no. 1, pp. 10-16, Mar. 2007.

[171] M. Albadi and E. El-Saadany, “A summary of demand response in electricity markets,” Electric Power Systems Research, vol. 78, no. 1, pp. 1989-1996, Nov. 2008.

[172] B. Ramanathan and V. Vittal, “A framework for evaluation of advanced direct load control with minimum disruption,” IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1681-1688, Nov. 2008.

[173] A. Teixiera, S. Amin, H. Sandberg, K. Johansson, and S. Sastry, “Cyber security analysis of state estimators in electric power systems,” in Proc. 49th IEEE Conference on Decision and Control, 2010.

[174] Fengji Luo, Junhua Zhao, Zhao Yang Dong, Yingying Chen, Yan Xu, Xin Zhang, Kit Po Wong, “Cloud-Based Information Infrastructure for Next-Generation Power Grid: Conception, Architecture, and Applications,” ,” IEEE Trans. Smart Grid, vol. pp, no. 99, pp.1, Sept. 2015.