Distributed Control Methods for Integrating Renewable Generations and ICT Systems

XU, JIANGJIAO

Distributed Control Methods for Integrating Renewable Generations and ICT Systems

Jiangjiao Xu

A Thesis presented for the degree of
Doctor of Philosophy

Department of Engineering
University of Durham
United Kingdom

August 2018

Dedicated to

My parents and supervisors

Abstract

With increased energy demand and decreased fossil fuels usages, the penetration of distributed generators (DGs) attracts more and more attention. Currently centralized control approaches can no longer meet real-time requirements for future power system. A proper decentralized control strategy needs to be proposed in order to enhance system voltage stability, reduce system power loss and increase operational security. This thesis has three key contributions:

Firstly, a decentralized coordinated reactive power control strategy is proposed to tackle voltage fluctuation issues due to the uncertainty of output of DG. Case study shows results of coordinated control methods which can regulate the voltage level effectively whilst also enlarging the total reactive power capability to reduce the possibility of active power curtailment. Subsequently, the communication system time-delay is considered when analyzing the impact of voltage regulation.

Secondly, a consensus distributed alternating direction multiplier method (ADMM) algorithm is improved to solve the optimal power flow (OPF) problem. Both synchronous and asynchronous algorithms are proposed to study the performance of convergence rate. Four different strategies are proposed to mitigate the impact of time-delay. Simulation results show that the optimization of reactive power allocation can minimize system power loss effectively and the proposed weighted autoregressive (AR) strategies can achieve an effective convergence result.

Thirdly, a neighbouring monitoring scheme based on the reputation rating is proposed to detect and mitigate the potential false data injection attack. The simulation results show that the predictive value can effectively replace the manipulated data. The convergence results based on the predictive value can be very close to the results of normal case without cyber attack.

Declaration

The work in this thesis is based on research carried out at the School of Engineering, Durham Univeristy, England. No part of this thesis has been submitted elsewhere for any other degree or qualification and it is all my own work unless referenced to the contrary in the text.

Acknowledgements

Foremost, I would like to thank my principal PhD supervisor, Dr. Hongjian Sun, for giving me the great opportunity, warm encouragement, continuous support and guidance throughout my PhD research at Durham University. He not only gives me continuous help and tremendous academic support, but also provides his endless patience and enthusiasm to keep me always stay positive during my PhD research over the past four years. I have learned rigorous academic attitude and unique research perspective from Dr. Sun, which will benefit all my life.

I would like to express particular gratitude to Dr. Chris Dent for his supervision. Dr. Chris Dent has offered a great deal of advices and opportunities including conferences and workshops during my PhD research. The enthusiasm he has for research has deeply encouraged me. I also wish to thank Dr. Junjie Wu and Dr. Behzad Kazemtabrizi for their time and valuable discussions during my PhD study.

I am very grateful to my great colleagues and friends at Durham, especially to Dan Li, Qitao Liu, Minglei You, Lei Fan, Meng Xu and Ahmad Ibrahim. Without them, the work wouldn't be full of joy, interesting discussions and lovely memories.

The most special thanks is to my wife, Yan Cheng. Without her, I would not complete my PhD study so smoothly. She has been silently supporting and giving me confidence. Moreover, I would like to thank my parents and my family members for their boundless love.

Finally, I would like to thank the support and funding provided by the Durham University and Engineering and Physical Sciences Research Council, and the Great Britain-China Center also provides the students awards for me.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This thesis mainly addresses the issues of voltage rise and optimal power flow (OPF) in power distribution system. Because current centralized control strategies cannot effectively manage system efficiency caused by distributed generator(DG), innovative decentralized voltage control method and alternating direction multiplier method (ADMM) based optimization OPF algorithm combined with communication model are designed to address the research challenges. In addition, the cyber attack analysis in such distribution network is studied to test the performance on the convergence results of ADMM. Communication system is a critical component in future smart grid network due to the need of integrating renewable generators, distributed storages and electric vehicles. However, communication system may have a certain side effect on the normal control operation and optimization results for the distribution power system. This thesis will present communication time-delay model to both decentralized voltage control strategy and ADMM-based optimization algorithm. Subsequently, the cyber attack of communication system is also simulated to show the performance of these algorithms.

1.1 Motivation

A complete electric power system is made up of power generation system, transmission system, subtransmission system and distribution system [1]. Modern power grid is the most complex artificial system and energy transmission network in the world. Figure 1.1 demonstrates the basic elements for a traditional power system. A complex transmission network consists of transmission lines, transformers and switching devices. The transmission system mainly interconnects the power generation facilities and various distribution load centers. In general, the generation and transmission systems are referred to as bulk power systems. The voltage level in transmission system always operates at the highest voltage levels (generally, 230 kV or more) [2]. The subtransmission system and distribution system transfer the electricity to the terminal consumers. The subtransmission system mainly transfers the power to large industrial consumers. The distribution system represents the final stage in the transfer of electricity power to the individual consumers. The primary distribution voltage is usually in the range of 4 kV to 34.5 kV and the secondary distribution voltage is typically at 120 V and 220/240 V (Data is based on the North American interconnected power system in [3]). The overall system consists of multiple power supplies and multilayer transmission networks which provide a high degree of structural redundancy to improve the stability of the power system.

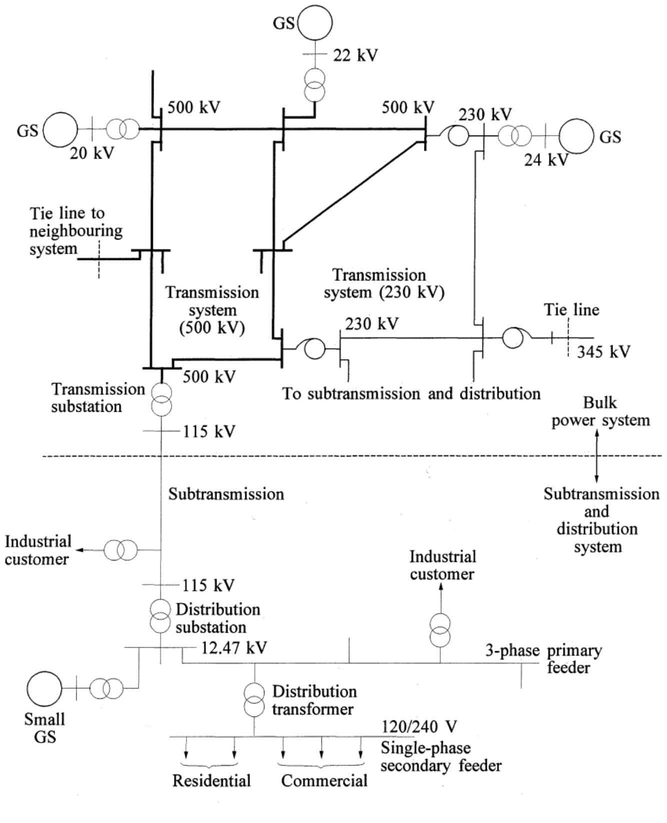


Figure 1.1: The basic elements for power system [1]

As the world enters a period of rapid development under the backdrop of ever-expanding world economy, increased energy demand, improvement in reducing environmental pollution, adjustment of energy structure and stringent requirements on sustainable development are just several hotly debated subjects. The smart power system, known as smart grid (SG), refers to a new generation of modern electrical power system that aims to provide efficient, secure, reliable and high quality renewable energy using modern communications, sensor measurement, automatic control and analysis decision technologies [4]. The renewable energy sources (RESs), such as sunlight, wind, tides, plant growth and geothermal heat, will become progressively more important as time goes on in future SG. The large penetration of DGs has been encouraged in order to achieve the government's goals related to the promotion of a more sustainable development. In 2007, the United Kingdom Government agreed with European Union's overall goal of generating 20% of the European Union's energy supply from renewable sources by 2020 and the allocated target of the United Kingdom is 15% [5]. In 2009, the European Community has officially recognized the requirement to promote the RES as a major resource in energy sector [6]. A drastically increasing RESs are expected in upcoming years through the world.

Nevertheless, the unpredictable output of DGs to distribution network (DN) will cause a series of technical challenges, such as voltage problem and power loss problem [7]. Furthermore, traditional centralized control strategies may not control power system effectively and also can not be done in real-time. Thus, it is necessary to develop proper control techniques not only to maintain the system security and stability, but also to reduce the economic loss in real-time. Controlling the real and reactive power output by means of DGs implies that RES units can directly participate to control the voltage level and optimize the system efficiency [8–10]. In light of the requirement of new technologies and higher penetration of DGs, reactive power control strategy has emerged to alleviate voltage rise and optimization issues. An appropriate reactive power control method not only can deal with these problems effectively, but also reduce the need of new assets and reinforcements from the network.

Many extensive studies have been carried out to develop efficient reactive power control methods. Although numerous reactive power control strategies are reported in the literature [11–21], few of them mention the communication time-delay problem although the decentralized control operation contains a limited information exchange during the system optimization. When the practical communication delay is considered, some control strategies may not obtain the optimal target and sometimes could not even get the effective result. For voltage stability issue, a few coordinated control methods in [15–21] were proposed to maintain the voltage level. However, these algorithms did not consider the impact of communication time-delay on the operation of coordination algorithms. For economic loss problem, a few papers [22–24] introduced synchronous communication time-delay system into the decentralized ADMM algorithm, which was based on a master-slave strategy. The proposed algorithms in these papers could still be treated as centralized control approaches. Because the master could be considered as a control center which would collect information from all other independent workers. Only when all the information had been received by the master, the master would broadcast to other nodes to proceed the next step. To the best of the author's knowledge, the majority of recent papers have not investigated this subject, particularly the fully decentralized control strategy in distribution power system with communication time-delay.

1.2 Aims of Research

The aim of this thesis is to study the performance of the algorithms combined with communication time-delay in distribution power system, including coordinated voltage control, optimization OPF problem, and cyber attack issues. More specifically, the research has the following objectives:

- To analyze the performance of decentralized coordinated voltage control methods with the communication time-delay model.

- To develop the ADMM-based decentralized optimization algorithm that is applicable to solve the OPF problem. In addition, the communication time-delay model is applied in this algorithm to analyze the performance on the convergence results with both synchronous and asynchronous algorithm. Finally, four possible strategies are also proposed to reduce the impact of the convergence results and improve the algorithm efficiency.

- To analyze the possible impacts of cyber-attack on the control and optimization algorithm, two possible cyber-attack models in decentralized reactive power control strategies are summed up to analyze the vulnerability of the algorithms and two targeted countermeasures are proposed to mitigate the impacts of attacks.

This research mainly studies local reactive power allocation, which can maintain voltage level and optimize reactive power in order to minimize system power losses. It is construed that my research tends to be centred around the optimization of local reactive power absorption/injection of the distribution generator. Figure 1.2 shows that the local reactive power is a significant part of the distribution network and has a close connection to my three research directions. Firstly, the voltage level in distribution network can be adjusted by both reactive power and reactive power, where the reactive power has the greatest influence on the voltage level. Secondly, the effect of reactive power change on the system power loss is significant. Therefore, it is necessary to optimize the distribution of local reactive power loss. Finally, although distributed algorithm reduces the requirements for communication systems, certain information exchange to complete the execution of the algorithm still exists. Hence, the communication time-delay will become a problem that has to be considered. And It is necessary to consider the impact of cyber-physical issue on the algorithm.

1.3 Original Contributions

The main contributions of this research are summarized as follows:

- Given the little literature in the research of analyzing communication time-delay in smart grid so far, this thesis links an imperfect communication system to a

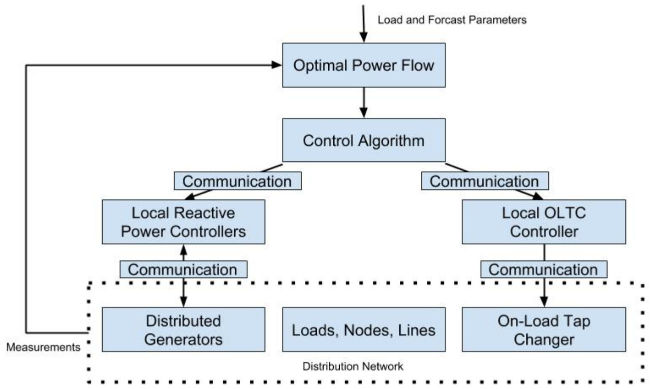


Figure 1.2: The basic connection of reactive power in distribution network

coordinated voltage control problem. The time-delay analysis is presented to show the impact of communication time-delay to a coordinated voltage control strategy. Simulation results show that, with time-delay, existing approaches cannot control the voltage level as expected and thus may affect the system stability. The existing control method should be modified to adapt to the applied time-delay introduced by communication systems.

- ADMM algorithm [25] is improved to achieve the convergence results in the OPF problem in power system. We propose to utilize improved iterative steps to optimize the power loss which presents an efficient convergence result in this thesis. The ADMM algorithm has been investigated for decades in power system, we focus on the OPF formulation by a fully decentralized reactive power control approach with time-delay model to optimize the results. The communication is based on the information exchange between neighbouring nodes. The investigation of convergence speed could provide a reference to design such kind of algorithm.

- Both synchronous and asynchronous algorithms considering communication time-delay are proposed. Comparing with the results of synchronous no-delay algorithm, the proposed asynchronous no-delay algorithm still has a better convergence speed and optimization results during the same wall clock time whilst the asynchronous algorithm has a larger time-delay tolerance during the iterative process. Compared with other decentralized OPF algorithms, this work not only adds the state-of-the-art communication delay model to the ADMM algorithm, but also explores the performance of proposed synchronous and asynchronous algorithms with time-delay in decentralized OPF problem. Furthermore, the simulation results prove that the communication delay has a great influence on the results of decentralized ADMM algorithm. With time-delay considered, the traditional decentralized algorithm even can not converge normally.

- Due to large fluctuations arising from the results of the experiment of convergence performance analysis with communication time-delay, we propose four d-ifferent strategies, such as skipping strategy (SS), previous value strategy (PVS), autoregressive (AR) strategy (ARS) and weighted autoregressive strategy (WARS), to optimize the synchronous and asynchronous convergence results. The proposed WARS can effectively improve the convergence results for both synchronous and asynchronous algorithms and also reduce the fluctuation of the results significantly in the synchronous optimization algorithm with 10% probability of time-delay.

- The simulation results on two cyber attack models are also demonstrated to analyze the vulnerability of control algorithms. According to the simulation, the proposed algorithms have some shortcomings when the cyber attack occurs. Both cyber attacks can significantly influence the results compared with the no-attack case. Neighbouring monitoring strategy (NMS) based on the predictive value is proposed to mitigate the impact of cyber attacks of information exchange between neighbouring nodes on the OPF algorithm and achieve an improved convergence result.

1.4 Thesis Outline

The remainder of thesis is described as follows:

Chapter 2

This chapter first introduces some traditional voltage control methods and also shows the basic principle of reactive power output adjustment of DGs. Moreover, the optimization OPF problem is also summarized in traditional power system. For OPF problem in decentralized algorithms, a modified consensus version of the

ADMM is adopted to solve problem. Finally, information and communication technology (ICT) challenges for stochastic communication time-delay and cyber attacks in electrical power system network are discussed.

Chapter 3

This chapter introduces the decentralized coordinated voltage control method by using the reactive power output of DGs. Since the algorithm includes a certain information exchange during the algorithm iteration, the simulation results with time-delay are displayed to analyze the performance on this decentralized coordinated voltage control method.

Chapter 4

This chapter proposes ADMM-based synchronous and asynchronous algorithms considering stochastic time-delay. Using the stochastic communication time-delay model, the convergence performance of both synchronous and asynchronous algorithms is simulated. In addition, different strategies, for example, skipping strategy, previous value strategy, AR strategy and weighted AR strategy, are proposed to reduce the fluctuation of the results and also improve the efficiency of convergence results for both algorithms.

Chapter 5

This chapter studies two cyber attack models, time-delay model and false data injection model, to test the stability of OPF algorithm. The performances of both attack models are presented and simulations can effectively show the weak points of current algorithms. According to the experimental results, we propose a neighbouring monitoring strategy to mitigate the potential impact of cyber threats to improve the vulnerability of the algorithm.

Chapter 6

This chapter draws the conclusions and also presents several new research directions for future work.

Chapter 2

Background

The penetration of renewable energy source (RES) units and use of information and communication technologies (ICT) will be integral parts in a new generation of power system, also known as smart grid. A crucial role of RES units is that they can mitigate the environment pollution, increase the energy diversity and reliable the power system. However, there are two main challenges that need to be addressed in real time, i.e., stability of the system voltage profile and optimization of the power loss. Due to the installation of DGs in local buses and the uncertainty of DG output, the local voltage level for each bus will become variable. Thus, it is necessary to propose an effective control strategy to maintain the voltage level in real-time. Another issue is to minimize the power loss in terms of the reactive power capability of DGs. Due to the requirement of wireless communication in real-time, it is necessary to apply the probabilities of time-delay to analyze the effects on the performance of normal results. By integrating the power system with a cyber system, it shows the significant cyber security challenges and makes the entire power system more vulnerable to cyber attacks. Thus, it is desirable to analyze and protect power system in advance or detect the cyber attacks and mitigate the possible cyber threats.

In this chapter, Section 2.1 presents the reactive power voltage control techniques. Traditional voltage control methods are shown in Section 2.1.1 and the reactive power voltage control method is introduced in Section 2.1.2. A literature review of

OPF algorithms is given in Section 2.2.1. Then the ADMM-based OPF algorithm is discussed in Section 2.2.2. Finally, the stochastic communication time-delay and cyber-physical attacks in smart grid are presented in Section 2.3.

2.1 Reactive Power Voltage Control Techniques

The voltage profiles of all nodes are controlled by absorption, production and flow of reactive power at all levels in the power system. The unpredictable output of renewable energy sources can cause a series of technical challenges. The variable output of renewable energy would need additional actions to balance the power system. The larger flexibility may be required to accommodate the variability of the supply side and the relationship to power generation levels and loads. Sometimes renewable power can increase with load. But when load levels drop and renewable energy generation increases, additional measures may need to be taken to balance the power system. The system operators need to ensure that they have sufficient resources to accommodate significant increases or decreases of reactive power to maintain system balance. Another challenge arises when renewable energy is available at low load levels. One of the main challenges is voltage fluctuation that needs an appropriate control method to stabilize the voltage. The voltage regulation approaches can be classified into two categories: centralized control strategies and decentralized control strategies.

2.1.1 Traditional Voltage Control Methods

In the past few decades, the traditional devices used for voltage regulation can be divided into three categories:

a Tap changer in transformers, such as No Load Tap Changers (NLTP) and On Load Tap Changers (OLTC).

b Sources of reactive power, such as shunt reactors, shunt capacitors and Distribution Static Compensator (DSTATCOM) .

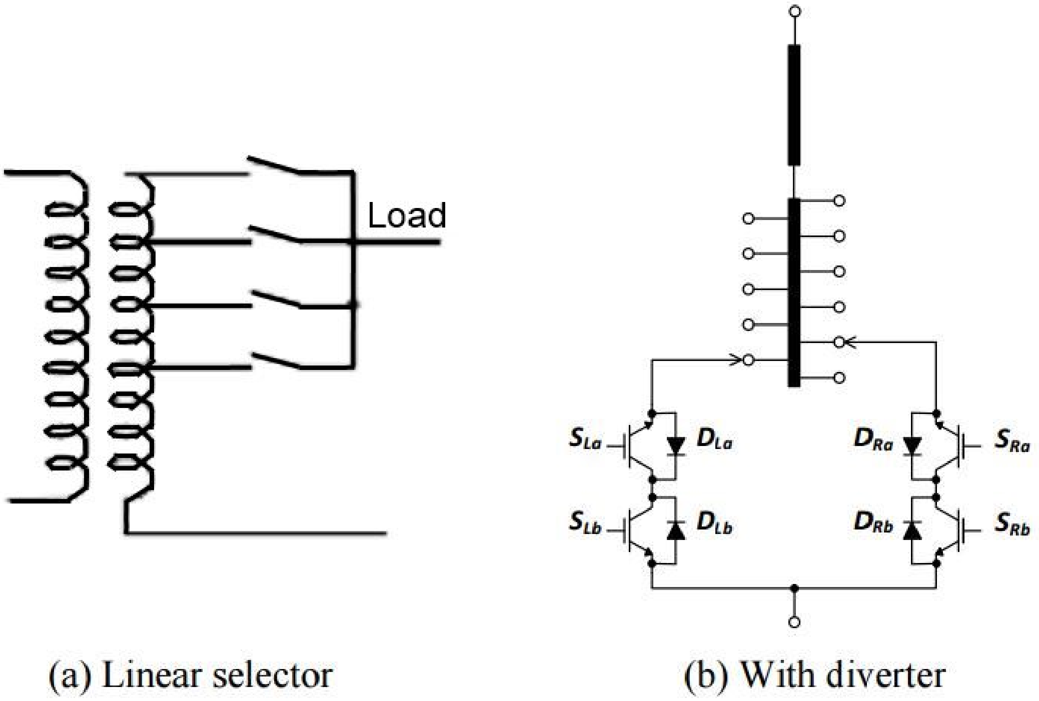
c Line reactance compensator, such as series capacitor.

Tap Changer

A tap changer in transformers is a mechanism to change the voltage level by selecting the different turns ratios. The transformer can achieve the different turns ratios by setting a number of access points, known as taps, in one or more windings. It is necessary to change the turns ratios to satisfy the requirement of voltage regulation from the power system point of view. There are two types of tap changers, No Load Tap Changers (NLTC) and On Load Tap Changers (OLTC).

The NLTC, also called off-circuit tap changer, requires to be de-energized before the tap is changed. This tap changer can be used in several scenarios in which a frequent tap changing requirement is not needed and the power transformer system is accepted to be interrupted. It is often employed in low voltage transformer due to the seasonal change, system expansion and load growth. Furthermore, the NLTC is also employed in high voltage transformer in which the tap changer normally will be set just once at the time of installation.

For many power transformer systems, a sudden interruption of a tap changing is unacceptable. Hence, the OLTC, also called on-circuit tap changer, is installed to control the voltage level. This kind of tap changer often utilizes the numerous tap selector switches to regulate the voltage level under load. Fig. 2.1 presents the basic structure of OLTC, which is suitable for applications requiring high changing frequency. Fig. 2.1(a) shows when one tap selector switch A closes, other switches will open. If another tap selector switch B is selected to change the voltage, it will be turned on to short switch A. Then switch A will open and switch B has completed the selection. Another type of tap changer is shown in Fig. 2.1(b). It commences operation at left side with electronic devices. In moving to other tap at right side, the operation can change the tap selector switch by controlling the power electronic components when other switch is selected.



(a) Linear selector

(b) With diverter

Figure 2.1: The basic structure of on-load tap changer [1].

Series Capacitors

The series capacitor has been used to regulate the voltage level for distributed and industrial feeder since the 1930s [26]. It can compensate the inductive reactance of transmission line by connecting in series with the line conductors. Meanwhile, the installation of series capacitor can reduce transfer reactance, increase maximum transmission power and reduce effective reactive power loss. Although series capacitor usually is not utilized in regulating the voltage level directly, it can improve voltage profile and balance the reactive power in the power system.

2.1.2 Reactive Power Voltage Control Method

The synchronous generators can produce or absorb reactive power depending on the excitation. If the generators are overexcited, they can produce reactive power to the grid. If the generators are underexcited, they can absorb the reactive power from the grid. The capability of the active/reactive power is limited by the field current, armature current and end-region heating limitation, the application for a distributed generator will be discussed in Section 3.2.2. The synchronous generators provide the voltage control on the supply side. Hence, additional voltage control methods are usually required to balance the voltage level on the demand side.

The compensating devices can be classified into two types: passive compensation and active compensation. Shunt reactors, shunt capacitors and series capacitors can be treated as the passive compensation. They are often fixed on the transmission and distribution system to contribute to voltage control by modifying network characteristics. Synchronous condensers and SVC can be treated as the active compensation. They can connect to the buses directly and compensate reactive power automatically to regulate the voltage level. As sketched in Fig. 2.2, SVC which is comprised of one or more banks of fixed or switched shunt reactors or capacitors, can be installed in some special nodes in power system, unlike the generator only can be adjusted the voltage level at the terminal node. However, SVC has a limited overload capability and an expensive investigation.

These reactive power control strategies only concern with the planning of the reactive power. Hence, there is a need to adopt a more efficient voltage control method in order to regulate the voltage profile in smart grid with high penetration of DGs in real-time. The voltage control by reactive power and allocation problem has been researched extensively in the literature [27–32]. More recently, a group of researchers have overcome the voltage fluctuation issues of distribution network with inverter-based distributed generators. Compared with the preceding voltage control methods, the inverter-based DG reactive power control has more advantages. First, it is more effective. Second, it has superior real-time performance. Thirdly, it does not need additional investigations.

Generally, the approaches of voltage regulation based on the apparent power capability of DG with inverter can be classified as follows: centralized control strategies and decentralized control strategies [33–35]. Centralized control strategies can monitor the status of all reactive power compensation equipments, perform a certain load forecast, optimize reactive power allocation based on the forecast, determine reactive

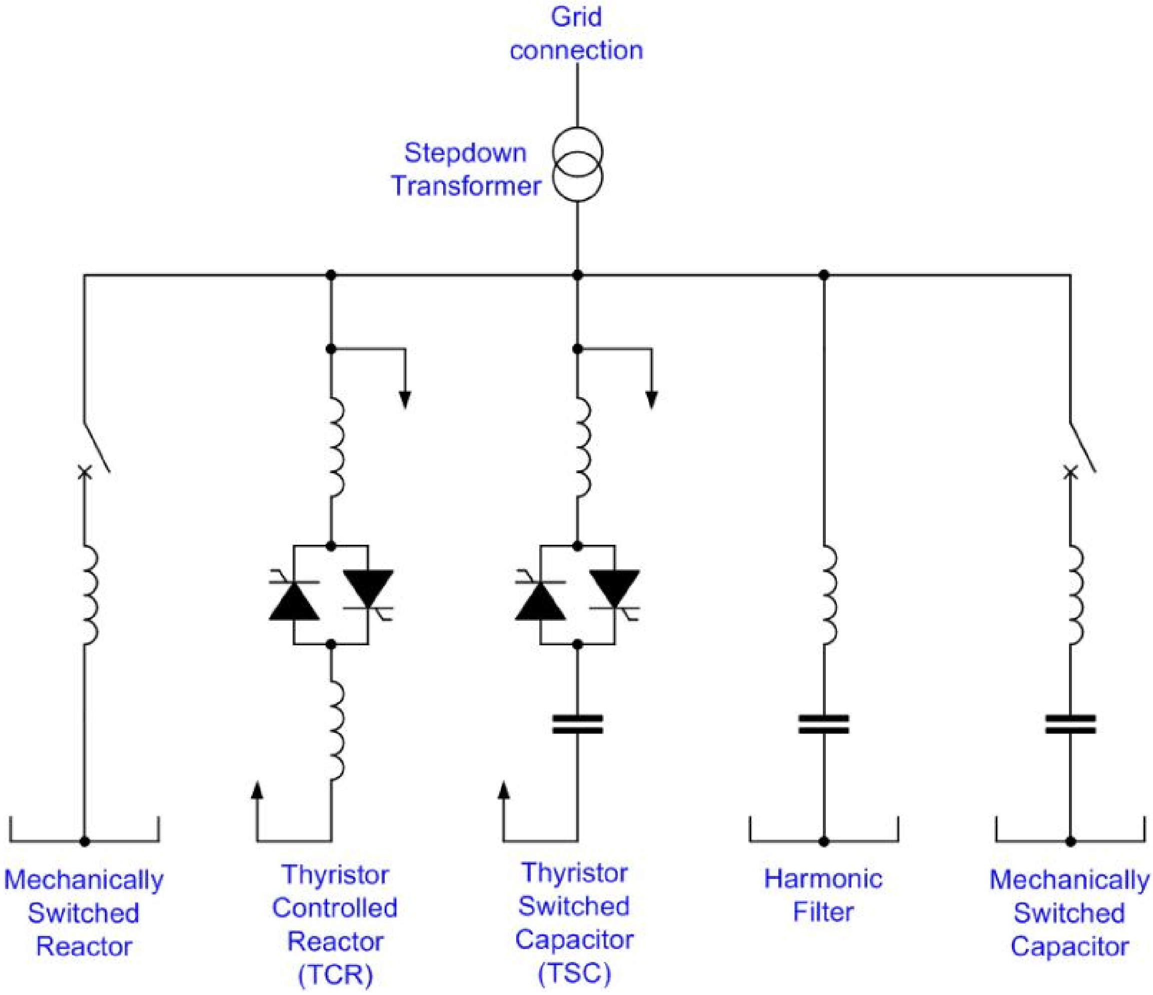

Grid connection
Stepdown Transformer
Mechanically Switched Reactor
Thyristor Controlled Reactor (TCR)
Thyristor Switched Capacitor (TSC)
Harmonic Filter
Mechanically Switched Capacitor

Figure 2.2: One-line diagram of a typical SVC configuration with a thyristor controlled reactor, a thyristor switched capacitor, a harmonic filter, a mechanically switched capacitor and a mechanically switched reactor [3].

power injection/absorption for each device and send control signals to local reactive power control equipment. However, there are two issues need to be discussed. First, the process for such a large power system is too cumbersome that may induce a large time-delay. Second, a certain forecasting error would be possible due to the large time-delay and uncertainty of output power, which may result in the optimal reactive power allocation being a bad accuracy of the solution.

To mitigate the effect of time-delay, decentralized control approaches were proposed to optimize the voltage level which could reduce the time of the control process dramatically. An autonomous decentralized control strategy was studied in [11] by employing a multi-agent system. The cost of additional communication network will be lower compared with the requirement of information exchange in a centralized strategy. In [36], a decentralized control method that considers the control priority was proposed to adjust the reactive power output by changing the power factor of a PV system. Using this control approach, each DG is independent from the others, thus it may not deal with some special circumstances without any cooperation in real time, e.g., DG out of service, greater demand load than usual or larger active power output. If one DG is out of service, the other DGs will not help to improve the voltage level of the node that has broken down. Reference [37] presented a coordinated control strategy of DGs to improve the voltage fluctuation issues which can adjust itself cooperatively to optimize the reactive power allocation. However, these works did not consider the effect of time-delay on the performance of voltage fluctuation in the distribution system.

Therefore, it is anticipated to propose a coordinated reactive power voltage control strategy to realize real-time control in order to meet the uncertain output of DGs. Meanwhile, the analysis of communication time-delay system on the performance of control method will be an important part for the study of control strategy.

2.2 ADMM Based OPF Problem of Reactive Power Control

When electricity power is transmitted across the transmission and distribution system, a fraction of the energy will be dissipated due to the resistance which is dependent on the conductor, current and length of the line. As the power loss is a quadratic function of the current (I^2R) which is subject to the power flow, there is a largest loss when the peak load demand occurs in the distribution network. In addition, the distribution transformers contribute to power losses in the form of a) heat loss within the iron core, and b) load loss represented by the current flowing through the windings.

The resistance and reactance of the conductors will be a significant part of the system power loss calculation for underground cables and overhead line in alternating current system. Compared with the conductor loss, sheath loss and dielectric loss can be neglected since they are relatively too small. The reactive power flow (the reactive current flow solely in reaction to the circuit) transmits no 'real' power to the load which can result in an additional heating loss in the transmission line. When the reactive current increases, the reactive power will increase and the power factor will decrease (Power factor means the ratio of active power to apparent power). The power loss will be higher due to the low power factor in the transmission and distribution networks. Hence, the additional reactive power compensation methods can help to compensate for the reactive power flow through the power system. In other words, reactive power can stabilize the system voltage level. If the reactive power decreases, the total system power loss will also be reduced.

The future smart grid will become more and more granular because of the high penetration of DGs. It can reduce the amount of the transfer of apparent power from remote generation via transmission and distribution networks if DGs connect to the buses directly. And the total power loss of the system will also be decreased. In order to analyze the basic characteristic of voltage level and power loss in a large complex power system, detailed analysis of power flow needs to be studied in order to demonstrate the performance of optimization results in a distributed power system.

2.2.1 Overview of OPF Problem

In this subsection, the power flow analysis will be described to study the performance of the power system.

Bus Classification

There are four quantities associated with each bus: active power, reactive power, voltage magnitude and voltage angle. All buses can be classified as follows:

- PV bus: Active power and voltage magnitude are fixed. Meanwhile, the reactive power output is limited by the characteristics of the individual devices, such as generators, synchronous condensers and SVC.

Table 2.1: Classification of Buses

	P	**Q**	**V**	$\boldsymbol{\theta}$
PV bus	*known*	*known*	*unknown*	*unknown*
PQ bus	*known*	*unknown*	*known*	*unknown*
Slark bus	*unknown*	*unknown*	*known*	*known*
Device bus	*unknown*	*unknown*	*unknown*	*unknown*

- PQ bus: Active power and reactive power are fixed. Generally, loads are assumed to be constant. When the tap changer operation of distribution transformer can be neglected, active power and reactive power are set as functions of voltage.

- Slack bus: It is also known as the reference bus. The voltage magnitude and phase angle are fixed. Since the power loss in the power system is unknown in advance, the slack bus can be utilized to balance the active power and reactive power to increase/decrease the power loss in the system.

- Device bus: These buses are special boundary conditions associated with electronic equipments, for example, HVDC converters.

In general, the slack bus injects or absorbs the active power and reactive power which is crucial to the power flow issue since it can account for transmission line losses. And it is the only bus to be known as the reference phase angle. The summary can be found in Table 2.1.

Power Flow Analysis

As the balanced operation of power system is considered only, each element will be modelled in the light of its single-phase equivalent. The relationships between voltages and currents of nodes can be written as either loop equations or node equations. Since the number of independent loop equations is larger than the number of independent node equations, it is obvious that the node equations will be adopted in this chapter.

The equations in the light of node admittance matrix can be found as follows:

$$\begin{bmatrix} \bar{I}_1 \\ \bar{I}_2 \\ \cdots \\ \bar{I}_n \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n} \\ Y_{21} & Y_{22} & \cdots & Y_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ Y_{n1} & Y_{n2} & \cdots & Y_{nn} \end{bmatrix} \begin{bmatrix} \bar{V}_1 \\ \bar{V}_2 \\ \cdots \\ \bar{V}_N \end{bmatrix} \tag{2.1}$$

where

n is the number of total nodes.

$\bar{I}_i$ is the phasor current flowing to the network at node i.

$\bar{V}_i$ is the phasor voltage to the ground at node i.

Y_{ii} is the self admittance of node i and also means the total admittances terminating at node i.

Y_{ij} is the admittance between node i and node j and also means the negative of the sum of total admittances between node i and node j.

The form of nonlinear loads and other devices connecting to the nodes is represented as the node current. Meanwhile, constant linear loads will be included in the node admittance matrix. The general observations regarding to the node admittance matrix can be found as follows:

1. It is a sparse matrix and the degree of sparsity depends on the size of the network.
2. It is singular if there are no shunt branches to the ground.
3. It has a weak diagonal dominance, for example, $|Y_{ii}| \geq \sum\limits_{i \neq j} |Y_{ij}|$.
4. It is symmetrical if there are no phase-shifting transformers.

Equation 2.1 will be linear if the injected phasor current is known. However, the injected phasor current is not known for most nodes in the network in practice. The phasor current at any node i is determined by active power, reactive power and phasor voltage. It is clear that the boundary conditions of different types of nodes make the issue nonlinear. Hence the power flow analysis needs to be addressed iteratively using methods such as Gauss-Seidel method or Newton-Raphson method. The principles of the application are brief in [1]. The comprehensive reviews of numerical methods of power flow calculation can be found in [38, 39]

Comparison of the Power Flow Calculation Methods

The Gauss-Seidel method, also known as the Liebmann method or the method of successive displacement, is the oldest way to solve the power flow problem in power system [40]. It is a simple and reliable way usually with a tolerant of poor voltage and reactive power conditions. Meanwhile, it has a relatively low requirement of computer memory. However, when the power system is large, the calculation time of power flow will increase significantly. In addition, when the power system is stressed in terms of the high levels of active power transmission, the Gauss-Seidel method often has a slow convergence speed and presents a bad convergence result.

The Newton-Raphson method, named after Isaac Newton and Joseph Raphson, is an efficient way to solve the power flow problem with a good convergence rate [41]. In addition, the calculation time shows a linear increase with the increased size of power system. However, this method requires a very good initial estimate to obtain a final globally optimal result, a poor initial estimate can contribute to the non-convergence of the method. If the voltage solution is near to the true solution, the convergence rate will be very quick and the result will be close to the globally optimal result. Therefore, it is suitable for particular applications that require very accurate solutions.

The Fast Decoupled Load Flow (FDLF) method is a variation form of Newton-Raphson method that utilizes the approximate decoupling of active and reactive power flows in well-dehaved power network. In addition, the FDLF method fixes the Jacobian matrix during the iterations in order to reduce the recalculated and refactorized in every iteration. Although the number of iterations will have a certain increase, the calculation process for each iteration will be reduced dramatically. And the requirement of computer memory will be low compared with requirement of the Newton-Raphson method. The convergence rate of FDLF method can also be improved to linear. Furthermore, the FDLF method is less sensitive to the initial estimate conditions than the Newton-Raphson method. However, when the particular system conditions, such as large angles across lines and particular control devices, affect the active and reactive power flow significantly, the Newton-Raphson method with updated Jacobian matrix may be more suitable for adoption.

In the previous discussion, these methods, based on the off-line centralized optimal strategy, require a single control center to have a fully accurate observation of the power system network structure in advance. Hence, such a power system needs a bi-direction information exchange between control center and nodes. The optimization process requires a highly reliable communication process. When some nodes' information is not delivered promptly during the iteration, the entire system may not achieve the iterative result. Meanwhile, the information exchange has a large computation and communication delay which may prevent the objective of real-time optimization. The development of smart grid requires ICT architecture to maximise the system's potential. It is clear that ICT will become an integral part in the next generation of power system, and the decentralized optimization strategy in power system will require the ICT to connect all independent nodes to implement the real-time optimization during the system operation. Furthermore, the uncertainty output power of penetrating DGs also requires the power system to realize the autonomous control in real-time. It is significant to migrate control strategy from a traditional centralized approach to a decentralized approach. As a result, it is crucial to develop algorithms that can not only capture the complexity of big data, but also process huge data in a parallelized or fully decentralized way.

2.2.2 ADMM Based OPF Problem

A simple but powerful iterative algorithm, the alternating direction method of multipliers (ADMM), is well suited to distributed convex optimization problem and in particular to large-scale power system due to the robust and fast convergence results both in theory and practice [42]. Before the current large-scale distributed computing system was proposed, the ADMM has already been developed. It utilizes a decomposition coordination procedure to separate the problem into local subproblems to find a global solution. It is worth emphasizing that the ADMM algorithm is not a new algorithm, but try to blend the advantages of augmented Lagrangian method and dual decomposition method for constrained optimization [43, 44]. This algorithm can be extended to solve many big data problems and provide easy implementation for many applications.

The algorithm of ADMM

ADMM is a blend algorithm that is trying to decompose the global problem into subproblems. The global problem can be written as follows:

$$minimize \;\; f(x) + g(x) \tag{2.2a}$$

$$subject\ to\ Ax + Bz = c. \tag{2.2b}$$

where $A \in \mathbf{R}^{p\times n}$, $B \in \mathbf{R}^{p\times m}$ and $c \in \mathbf{R}^{p}$. $x \in \mathbf{R}^{n}$ and $z \in \mathbf{R}^{m}$ are the variables. We assume that function f and g are convex. The only difference from the general linear problem is that the objective function (2.2a) has two independent variables which are x and z. The optimal value of the problem in (2.2) can be written as:

$$p = inf\{f(x) + g(x) | Ax + Bz = c\}. \tag{2.3}$$

Then the augmented Lagrangian formula can be given by

$$L(x, z, y) = f(x) + g(x) + y^T(Ax + Bz - c) + \tfrac{\rho}{2} \left\| Ax + Bz - c \right\|_2^2. \tag{2.4}$$

where y is the Lagrangian multiplier (dual variable) and ρ is the penalty factor.

Then the ADMM recursive algorithm for k^{th} iterative step can be written as follows

$$x^{k+1} := \arg\min_{x} \mathcal{L}_\rho(x, z^k, y^k) \tag{2.5a}$$

$$z^{k+1} := \arg\min_{z} \mathcal{L}_\rho(x^{k+1}, z, y^k) \tag{2.5b}$$

$$y^{k+1} := y^k + \rho(Ax^{k+1} + Bz^{k+1} - c). \tag{2.5c}$$

where $\rho > 0$. The algorithm contains three steps: x-minimization step (2.5a), z-minimization step (2.5b) and dual variable update step (2.5c).

As in the method of multipliers, the dual variable update uses a step size equal to the penalty factor ρ [45]. However, the augmented Lagrangian is minimized together with two primal variables. The method of multipliers can be defined as follows

$$(x^{k+1}, z^{k+1}) := \arg\min_{x,z} \mathcal{L}_\rho(x, z, y^k) \tag{2.6a}$$

$$y^{k+1} := y^k + \rho(Ax^{k+1} + Bz^{k+1} - c). \tag{2.6b}$$

where the two variables x and z need to be minimized jointly. On the contrary, the ADMM method can update x and z in a sequential way which means the alternating direction term. In other words, the ADMM can be treated as a special form of method of multipliers that can minimize the x and z separately instead of the joint minimization. When the global problem can be separable, the minimization of x and z can be also divided into two steps.

Moreover, the ADMM can be modified slightly to achieve a better and more convenient version, scaled ADMM. The expression of ADMM can be modified as

$$x^{k+1} := \arg\min_{x}(f(x) + \frac{\rho}{2}\left\|Ax + Bz^k - c + u^k\right\|_2^2) \tag{2.7a}$$

$$z^{k+1} := \arg\min_{z}(g(z) + \frac{\rho}{2}\left\|Ax^{k+1} + Bz - c + u^k\right\|_2^2) \tag{2.7b}$$

$$y^{k+1} := y^k + Ax^{k+1} + Bz^{k+1} - c. \tag{2.7c}$$

where $u = \frac{1}{\rho}y$ is the scaled dual variable. We define the residual of the kth iteration as $r^k = Ax^k + Bz^k - c$, then we have

$$u^k = u^0 + \sum_{i=1}^{k} r^i. \tag{2.8}$$

where u^k is the sum of the residuals.

Both two forms are clearly equivalent, but the scaled form (2.7) is usually shorter than the unscaled form (2.5). The unscaled form can be used when the role of the dual variable need to be emphasized.

The convergence of ADMM

There are many literatures that discuss about the convergence issue for ADMM [46]. Here a basic but still general result will be studied for general applications. We propose two assumptions to the convergence issue for ADMM.

Assumption 1. The real value function $f(x)$: $\mathbf{R}^n \rightarrow \mathbf{R} \cup \{+\infty\}$ and function $g(z)$: $\mathbf{R}^m \rightarrow \mathbf{R} \cup \{+\infty\}$ are convex, closed and proper.

Explicitly, this assumption can be shown compactly using the epigraph of a function [47]. $\mathbf{R}^n \rightarrow \mathbf{R}$ is the sets of points lying on or above its graph. And the function f satisfies the assumption 1 if and only if its epigraph $\mathbf{epi}f$ is a closed non-empty convex set.

$$\mathbf{epi}f = \{(x, \mu) : x \in \mathbf{R}^n, \mu \in \mathbf{R}, |f(x) \leq \mu\} \tag{2.8}$$

The assumption 1 indicates that the subproblems $f(x)$ and $g(z)$ can be solved to obtain the minimizations by augmented Lagrangian in (2.5a) and (2.5b)(without further assumptions on A and B). It is important to note that assumption 1 permits function $f(x)$ and $g(z)$ to be nondifferentiable and the value of function can be $+\infty$. We assume that the function $f(x)$ is the indicator function of a closed non-empty convex set $\mathbf{C}$, for example.

$$x = \begin{cases} 0 & x \in \mathbf{C} \\ +\infty & x \nsubseteq \mathbf{C} \end{cases} \tag{2.9}$$

Hence, the x minimization step in (2.5a) will involve solving a quadratic programming under several constraints within a valid domain **C** for function $f(x)$.

Assumption 2. The unaugmented Lagrangian function L_0 has a saddle point.

This assumption 2 can be presented that there is not a necessary unique solution (x^*, z^*, y^*), which has the form for all x, y, z.

$$L_0(x^*, z^*, y) \leq L_0(x^*, z^*, y^*) \leq L_0(x, z, y^*). \tag{2.10}$$

For any saddle point x^*, z^*, y^* with assumption 1, $L_0(x^*, z^*, y^*)$ is $+\infty$. Therefore, it can be found that x^*, z^* are the solution for equation (2.4). Then $Ax^* + Bz^* = c$ and $f(x^*) \leq \infty$, $f(z^*) \leq \infty$. Meanwhile, y^* is a dual optimal point which implies that the optimal results of the dual problem and primal problem are equal. Note that A, B and c have no additional assumption under assumption 1, except under assumption 2. In addition, neither A nor B is needed to be full rank.

Under assumption 1 and 2, the iterative results of ADMM should satisfy as follows

1. Objective convergence: $f(x^k) + g(z^k) \rightarrow p$ for $k \rightarrow \infty$. It means that the objective function of the iterative algorithm ia approaching the optimal solution.

2. Residual convergence: $r^k \rightarrow 0$ for $k \rightarrow \infty$. It means that the iterative algorithm is feasible.

3. Dual variable convergence: $y^k \rightarrow y^*$ for $k \rightarrow \infty$. It means that y^* is a dual optimal parameter.

The proof of the residual convergence and objective convergence results can be found in [48]. Note that we do not need x^k and z^k ($k \rightarrow \infty$) converge to the optimal points.

ADMM-based distributed optimization

Here we present a general consensus version of ADMM algorithm to solve a distributed optimization problem. Consensus issues with ADMM can be found since the 1980s [49]. First of all, we consider a global function with a global variable.

Then the global objective function and variable can be split into N sub-objective functions and constraints.

$$minimize \quad f(z) = \sum_{i=1}^{N} f_i(z). \tag{2.11}$$

where $z \in \mathbf{R}^n$ and $fi : \mathbf{R}^n \to \mathbf{R} \cup \{+\infty\}$ are convex. $f_i(z)$ is the ith sub-objective function. The goal of the global function is to solve the problem in a distributed way that each sub-objective function can be solved by its own parameter.

Assume that we have sub-objective functions $f_1(x_1), \cdots, f_n(x_n)$ with their own local variables $x_i \in \mathbf{R}^n$, $i = 1, ..., n$. Each local variable is made up of a selected components of the global variable $z \in \mathbf{R}^n$, which means each local variable is associated with some global variables $z_{(i,j)}$. Then the consensus between the local variables and global variables can be written as

$$x_i = z_{(i,j)}, i = 1, ..., n, j = 1, ..., m. \tag{2.12}$$

If $z_{(i,j)}$ is equal to z_i, then each local variable x_i is just a copy of global variable which means that the consensus decrease to global variable consensus, $x_i = z_i$. General consensus optimization form implies that each local variable can have a few number of global variables. In Fig. 2.3, the left side is the local independent objective functions with local variables and the right side is the global variables. Fig. 2.3 shows that each local objective function may be associated with a few number of global variables. In this case, there are three sub-objective functions and four global variables. Each local function f_1, f_2, f_3 is associated with 4, 2, 3 global variables, respectively. Each edge implies a consensus constraint between a local variables component and a global variable.

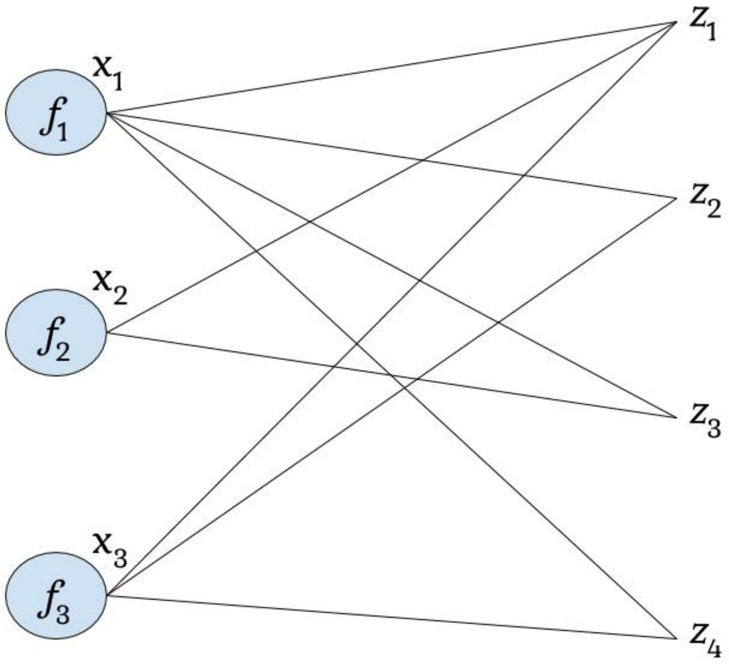


Figure 2.3: The general consensus optimization form.

Assume $\overline{z}_i$ be the global variable of what the local variable x_i should be. Then the general consensus problem with consensus constraint can be given as

$$minimize \quad f(z) = \sum_{i=1}^{n} f_i(x_i) \tag{2.13a}$$

$$subject\ to\ x_i - \overline{z}_i = 0, i = 1, ..., n. \tag{2.13b}$$

Then the augmented Lagrangian for equation (2.13) can be written as follows:

$$L_\rho(x, z, y) = \sum_{i}^{N}(f_i(x_i) + y_i^T(x_i - \overline{z}_i) + \tfrac{\rho}{2}\left\|x_i - \overline{z}_i\right\|_2^2. \tag{2.14}$$

Then the improved ADMM recursive algorithm of node i derived from (2.14) for kth iterative step can be given as:

$$x_i^{k+1} := \arg\min_{x_i}(f_i(x_i) + y_i^{kT}x_i + \frac{\rho}{2}\left\|x_i - \overline{z}_i^k\right\|_2^2) \tag{2.15a}$$

$$z^{k+1} := \arg\min_{x}(\sum_{i=1}^{m}(-y_i^{kT}\overline{z} + \frac{\rho}{2}\left\|x_i^{k+1} - \overline{z}_i\right\|_2^2) \tag{2.15b}$$

$$y_i^{k+1} := y_i^k + \rho(x_i^{k+1} - \overline{z}_i^{k+1}). \tag{2.15c}$$

where the update of x_i and y_i can be achieved independently in parallel for each node i with local constraints. Because the global objective function can be totally separable, then the update of z_i can be decoupled only by the associated global variables.

$$z_i^{k+1} = \frac{\sum\limits_{i=1}^{m^*}(x_{(i,j)}^{k+1} + \frac{1}{\rho}y_{(i,j)}^{k+1})}{m^*}. \tag{2.16}$$

where m^* is the total number of global variables associated to node i. $x_{(i,j)}$ and $y_{(i,j)}$ are the sets of local variables associated to global variable z_i. $x_{(i,j)}^{k+1} + \frac{1}{\rho}y_{(i,j)}^{k+1}$ is the sum of all terms associated to global variable z_i. When each local variable x_i is just a copy of global variable z_i and the same type of argument is applied into the global consensus case, a simple form of z-update can be written as:

$$z_i^{k+1} = x_i^{k+1} + \frac{1}{\rho}y_i. \tag{2.17}$$

In other words, the update of z is the local average value rather than the global average value which could reduce the cost of communication among all independent nodes in a large system. We have discussed ADMM and demonstrated its applicability to distributed convex optimization problem in analysis of modern massive datasets. In such ADMM, the based operations are intend to solve several small convex optimization problems, e.g., a simple quadratic formula. When a very large model problem is required to solve, the ADMM can decrease the global problem to a number of small subproblems. These subproblems can be treated as a coordinated decentralized algorithm to collaborate to solve a large global problem rather than a centralized algorithm. This general form of consensus optimization provides a fully decentralized way to solve a distributed OPF problem in power system.

As can be seen from the ADMM algorithm, there still are certain communications between neighbouring nodes. When time-delay is considered in the ADMM algorithm, the synchronization will become a critical problem. Although the synchronization of all nodes enables the algorithm to be effectively controlled, the communication time delay in a synchronous algorithm will be limited due to the slowest nodes communication transmission. A few papers [22–24] have introduced synchronous communication time-delay system into the decentralized ADMM algorithm, which was based on a master-slave strategy. The proposed algorithms in these papers could still be treated as centralized control approaches. Only when all the information was received by the master, the master would broadcast other nodes to proceed the next step. To analyze the influence of the communication time-delay model on the performance of the iterative results, we will primarily a stochastic end-to-end time-delay model.

2.3 ICT Challenges in the Smart Grid

The next generation of power system has to be rebuilt due to the need of efficiency, flexibility of energy requirement, reliability of power delivery and security of network. In order to manage the loads and demand response system, it should be addressed by collecting and analyzing the information in real time. Therefore, a new emerging concept of smart grid, a complex system with energy, power, sensory, communication, computing and control, is proposed which can utilize the ICT infrastructure to maximise the system potential. One of the main issues to realize the real-time control is time-delay problem. It is a common phenomenon in engineering control and optimization system. The effect of time-delay on the stability of control system has been an important subject of many researches. It is necessary to propose effective strategies to eliminate or minimize the unwanted effects for the control approaches.

2.3.1 Stochastic End-to-end Time-delay

The components of end-to-end delay

During recent decades, the automatic control system has contributed to many problems in the world. It is clear that the investigation of time-delay is a great importance to evaluate the performance of control strategies. The measurement of end-to-end time-delay offers an opportunity to learn about the underlying property of the topology and traffic pattern. Several literatures report the end-to-end time-delay measurement which is based on round-trip time [50–52]. However, these measurements methods do not consider the one-way delay measurements. The end-to-end delay D, a probe-packet over a fixed internet with several routers, can mainly be classified as four components: processing delay D_p, queueing delay D_q, transmission delay D_t and propagation delay D_{prop}.

Processing delay D_p: is the time that the router processes a packet header at each node and prepare to transmit the packet. It is a key component in a network delay and can check for bit errors and determine output link. This delay is determined by the complexity of protocol stack, the available computational ability and link driver. In the past, it is always ignored since the delay is often on the order of 10^{-6} seconds or less. However, in some cases, the processing delay can be large when the router operate a complex encryption algorithms. It can be viewed as a stochastic random value because the probe-packet is not always the same size in terms of the various requirements of the information exchange. Therefore, this delay can be divided into two components: a deterministic delay D_{pd} and a stochastic delay D_{ps}.

Queueing delay D_q: is the time that packet spends waiting in a queue at the buffer of router until it can be executed before transmission. The queueing delay is highly dependent on intensity and nature of traffic arriving at queue. It is typically stochastic in nature in terms of the interference of the probe-packet with other packets on the path. The basic queueing model is presented in Fig. 2.4.

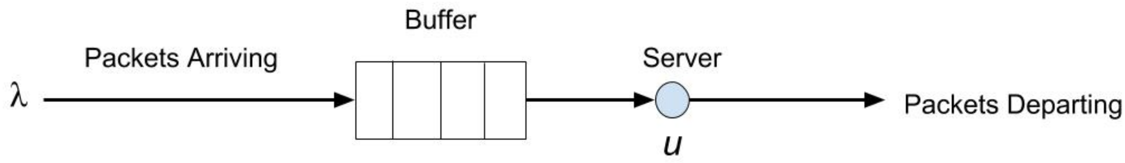


Figure 2.4: The basic queueing model.

A queueing delay model can be characterized by the arrival process of packets, the behaviour of packets, the waiting room, the service times, the service discipline and the service capacity. Kendall's notation is the standard system which is utilized to introduce a queueing model. It is a three-factor code A/B/C which is proposed in 1953 [53]. A specifies the inter-arrival time probability density, B specifies the service time probability density and C specifies the number of servers. For example, M/M/1, M/M/c, M/G/1, G/M/1 and M/D/1. M means the exponential probability density (M is also for Markov), D means all packets have the same value (D stands for deterministic) and G means the general probability density (arbitrary probability density). In a general model, packets arrive one by one and all the packets are permitted to queueing buffer, the buffer size is enough for all the arriving packets and there are no priority rules and the packets are served in order of arrival.

Transmission delay D_t: is the time (also known as store-and-forward delay) that an entire packet is sent out from first bit to last bit into a wire. In other words, the delay is mainly caused by the data rate and capability of the communication link. It is a function of the packet size and has nothing to do with the distance between two routers. This delay can be given by the following formula:

$$D_t = \tfrac{L}{R}. \tag{2.18}$$

where L is the packet size (all of the packet bits) and R is the rate of link transmission. Since this delay is typically on the order of 10^{-6} seconds to 10^{-3} seconds, it can be treated as a same value for each probe-packet.

Propagation delay D_{prop}: is the time that takes for the head of the signal to propagate from the source to the destination at the propagation speed of the link. The time depends on the physical medium of the link. This delay can be computed as:

$$D_{prop} = \tfrac{d}{s}. \tag{2.19}$$

where d is the distance between source and destination, s is the propagation speed of the specific medium. It can be negligible for two routers on the same local area network and significant for two geostationary satellites.

From a measurement point of view, the end-to-end delay over a fixed path consists of two categories: the deterministic (constant) delay D_d and the stochastic delay D_s. Fig. 2.5 shows the histogram of a typical end-to-end communication delay on a link from Amsterdam to London.

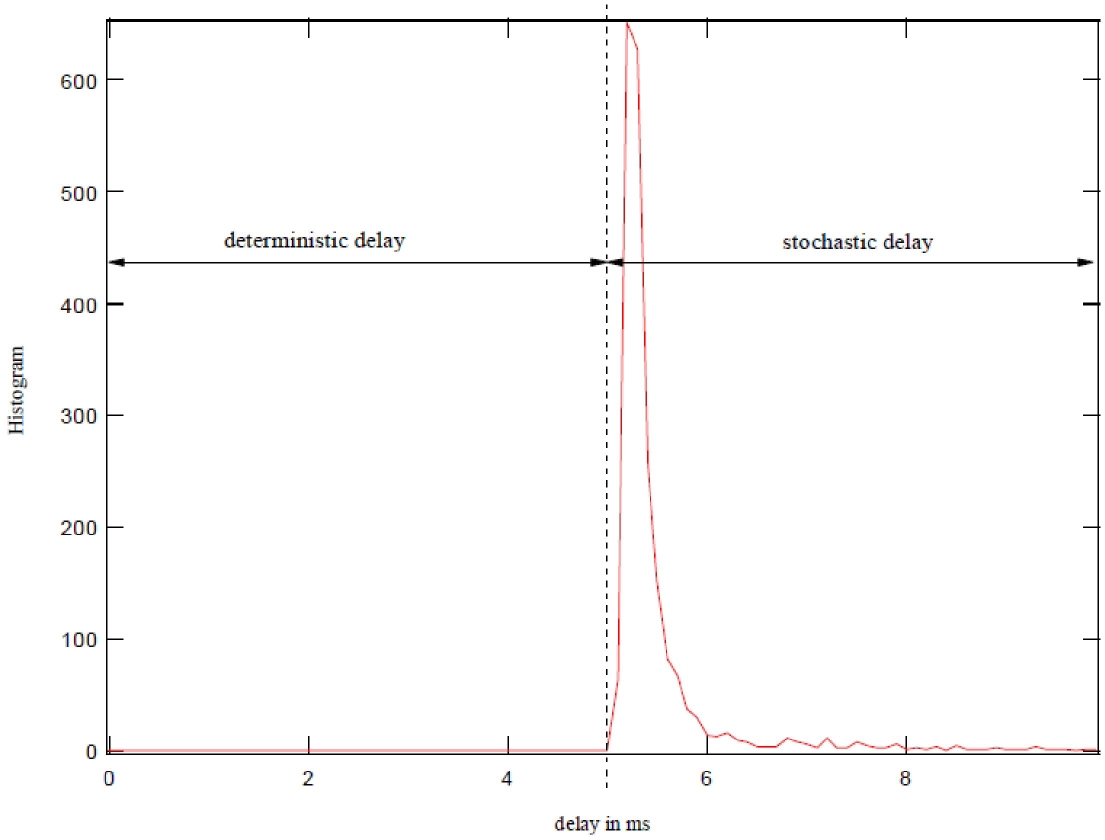


Figure 2.5: The typical delay histogram with the separation into deterministic and stochastic delay [54].

Then we have the description of delay from a measurement point of view as [55]

$$D_d = D_{pd} + D_t + D_{prop} \tag{2.20a}$$

$$D_s = D_{ps} + D_q. \tag{2.20b}$$

The formula (2.20a) presents that the deterministic delay D_d is mainly caused by physical delay, the time between time-stamp generation, the effective start of transmission and the bandwidth of the link. The formula (2.20b) presents that the stochastic delay D_s adds the contributions by the interfering internet traffic (also known as the queueing delay) and the random part of processing delay.

The stochastic analysis of end-to-end delay

The independent sum of delay consists of the minimum deterministic delay, the internet traffic delay and router processing delay. The router processing delay which includes the minimum deterministic delay $\varphi_d(t)$ can be approximated as a Gaussian density. An extensive research [56] assesses the distributions of on-periods and off-periods for internet traffic. There are three proposed parametric models for the stochastic delay D_s caused by the queueing delay which are the exponential model, the Weibull model and the Pareto model.

The exponential density can be obtained by one alternating renewal process with exponential on-periods [56]. The on-period correspond to the periods where the queueing delay has a closure period. This density can be given as

$$\varphi_{exp}(t) = \lambda e^{-\lambda t}, \quad t \geq 0. \tag{2.21}$$

where λ^{-1} is the mean length of the on-period. Then the end-to-end delay can be written as

$$\varphi_(t) = p\varphi_d(t) + \lambda(1-p) \int_{-\infty}^{t} e^{-\lambda(t-s)} \varphi_d(s) ds. \tag{2.22}$$

We assume that the mean μ and standard deviation σ in Gaussian density is known. λ and p can be obtained by the method of maximum likelihood.

When the random time-delay is applied into the real-time research problems, it becomes necessary that the effects of time-delay on the performance of different algorithms are analyzed. Therefore, in this thesis, all the real-time control algorithm will analyze the effects of time-delay and propose an appropriate way to mitigate the effects of time-delay.

2.3.2 Cyber-physical Attack Problem

Time-delay occurs in a wide variety of artificial control system which can affect the stability of the system and reduce system performance. Power system is one of the control systems that is sensitive to the time-delay. Future smart grids will rely mainly on computers and communication systems, which make this type of network vulnerable to cyber-physical attacks. Although electricity supply generation and consumption demand develop rapidly, the underlying power infrastructures have not been updated in unison. It is necessary to observe vast deployment of sensors and actuators on all levels of electrical power system. Research on the attack methods of sensitive infrastructure industrial control systems, the development of countermeasures and security control protocols, has attracted the attention of academia, industry and government. Cyber-physical (CP) system consists of communication, computation, and physical systems and processes. CP security becomes one of the most important issues for a complex network. According to the information and computation resources in the smart grid, malicious attackers can utilize the vulnerabilities of the network to conceive attack plan to endanger the normal operation of the grid. In the meantime, existing investigations have already shown several disastrous consequences which are unprepared by the government, industry and the public [57,58]. Therefore, it is imperative to assess the vulnerability against the CP attacks and emergency response of critical power infrastructure for a comprehensive defence plan.

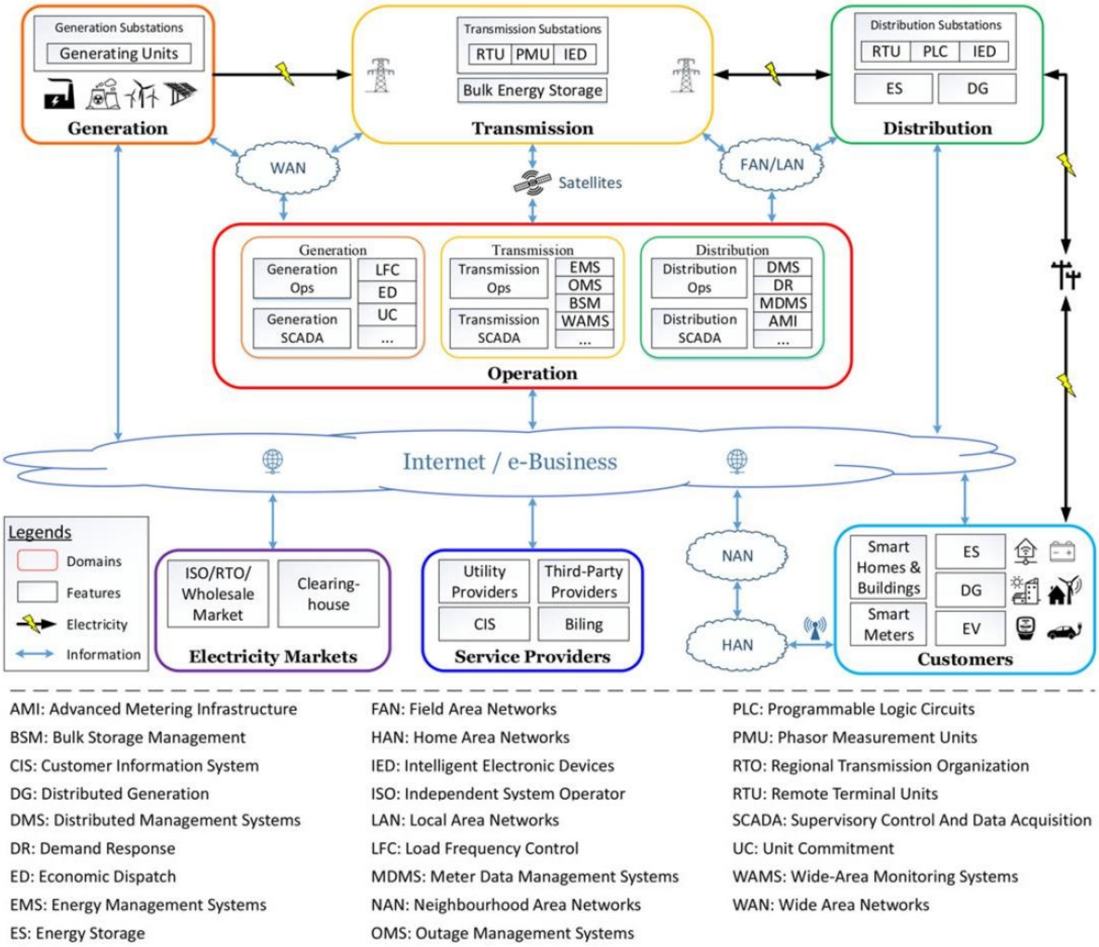
2.3.2.1 Cyber-physical Perspective of Smart Grid

The innovative technologies have transformed the traditional power system to smart grid in several areas, such as distributed energy resources, phasor measurement unit and advanced metering infrastructure system. In addition, the increased energy s-torages and electrical vehicles are changing the current power system. The National Institute of Standards and Technologies (NIST) introduces an overview of smart grid architecture in Fig. 2.6 which contains generation, transmission, distribution, operation, electricity markets, service providers and customers [59]. The communication and computation systems have established cyber infrastructures that are interwoven with the physical system. Based on the measurements, the system operator determines the optimal control strategy and issues control command to execute the actuators cooperatively in the physical system. Sensor measurements are handled by centralized and decentralized equipments deployed at different levels and locations. In traditional power system, system operations are based on the energy management system located in control center. The recent installation of intelligent devices and programmable logical circuits have enhanced the utilization of distributed computation to increase the efficiency and flexibility. The smart grid is introducing new communication standards to accommodate the integration of renewable energy and phase measurement units (PMUs). PMUs measure the electrical waves on a power grid using a common time source for synchronization. In order to increase the efficiency and decrease the investment, smart grid is increasingly dependent on public communication infrastructure. Bi-direction communication between providers and customers is also widely established through the advanced metering infrastructure. Therefore, the security challenges in smart grid are on the rise in both cyber and physical areas [60].

Next, we will briefly talk about the advantages and disadvantages of physical security and cyber security and emphasize the importance of CP security in smart grid. The general structure of cyber-physical system can be found in Fig. 2.7.

1. **Physical security**: The physical security can be protected by evaluating e-mergencies. Contingency analysis, including failures, interruptions and planned outages, could ensure the survivability of the power system with minimum disruptions. However, an emerging interconnected power system poses a challenge to physical security issues. The increasing size of power system will significantly increase the complexity and cost of contingency analysis which makes it difficult to implement contingency analysis as a whole. Without adequate coordination, the remediation in multiple locations may compete with each other rather than collaborate with each other which can also lead to deterioration of cascading failures or blackouts [61]. In the meantime, most equipments and system designs do not have enough security features to prevent bad events

from cyberspace. Hence, lack of adequate protection against coordinated cyber attacks can be catastrophic. It is necessary to design an intelligent and automatic system to increase system security and reliability against the cyber attack in smart grid. The traditional power system security deserves a deep study in the coming era of next generation of power system.



AMI: Advanced Metering Infrastructure
BSM: Bulk Storage Management
CIS: Customer Information System
DG: Distributed Generation
DMS: Distributed Management Systems
DR: Demand Response
ED: Economic Dispatch
EMS: Energy Management Systems
ES: Energy Storage
FAN: Field Area Networks
HAN: Home Area Networks
IED: Intelligent Electronic Devices
ISO: Independent System Operator
LAN: Local Area Networks
LFC: Load Frequency Control
MDMS: Meter Data Management Systems
NAN: Neighbourhood Area Networks
OMS: Outage Management Systems
PLC: Programmable Logic Circuits
PMU: Phasor Measurement Units
RTO: Regional Transmission Organization
RTU: Remote Terminal Units
SCADA: Supervisory Control And Data Acquisition
UC: Unit Commitment
WAMS: Wide-Area Monitoring Systems
WAN: Wide Area Networks

Figure 2.6: The overview of smart grid infrastructure based on the NIST framework [59].

2. **Cyber security**: Cyber security has been identified as an important part of smart grid development [62]. The deployment of Intrusion Detection Systems (IDSs) and firewalls could defend control center and field devices against external intrusion. The safety protocol can also protect the communication system among control center, substations and field devices. Furthermore, AMI and PMU system could obtain secure and reliable communication from

secure wireless communication. However, cyber security is also required to accommodate physical properties of power system. Meanwhile, real-time data flow between neighbouring nodes in smart grid poses tremendous data challenges to network security and further affects power flow calculation of the system [63]. Consequently, it is necessary to add the physical aspects into the cyber security analysis of smart grid.

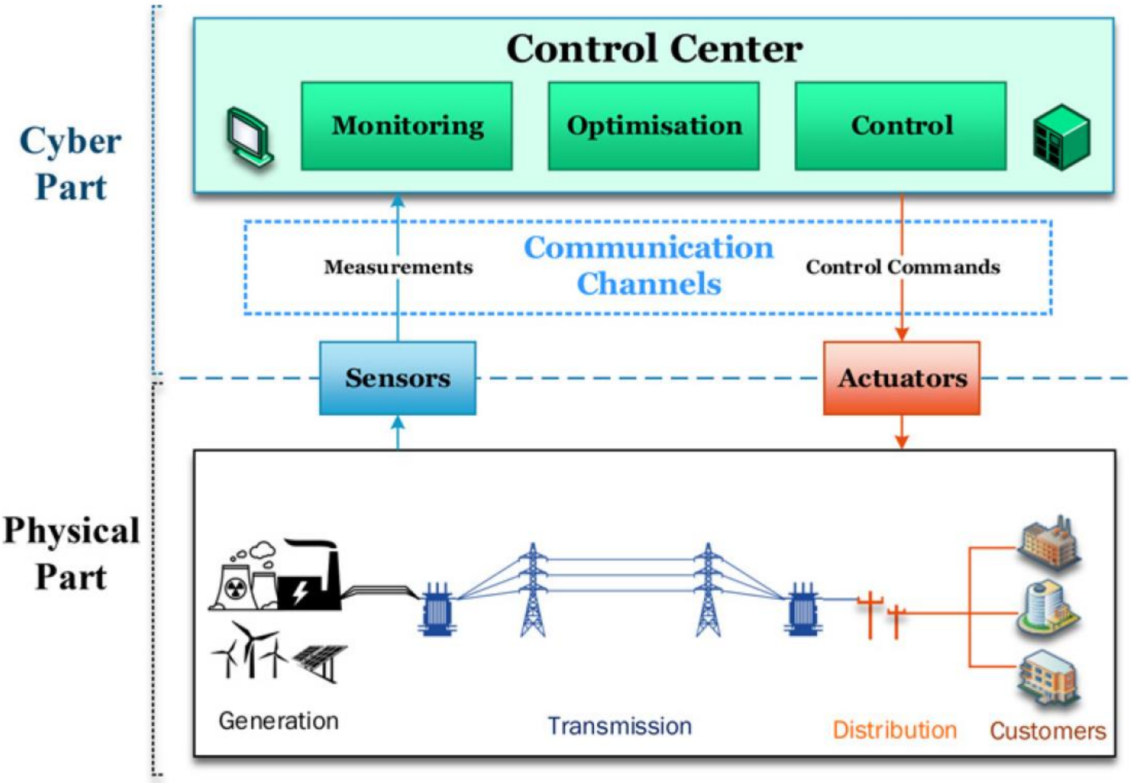


Figure 2.7: The general structure of CP system in smart grid [59].

3. **CP security**: A secure smart grid depends on comprehensive security, which combines the benefits of physical and cyber security analysis in every possible events. It is obvious that the interdependence and interoperability between cyber space and physical space need to be considered to reduce the risk of combined CP attack. The system operators should be aware of the potential risk destroyed by the attacker and propose appropriate ways to mitigate the impact of network attacks. During the security analysis, the vulnerabilities are general revealed by attackers having feasible resources. The investigations of all possible attack events can help to figure out the potential vulnerabilities

of the power system. And these investigations can be used directly to solve the possible CP security problems and enhance the security of the current power system.

2.3.2.2 Cyber-physical Attacks in Smart Grid

This thesis mainly discusses CP security in a smart grid. Both cyber attack and physical attack can pose varying degrees of threat to the security of the power system, the research on the integration of both CP attacks has recently become a popular research direction. There are many reports of cyber intrusions, hacking, unauthorized operations and malicious attacks on the electrical power system, the types of CP attack can be divided into generation system attack, transmission system attack, distribution system attack and electricity market attack.

The generation system widely uses the automatic generation control (AGC) system to adjust the power output of multiple generators at different power plants. Load-frequency control (LFC) and Economic dispatch (ED) are two major functions of the AGC system [64]. ED does not affect the control system directly and LFC is more important to be investigated to avoid possible generator damage. The Aurora attack model, focused on the power generation system and can destroy physical components by a cyber attack, was tested to investigate the vulnerability of the primary controller of AGC system in [65]. The simulation results showed that the attack can eventually destroy the generator completely. A similar CP attack with incomplete information of power system was discussed in [66]. The vulnerability of the secondary controller has also demonstrated the potential effects on system stability. There are four general manipulations on the input of secondary controller, there are scaling, ramping, pulse and random attack [67]. Furthermore, the malicious control signal from LFC can lead to inter-area power swing which causes power shortages or outages [68].

The transmission system mainly delivers electrical power across long distance through transmission lines. There are many investigations on cyber-physical attacks for power transmission grids. The earliest research for a transmission grid is the interdiction attack which means the tripping of generators, lines, transformers and substations in the transmission system. Reference [69] utilizes game theory to defend electrical power systems against interdiction attack. A mixed-integer bilevel programming model is presented to solve the disruptive threat problem [70]. In addition, multiple concurrent tripping has been investigated to show the risk of blackout [71,72]. Both sequential schemes have been used by considering different attack levels and various vulnerabilities. A complex network based attack is another type of attack which utilizes the interdiction as the means of attack. The attacker can only use topological and structural information to identify the vulnerabilities of the transmission grid. Both the topological model [73] and the hybrid model [74] have analyzed the risk of cascaded attacks. The transmission substations have multiple measurement, control and communication facilities. A substation attacks can often lead to the simultaneous loss of the victim substation as well as the transmission line. Cyber security problems of substation system have been comprehensively demonstrated in [75]. Cyber-physical switching attack is also one of the CP attacks against the power transmission grids. An attacker can manipulate switching signals to re-configure power transmissions and switch the power system to an unstable operation state. Reference [76] presents that single switching attack can result in the instability of both frequency and voltage in transmission grid. State estimation (SE) attack is another kind of centralized attack based on the entire system topology structure. The state estimation function can achieve the estimation of the state variables to optimize the system performance [77]. The false data injection attack (FDIA) is often proposed to analyze the vulnerability in the power system. The SE-based FDIA has been discussed that an undetectable attack can be generated to affect the system performance [78,79]. Load redistribution attack, a variant of FDIA, can redistribute the bus load without changing the total load demands to damage the power system operation in different time steps [80,81]. A phasor measurement unit (PMU) is considered to be one of the most important devices in the future of smart grid. However, GPS signal based on time synchronization can also be attacked by manipulating the precise timing information in the transmission system [82].

The distribution system is the final stage in the delivery of power electricity. It carries the electricity from the transmission system to the individual customer. Millions of smart meters have been installed in the demand side and more smart meters will be installed in the future. These smart meters provide bi-link communication between customers and utilities. The security issue of smart meter is one of the important challenges against the cyber-physical attacks [83]. This issue mainly can be identified as energy thefts [84] and information leakages [85]. The former can lead to varying degrees of economic losses, while the latter may be used to infer customer behaviour and information.

The electricity market is a system which enable purchases, sales and short-term trades, generally in the form of electricity price. Bids and offers in electricity market can supply and demand principles to set the price. The locational marginal prices (LMPs), determining the price of electricity, is vulnerable to be attacked through SE function [86]. Many investigations have identified potential schemes for electricity market attacks [87–90].

2.3.2.3 Defence against CP attacks in Smart Grid

The investigation of potential CP attack schemes can be set into three stages: protection, detection and mitigation. Protection mainly depends on establishing secure communications, preserving critical information and mitigating vulnerabilities [91]. A secure communication can effectively remove most of the CP attack threat in smart grid and reduce the threat of FDIA schemes. In addition, the deployment of secured devices on critical location is another way to protect the system when the devices are too expensive to install at all locations in a grid network. Despite the protection measures, attackers can still launch attacks on components that are poorly protected. Hence, intrusion detection systems (IDSs) will be the next major step to defend the smart grid. Early warnings allow system operators to take corrective action to minimize the impacts of attacks. Many detection mechanisms have been developed in CP attack control system [67, 92–96]. When the warning signal of CP attacks are confirmed, the system operators will take mitigation measures to minimize potential disruption and damage. If the attack has been removed from the control system, existing recovery mechanisms can effectively restore power system operations. However, if the threat of attack is not resolved immediately, system operators need to take other measures to mitigate the potential impact of the threat or clear threat. Game theoretic approaches have been improved against CP attack in electrical power system [97]. A three-level decomposition approach is proposed to optimize the economic cost and to mitigate the interdiction attack [98]. This model identifies the most critical network component to defend against possible CP attack-s. For mitigation against FDIA, a coordinated mitigation framework is developed and the security metrics are proposed to quantify the importance of substations and the cost of attacks against measurements [99].

2.3.2.4 The Opportunities and challenges in Smart Grid

A smart grid contains a large number of different devices and is vulnerable to be attacked through cyber-physical structures. Although many researchers have conducted extensive research on CP attacks, the vulnerability of most components in a smart grid still requires check in case of potential attacks. Demand response and distributed intelligence may also become one of the most attractive targets for CP attack in the smart grid network. In addition, there are still many potential unknown threats. The integration of energy storage, distributed generation and electric vehicles will create uncertain changes which may cause instability and catastrophic damage to electrical power system.

The challenges of CP attack for future smart grid can be divided into four main areas: interdependence, temporal vulnerability, practical attacks and designs of attack-resilient.

1. **Interdependence**: Interdependence is the driving force of security development in a smart grid. So far, most CP attacks launch attacks in cyber space and few investigations are found in physical network. However, the threat can be disruptive when physical system is considered. The vulnerabilities of physical system should also be investigated in smart grid CP security. At the same time, the vulnerabilities of interdependence may also be used fre-

quently to manipulate the communication data or historical information to induce a power outage or further damage to some critical field devices. To date, such kind of investigation has remained limited. The interdependence of smart grid does not only mean the connection between cyber and physical space, other critical infrastructures are also vulnerable as shown in Fig. 2.8. Smart grid could interconnect actuating devices and monitoring devices such as circuit breakers, relays, transformers, smart meters and PMUs by way of intelligent signal processing technologies. These devices can communicate, perform control strategies locally and intelligently actuate. The information-centric cyber-enabled smart grid allows active nodes to respond to intelligent signal processing effectively and adaptively. These frequently changed information can be intercepted through cyber channels. Therefore, the revealing information about the network structure and operating trends can be gleaned by an attacker and be utilized to perpetrate an insidious CP attack during the system operation. The investigation of interdependence across infrastructure still has a lot of work to be done.

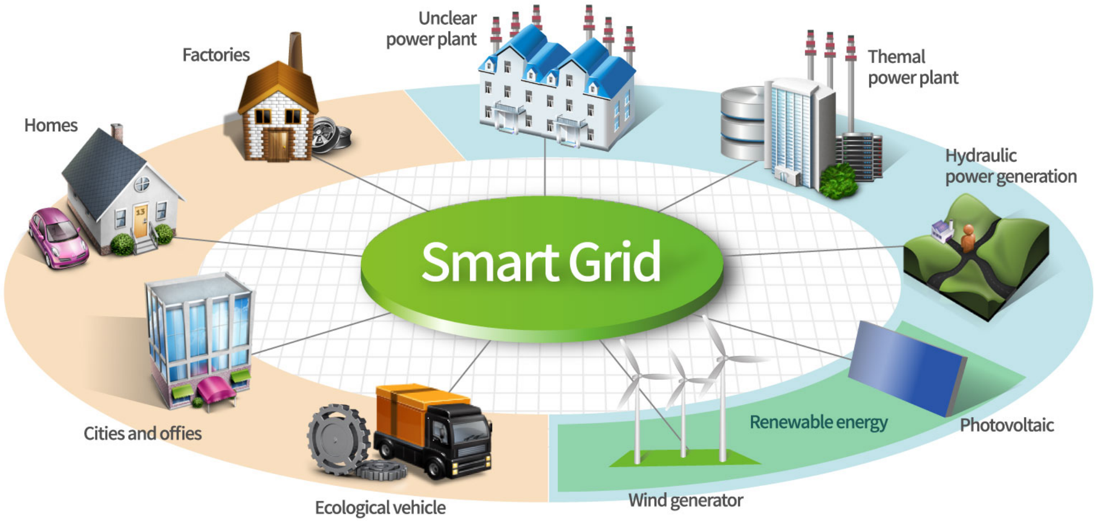


Figure 2.8: The overview of smart grid security market [100].

2. **Temporal vulnerability**: In general, a coordinated intrusion of multiple-devices can be initiated in a simultaneous manner, timing is not often considered in terms of the complexity of time domain. However, in practice, the

timing of attack is very important to the potential impact of a CP attack. Attacks during either peak or off-peak times are likely to have different effects on system stability. The timing and sequence of coordinated attacks will play an important role in the system blackout. Therefore, it is necessary for the timing factor to be analyzed for power system network to confirm system stability at the right time.

3. **Imperfect attacks**: The worst case study is often simulated to evaluate the potential impacts of control system. These studies are very important to demonstrate the possible maximal damage of the system. These studies which call perfect attacks usually contain all network information and control of the system. However, these perfect attacks are not feasible in real world scenario. The system operator may be faced with more imperfect attacks and some of which may be completely unknown. Therefore, it is necessary to consider incomplete information to investigate and evaluate all possible attacks due to limited information and limited available resources. According to the level of security, knowledge of the system and control compromised by the attackers, the corresponding hierarchical countermeasures should be proposed to mitigate the potential threats.

4. **Designs of attack-resilience system**: Due to the inability to eliminate each possible attack for a smart grid, the concept of attack-resilient should be proposed to mitigate all the potential threats. When the control and measurement systems are designed, it should be noted that the security features are crucial to the stability of the electrical power network. The intelligence devices in smart grid are not just the targets of the CP attacks, they can also be the tool to defend the threats. In terms of the upgrade of power system, the integration of all intelligence devices can enhance the flexibility of its own protection and be developed to improve the security of potential threats.

2.4 Conclusions

This chapter first gives an overview of voltage control techniques in power system, including traditional voltage control methods and reactive power voltage control methods. Next, the overview of OPF algorithms is presented, followed by the ADMM-based optimization algorithm. The modelling studies on the general consensus version of ADMM algorithm are reviewed in this chapter. Then, the IC-T challenges in smart grid are discussed, including the stochastic communication time-delay and the studies on the CP attack in the literature.

Computer modelling is not representative to real world scenarios due to the uncertainties of input values and the communication between the computer model and real world. More different scenarios are required to be simulated. In order to simulate real scenario in the reactive power control system, it is necessary to quantify the uncertainty of input values and addition the stochastic communication time-delay model into computer models. In order to systematically and efficiently manage the uncertainty of input and communication delay, it is necessary to create an appropriate strategy to mitigate all the possible damages that may be caused by the uncertainties. Finally, cyber-physical attacks during the information exchange need to be highly evaluated when the smart grid is developed in the future.

Chapter 3

Coordinated Reactive Power Voltage Control Model

3.1 Introduction

In order to reduce carbon dioxide emissions, deal with the growing world population, the decreasing fossil fuels and the rising energy demands, the increasing installation of DGs is a promising solution. Current hierarchical power system needs to be modified to adapt the large penetration of distributed generators for electrical energy. However, these DGs will destabilize the dynamic performance of electrical network. One of the main challenges is that an appropriate control method to stabilize the voltage in real-time is required to solve voltage fluctuation due to the unpredictable output power of DGs. There are several different traditional voltage control methods (see Section 2.1), such as, On-Load Tap Changer (OLTC), Step Voltage Regulator (SVR) and Static Var Compensator (SVC). However, these methods have certain limitations, such as fixed locations, harmonic generation, high investigation and additional failure points when the network is upgraded [28]. Considering the requirement of real-time control, low cost benefit ratios and flexibility of reactive power, we propose to utilize the electronic inverter in DGs based on the sensitivity analysis to regulate the voltage level. It is noteworthy that the proposed decentralized voltage control method in this chapter considers neighbouring nodes to optimize the reactive power allocation which can increase the total amount of controllable reactive power for a single node voltage control. In addition, the time-delay analysis is also considered to test the performance of the method.

This chapter mainly analyzes the the performance of coordinated decentralized reactive power voltage control strategy combined with the time-delay model. The contributions of this chapter are summarised as follows:

- Given the little literature in the research of analysing communication time-delay in smart grid so far, this chapter links an imperfect communication system to a coordinated voltage control strategy. This investigation provides a possible research direction to decentralized control algorithm with limited information exchange.

- The time-delay analysis is presented to show the impact of communication time-delay on the performance of a coordinated voltage control strategy.

- Simulation results show that, with time-delay, existing approaches cannot control the voltage level as expected and thus may affect the system stability. The existing control method needs to be modified to mitigate the impact of the time-delay introduced by communication systems.

The rest of the chapter is structured as follows. The sensitivity analysis and maximum capability of inverter for each according to the converter current and voltage limitations are both discussed in Section 3.2. Section 3.3 describes the proposed modelling of coordinated reactive power control method. When time-delay occurs during the information exchange, Section 3.4 derives the time-delay modelling into the proposed method. The simulation results are given in Section 3.5, followed by the chapter summary in Section 3.6.

3.2 Methodology for Reactive Power Control

Many methods can be used to maintain the voltage level. This section explores a coordinated control strategy to adjust the reactive power absorption/injection to regulate the node voltage. In a decentralized method, the limited information exchange still exists in contrast to centralized control manner. However, decentralized control strategy does not need a control center to gather all the network information to realize the control. The sensitivity matrix and power capability of inverter are the key points in the reactive power control strategy.

3.2.1 Network Sensitivity Analysis

The classical sensitivity theory, based on the Jacobian matrix, was utilized in high-voltage (HV) transmission network to perform the voltage regulation [101]. This method is known as the Newton-Raphson method which is written as a Taylor Series with the higher order term ignored. The relationship between the node voltages (magnitude $\triangle V$ and angles $\triangle\theta$) and node injection power (active power $\triangle P$ and reactive power $\triangle Q$) can be expressed as:

$$\begin{bmatrix} \triangle V \\ \triangle\theta \end{bmatrix} = -J^{-1} \begin{bmatrix} \triangle Q \\ \triangle P \end{bmatrix}. \tag{3.1}$$

where $\triangle P$ and $\triangle Q$ are the deviations of absorbed/injected active power and reactive power, respectively. J is the matrix of partial derivatives known as the Jacobian matrix (also called sensitivity matrix). The detail can be written as

$$\triangle P_i = -P_i + \sum_{k=1}^{N} |V_i|\,|V_k|\,(G_{ik}cos\theta_{ik} + B_{ik}sin\theta_{ik}) \tag{3.2a}$$

$$\triangle Q_i = -Q_i + \sum_{k=1}^{N} |V_i|\,|V_k|\,(G_{ik}sin\theta_{ik} - B_{ik}cos\theta_{ik}) \tag{3.2b}$$

$$J = \begin{bmatrix} \frac{\partial\triangle Q}{\partial V} & \frac{\partial\triangle Q}{\partial\theta} \\ \frac{\partial\triangle P}{\partial V} & \frac{\partial\triangle P}{\partial\theta} \end{bmatrix}. \tag{3.2c}$$

where (3.2a) and (3.2b) are called the mismatch equations. The method described above is generally valid, however, its computational complexity is too great for realistic voltage analysis. For radial distribution network (DN), only voltage magnitude is required to control the voltage level. Therefore, the simple sensitivity theory is proposed to our medium voltage distribution network (MVDN). The proposed theory is easier than normal theory and it is only suitable for the radial network.

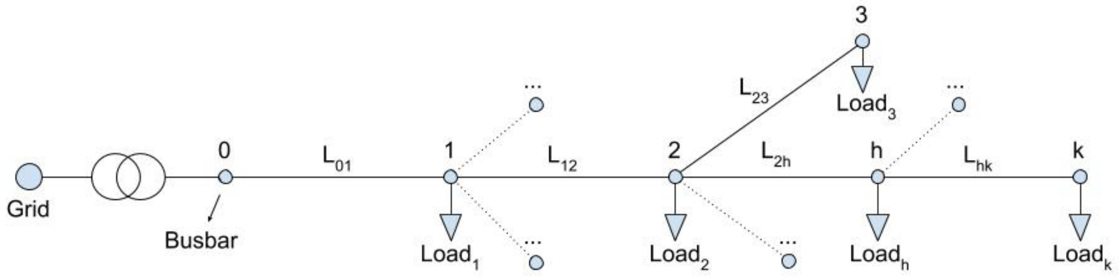


Figure 3.1: The tested network for proposed sensitivity theory

Let us consider the single-phase equivalent circuit of DN in Fig 3.1, which consists of N nodes. The MV busbar is considered at node 0, the numberings of other nodes are presented in Fig 3.1. The branch $L_{01}, L_{12}, ...$ are modelled using the RL-direct sequence equivalent circuit [102] (assuming the shunt parameters are neglected). The reference voltage level E_0 is a constant value set by the OLTC. In a radial DN, the MV busbar voltage is regulated at E_0, the voltage deviation V_{0i} between node 0 and node i can be given by:

$$V_{0i} = E_0 - E_i. \tag{3.3}$$

where V_{0i} can be treated as the sum of voltage deviation between neighbouring nodes from node 0 to node i. For example, if $i = 3$, the voltage deviation V_{03} can be calculated as the sum of voltage deviations V_{01}, V_{12} and V_{23}

$$V_{03} = V_{01} + V_{12} + V_{23}. \tag{3.4}$$

We define PT_i is the set of path from node 0 to node i. $h, k \in PT_i$ means node h and k are the neighbouring nodes which connect to one branch. If i equals to 3, the path PT_3 contains three branches which is $0-1$,$1-2$ and $2-3$ seen in Fig 3.1. The generalised voltage deviation function can be written as,

$$V_{0i} = \sum_{hk \in PT_i} V_{hk}. \tag{3.5}$$

For each branch voltage deviation V_{hk}, the relationship between voltage level and power flow can be given as [3],

$$\begin{aligned} V_{hk} = E_h - E_k &= R_{hk} I_{Sk} cos\varphi_{Sk} + X_{hk} I_{Sk} sin\varphi_{Sk} \\ &= \frac{E_k R_{hk} I_{Sk} cos\varphi_{Sk} + E_k X_{hk} I_{Sk} sin\varphi_{Sk}}{E_k} \\ &= \frac{R_{hk} P_{Sk} + X_{hk} Q_{Sk}}{E_k}. \end{aligned} \tag{3.6}$$

where R_{hk}, X_{hk}, and I_{Sk} are the branch resistance, reactance and current, respectively. P_{Sk} and Q_{Sk} are the active and reactive power flow from node h to node k, respectively. $cos\varphi_{Sk}$ is the power factor. And E_k is the voltage level at node k.

Normally, the voltage level at node k is close to rated voltage value $1p.u.$, so (3.6) can be approximated as:

$$V_{hk} \approx \tfrac{R_{hk} P_{Sk} + X_{hk} Q_{Sk}}{1} = R_{hk} P_{Sk} + X_{hk} Q_{Sk}. \tag{3.7}$$

We assume that the power loss is negligible compared to the load powers. Then active power P_{Sk} and reactive powers Q_{Sk} can be approximated as follows:

$$P_{Sk} \approx \sum_{q \in DE_k} P_q \tag{3.8a}$$

$$Q_{Sk} \approx \sum_{q \in DE_k} Q_q. \tag{3.8b}$$

where P_q and Q_q are the active power and reactive power of the loads connected downstream of node k, respectively. DE_k is the set of active and reactive powers of loads that installed downstream of node k.

Therefore, we can derive that the voltage deviation V_{0i} is a function of active power and reactive power of all loads. The voltage level of node i can be obtained in this way:

$$\begin{aligned} E_i = E_0 - V_{0i} &= E_0 - \sum_{hk \in PT_i} V_{hk} \\ &= E_0 - \sum_{hk \in PT_i} (R_{hk}P_{Sk} + X_{hk}Q_{Sk}) \\ &= E_0 - \sum_{hk \in PT_i} (R_{hk} \sum_{q \in DE_k} P_q + X_{hk} \sum_{q \in DE_k} Q_q). \end{aligned} \tag{3.9}$$

E_0 is the constant value, and we can rewrite the (3.9) as:

$$E_i = F(\mathbf{P}, \mathbf{Q}). \tag{3.10}$$

where **P** and **Q** are the active power sets $P_1, P_2, ..., P_N$ and reactive power sets $Q_1, Q_2, ..., Q_N$, respectively. The active and reactive powers are the control variables. When we change the active and reactive powers, the voltage level of each node will be changed accordingly. According to equation (3.10), the voltage variation $\triangle E_i$ of node i can be given as

$$\begin{aligned} \triangle E_i &= \frac{\partial E_i}{\partial P_1} \triangle P_1 + \frac{\partial E_i}{\partial P_2} \triangle P_2 + ... + \frac{\partial E_i}{\partial P_N} \triangle P_N \\ &+ \frac{\partial E_i}{\partial Q_1} \triangle Q_1 + \frac{\partial E_i}{\partial Q_2} \triangle Q_2 + ... + \frac{\partial E_i}{\partial Q_N} \triangle Q_N \\ &= \sum_{J=1}^{N} \frac{\partial E_i}{\partial P_j} \triangle P_j + \sum_{J=1}^{N} \frac{\partial E_i}{\partial Q_j} \triangle Q_j. \end{aligned} \tag{3.11}$$

where $\frac{\partial E_i}{\partial P_j}$ and $\frac{\partial E_i}{\partial Q_j}$ are the gain of the voltage variation to node i cased by the active and reactive power variations in node j, respectively. This partial derivative can be called as the sensitivity term. Moreover, we can derive the general sensitivity matrix for all nodes in the network:

$$\begin{bmatrix} \triangle E_1 \\ \triangle E_2 \\ \cdots \\ \triangle E_N \end{bmatrix} = \begin{bmatrix} \frac{\partial E_1}{\partial P_1} & \frac{\partial E_1}{\partial P_2} & \cdots & \frac{\partial E_1}{\partial P_N} \\ \frac{\partial E_2}{\partial P_1} & \frac{\partial E_2}{\partial P_2} & \cdots & \frac{\partial E_2}{\partial P_N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial E_N}{\partial P_1} & \frac{\partial E_N}{\partial P_2} & \cdots & \frac{\partial E_N}{\partial P_N} \end{bmatrix} \begin{bmatrix} \triangle P_1 \\ \triangle P_2 \\ \cdots \\ \triangle P_N \end{bmatrix} + \begin{bmatrix} \frac{\partial E_1}{\partial Q_1} & \frac{\partial E_1}{\partial Q_2} & \cdots & \frac{\partial E_1}{\partial Q_N} \\ \frac{\partial E_2}{\partial P_1} & \frac{\partial E_2}{\partial Q_2} & \cdots & \frac{\partial E_2}{\partial Q_N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial E_N}{\partial Q_1} & \frac{\partial E_N}{\partial Q_2} & \cdots & \frac{\partial E_N}{\partial Q_N} \end{bmatrix} \begin{bmatrix} \triangle Q_1 \\ \triangle Q_2 \\ \cdots \\ \triangle Q_N \end{bmatrix}. \tag{3.12}$$

The simplified form of equation (3.12) can be written as

$$\begin{bmatrix} \triangle \mathbf{E} \end{bmatrix} = \begin{bmatrix} \mathbf{s}_P \end{bmatrix} \begin{bmatrix} \triangle \mathbf{P} \end{bmatrix} + \begin{bmatrix} \mathbf{s}_Q \end{bmatrix} \begin{bmatrix} \triangle \mathbf{Q} \end{bmatrix}. \tag{3.13}$$

where $\triangle \mathbf{E}$ is the voltage variation vector. $\triangle \mathbf{P}$ and $\triangle \mathbf{Q}$ are the active and reactive power variation vectors, respectively. $\mathbf{s}_P$ and $\mathbf{s}_Q$ are the active and reactive sensitivity parameter matrix, respectively

It is important to note if the active and reactive power at node j do not change at the moment, then $\triangle P_j = 0$ and $\triangle Q_j = 0$. In this section, we give priority to consider the reactive power variation, which also means only reactive powers of DG nodes are regulated to maintain the voltage level of each node. According to the equation of sensitivity parameter matrix, it is obvious when we select one DG node as the main node, the farther away from the main node, the smaller the voltage variation for same reactive power deviation. Next, we will consider how to regulate the reactive power output through the power electronic inverter.

3.2.2 Active/Reactive Power Capability of Inverter

In general, the DG is installed to the DN by means of electronic inverter. Among the decentralized voltage control methods using the reactive power output of DGs, the maximum capability performance of inverter which could control the output value of active power and reactive power has recently been researched. Reactive power regulation from DGs can not only directly control the voltage level in real-time, but also reduce the requirement of extra reinforcements from the network. The typical layout of DG with power electronic converter is presented in Fig 3.2.

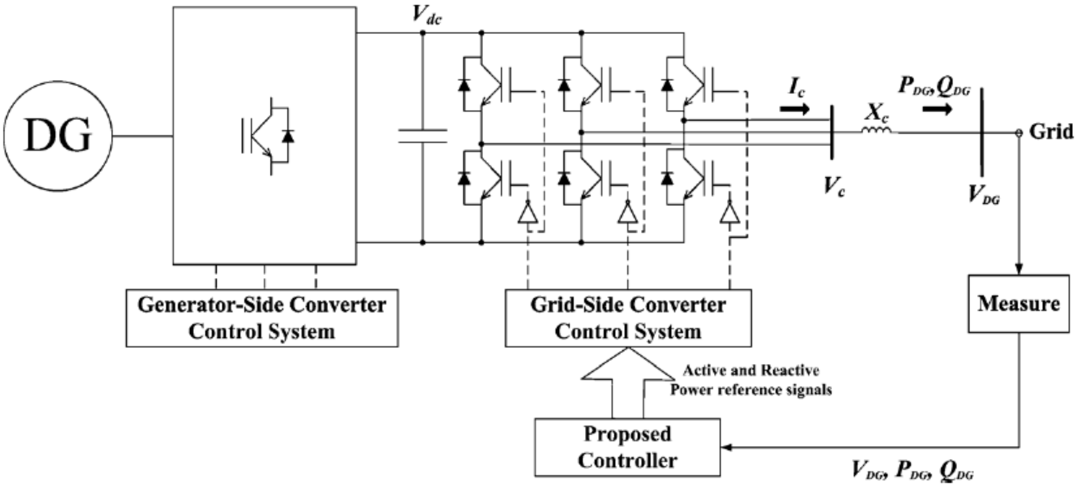

DG
V_{dc}
I_c
X_c
P_{DG}, Q_{DG}
Grid
V_c
V_{DG}
Generator-Side Converter Control System
Grid-Side Converter Control System
Measure
Active and Reactive Power reference signals
Proposed Controller
V_{DG}, P_{DG}, Q_{DG}

Figure 3.2: Outline of control system with power electronic converter

The grid-side converter has a certain maximum current-carrying capacity, which will impose a limit on the active and reactive power capability of DG. In Fig 3.3, the PQ plane of DG, for example, PV array and wind turbine, is similar to a synchronous generator [1]. The relationship between the active power P^c_{DG} and reactive power Q^c_{DG} under the converter current limit is

$$P^c_{DG}{}^2 + Q^c_{DG}{}^2 = (V_{DG} I_c)^2. \tag{3.14}$$

where I_c is the converter-side current. V_{DG} is the grid-side voltage. V_{DG} is not a constant value. If V_{DG} increases, I_C will decrease and vice versa.

Another limitation of the power capability is the converter voltage V_c, which is similar to the field current limit of a traditional synchronous generator. Then the relationship between the active power P^v_{DG} and reactive power Q^v_{DG} under the converter voltage limit is

$$P^v_{DG}{}^2 + (Q^v_{DG} + \tfrac{V_{DG}^2}{X_c})^2 = (\tfrac{V_{DG} V_c}{X})^2. \tag{3.15}$$

where V_c is the convert-side voltage. X_c is the total equivalent reactance of the

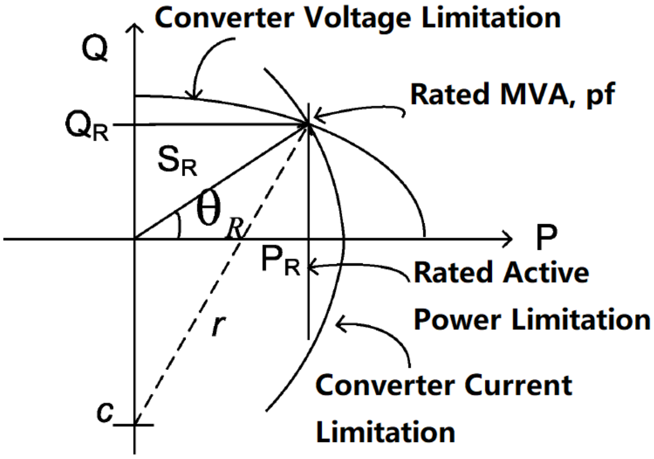


Figure 3.3: Capability curve with power electronic converter

transformers and grid filters from converter side to grid side (seen in Fig. 3.2).

In Fig 3.3, equation (3.14) represents the curve of converter current limitation and equation (3.15) represents the curve of converter voltage limitation. In addition, for converter voltage limitation, the equation (3.15) shows a circle with center c and radius r. The maximum reactive power output not only meets the constraints of converter current and voltage limitations, but also be determined by the current maximum output of active power. In order to calculate the maximum value of reactive power output, it is necessary to set a certain band of voltages and frequencies at the grid connection point. Let us define the $X_c = 0.3$, $V_{DG,max} = 1.05p.u.$, $V_{DG,min} = 0.95p.u.$, $f_{max} = 1.01p.u.$, $f_{min} = 0.98p.u.$ [103]. And θ_R is the rated power factor angle. In term of these parameters, we can calculate the maximum value of converter voltage and current. The converter current I_c in (3.14) can be written as

$$I_c = \frac{\sqrt{{P_{DG}^c}^2 + {Q_{DG}^c}^2}}{V_{DG}}. \tag{3.16}$$

where the active power P_{DG}^c and reactive power Q_{DG}^c are rated values, and the DG output voltage V_{DG} is the minimum value, the maximum value of converter current can be obtained.

$$I_{c,max} = \frac{\sqrt{{P^c_{DG,R}}^2 + {Q^c_{DG,R}}^2}}{V_{DG,min}} = \frac{\sqrt{{P^c_{DG,R}}^2 + {P^c_{DG,R} tan\theta_R}^2}}{V_{DG,min}}. \tag{3.17}$$

where $P^c_{DG,R}$ and $Q^c_{DG,R}$ are the rated active and reactive power, respectively. Then the maximum converter current $I_{c,max}$ can be converted into the format of p.u. by considering $P_{DG,R}$ as the base of the system

$$I_{c,max} = \frac{\sqrt{1 + tan^2\theta_R}}{V_{DG,min}}. \tag{3.18}$$

Then the converter voltage in (3.15) can be written as

$$V_c = \frac{X_c}{V_{DG}} \sqrt{{P^v_{DG}}^2 + (Q^v_{DG} + \frac{{V_{DG}}^2}{X_c})^2} = \frac{X_c}{V_{DG}} \sqrt{{P^v_{DG}}^2 + (P^v_{DG} tan\theta + \frac{{V_{DG}}^2}{X_c})^2}. \tag{3.19}$$

where the active power P^v_{DG} and reactive power Q^v_{DG} are rated values, and the DG voltage V_{DG} is the maximum value. The maximum converter voltage in p.u. can be given by

$$V_{c,max} = \frac{f_{max} X_c}{V^v_{DG,max}} \sqrt{1 + (tan\theta_R + \frac{{V_{DG,max}}^2}{f_{max} X_c})^2}. \tag{3.20}$$

According to (3.14), (3.15), (3.18) and (3.20), we can obtain the maximum reactive power output value by

$$Q^c_{DG} = \sqrt{(I_{c,max} V_{DG})^2 - {P^c_{DG}}^2} \tag{3.21a}$$

$$Q^v_{DG} = \sqrt{(\frac{V_{DG} V_{c,max}}{X_c})^2 - {P^v_{DG}}^2} - \frac{V^2_{DG}}{X_c}. \tag{3.21b}$$

where Q^c_{DG} and Q^v_{DG} are the maximum reactive power output by the limitation of maximum converter current and limitation of maximum converter voltage, respectively.

For different active power output value, the maximum reactive power output will be different with respect to the limitations. Combining (3.21a) and (3.21b), the maximum available reactive power capability can be given by

$$Q = \min\left(Q_{DG}^{c}, Q_{DG}^{v}\right). \tag{3.22}$$

According to the equation (3.22), with different active power output of DGs, each DG can adjust the power factor to absorb or inject the reactive power into the node to control the voltage level. Fig. 3.4 presents the reactive power capability curve under different power factor points. This curve explains that each number of active power with specific power factor working point has the maximum reactive power output. In other words, if the maximum reactive power injection/absorption can not maintain the node voltage into the operation point, it is necessary to curtail the active power output because of the constraint of bus voltage level. Consequently, the controllable P/Q capability curve is an important part for distribution generator to control reactive power output.

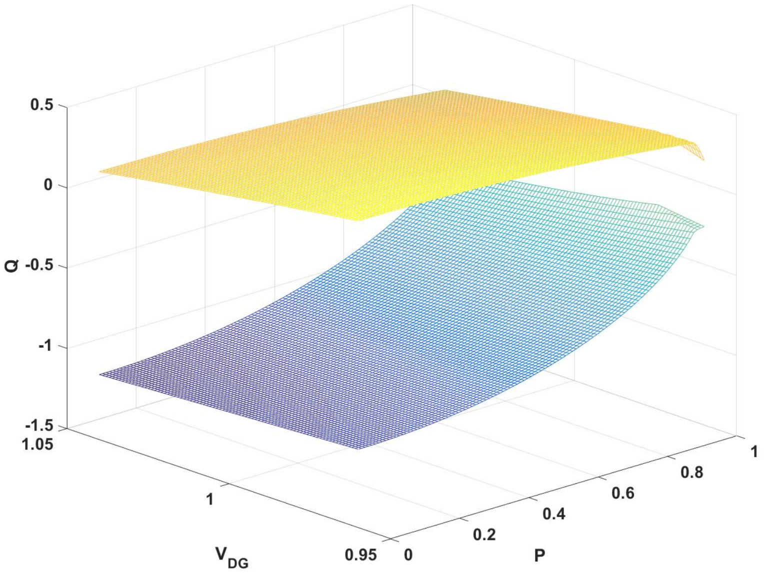


Figure 3.4: Reactive power capability curve.

3.3 Proposed Model of Coordinated Voltage Control Method

This section will present the coordinated voltage control strategy by controlling the active and reactive power between DGs. According to the above sensitivity coefficient matrix and the capability of power output, each DG can control the active and reactive power to regulate the voltage level. Reference [12] presents an independent voltage control strategy which only considers self-node's voltage regulation without any cooperation. However, if one DG is out of service or when other extreme situation occurs, the voltage of this node will be out of control by self node and only neighbouring nodes can control the voltage level. In the meantime, the independent control strategy will also be affected and may not be able to adjust the voltage to within the specified range. Hence, we propose a coordinated voltage control method which will control the voltage level cooperatively with neighbouring nodes and extend the controllable range. Meanwhile, it can prevent the disadvantage that the voltage level can not be controlled when the DG of main node loses its ability to work.

According to the sensitivity analysis, it is obvious that the active/reactive power output of each DG can both impact other nodes' voltage levels. We define a concept of Most Influential Generator (MIG) here. When node i is considered as the main node (MN), each DG in this network can regulate its own active/reactive power to control voltage level of node i. In terms of sensitivity parameters, the closer the distance from the node i, the greater the impact on the voltage level of node i. Therefore, we prefer to choose neighbouring DGs to regulate the voltage level cooperatively.

In this cooperative decentralized control approach, when DGs are connected to nodes and the network parameters are fixed, each node will have a constant sensitivity coefficient. Under normal conditions, we only consider to change the reactive power output to regulate the voltage level. In case reactive power output reaches the maximum value, the active power curtailment will be considered. The main voltage variation of node i can be shown as

$$\triangle V_i^P = \frac{\triangle P_{i1}^{DG}}{\rho_{i1}^P} + \frac{\triangle P_{i2}^{DG}}{\rho_{i2}^P} + ... + \frac{\triangle P_{iM}^{DG}}{\rho_{iM}^P} \tag{3.23a}$$

$$\triangle V_i^Q = \frac{\triangle Q_{i1}^{DG}}{\rho_{i1}^Q} + \frac{\triangle Q_{i2}^{DG}}{\rho_{i2}^Q} + ... + \frac{\triangle Q_{iM}^{DG}}{\rho_{iM}^Q}. \tag{3.23b}$$

where ρ_{i1}^P, ρ_{i2}^P,...,ρ_{iM}^P are the active power sensitivity coefficients of node i, respectively. ρ_{i1}^Q,ρ_{i2}^Q,...,ρ_{iM}^Q are the reactive power sensitivity coefficients of node i, respectively. ΔP_{i1}^{DG}, ΔP_{i2}^{DG},..., ΔP_{iM}^{DG} are DG active power variations, respectively. ΔQ_{i1}^{DG}, ΔQ_{i2}^{DG},..., ΔQ_{iM}^{DG} are DG reactive power variations, respectively. ΔV_i^Q, ΔV_i^P are voltage variation due to ΔQ_{DG} and ΔP_{DG}, respectively.

In general, the reactive power variations of neighbouring DGs will have the largest influence on the MN. The control strategy will control the voltage level cooperatively with neighbouring DGs. The outline of control strategy can be found in Fig. 3.5. The red box is the core of cooperative control part which can enlarge the controllable range of reactive power compensation. The detail is discussed as follows:

First of all, the measuring equipment will always detect the voltage level of DG node i and send the current detected parameters to neighbouring DG. The detected voltage deviation between current voltage level $V_i(k)$ and threshold value can be given by

$$\Delta V_i(k) = V_i(k) - (V_i^{max} - \varepsilon_i). \tag{3.24}$$

where k is the time step for each loop, V_i^{max} and ε_μ are the upper limit voltage value and upper threshold value of node i, respectively. The value for each ε_i is different and depended on the location of node in the network.

If the voltage of main DG (MDG) node exceeds the specified maximum or minimum value(we set the maximum voltage level 1.05 p.u. and the minimum voltage level 0.95 p.u.), the power electronic inverter will take action to regulate the reactive power output to adjust the voltage level into the operative range. At the beginning of control strategy, only reactive power compensation will be considered. In terms of the reactive power capability and sensitivity coefficients, the maximum allowed reactive power output will be computed and the exact requirement of reactive power can also be obtained. When the main DG receives the message from neighbouring DGs, it will compute to distribute the reactive power output of each DG according to the received message. In this strategy, we only consider the neighbouring nodes as the MIGs. Hence, the MDG and MIGs can regulate the voltage level of main node cooperatively. Then the total amount of injected/absorbed reactive power for node i, the sum of adjustable reactive power of all involved neighbouring MIGs based on the sensitivity coefficient from MIGs to the MN, will be shown as

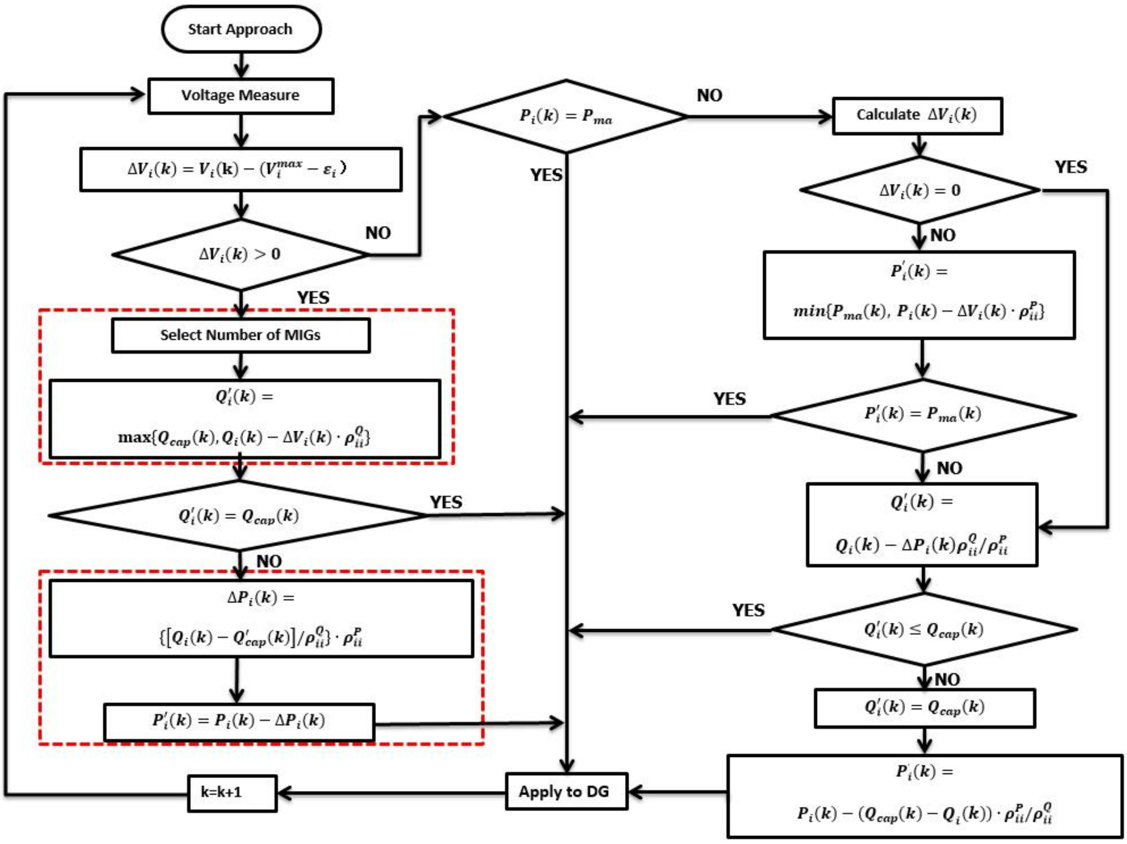

Start Approach
Voltage Measure
$\Delta V_i(k) = V_i(\mathbf{k}) - (V_i^{max} - \varepsilon_i)$
$\Delta V_i(k) > 0$
NO
YES
Select Number of MIGs
$Q_i'(k) =$
$\max\{Q_{cap}(k), Q_i(k) - \Delta V_i(k) \cdot \rho_{ii}^Q\}$
$Q_i'(k) = Q_{cap}(k)$
YES
NO
$\Delta P_i(k) =$
$\{[Q_i(k) - Q_{cap}'(k)]/\rho_{ii}^Q\} \cdot \rho_{ii}^P$
$P_i'(k) = P_i(k) - \Delta P_i(k)$
k=k+1
Apply to DG
$P_i(k) = P_{ma}$
NO
YES
Calculate $\Delta V_i(k)$
$\Delta V_i(k) = 0$
YES
NO
$P_i'(k) =$
$min\{P_{ma}(k), P_i(k) - \Delta V_i(k) \cdot \rho_{ii}^P\}$
$P_i'(k) = P_{ma}(k)$
YES
NO
$Q_i'(k) =$
$Q_i(k) - \Delta P_i(k)\rho_{ii}^Q/\rho_{ii}^P$
$Q_i'(k) \leq Q_{cap}(k)$
YES
NO
$Q_i'(k) = Q_{cap}(k)$
$P_i(k) =$
$P_i(k) - (Q_{cap}(k) - Q_i(k)) \cdot \rho_{ii}^P/\rho_{ii}^Q$

Figure 3.5: Cooperative decentralized reactive power control flowchart

$$Q_{cap}(k) = \Delta Q_i(k) + \frac{\Delta Q_{i+1}(k)}{\rho_{ii+1}^Q}\rho_{ii}^Q + \frac{\Delta Q_{i-1}(k)}{\rho_{ii-1}^Q}\rho_{ii}^Q. \tag{3.25}$$

where $\Delta Q_{i+1}(k)$ is the effectively adjustable reactive power. ρ_{ii+1}^Q and ρ_{ii-1}^Q are sensitivity coefficients of forward node and backward node to node i, respectively. ρ_{ii}^Q is the self node reactive power sensitivity coefficient. $\Delta Q_{i+1}(k)$ and $\Delta Q_{i-1}(k)$

are the available reactive power variations of forward node and backward node to node i, respectively.

It is obvious that $Q_{cap}(k)$ is larger than the reactive power capability of single DG $\Delta Q_i(k)$. According to the requirement of reactive power, it is necessary to determine whether to reduce the active power or not. The correlation expression can be shown as

$$Q_i^{'}(k) = max(Q_{cap}(k), Q_i(k) - \Delta V_i(k) \cdot \rho_{ii}^{Q}). \tag{3.26}$$

where $Q_i^{'}(k)$ is the current required reactive power output. $Q_i(k)$ is the current reactive power output. $\Delta V_i(k)$ is the voltage variation that requires to be adjusted.

According to equation (3.26), if the requirement of reactive power $Q_i^{'}(k)$ is smaller than $Q_{cap}(k)$, it means that the reactive power is enough to control the voltage level into operative range. The amount of reactive power compensation for each DG will be calculated. Then the detail of reactive power regulation that is required for each node will be sent to neighbouring DGs to perform the regulation. It should be noted that the reactive power variation of MDG and MIGs will also influence MIGs' voltage level. Therefore, the amount of reactive power allocated by each node will be taken into account carefully (through the reactive power sensitivity matrix) in case the voltage of neighbouring node exceeds the maximum value. After receiving the message from MDG, the control instruction will apply to the DG directly. Otherwise, the active power curtailment will happen. In the meantime, in terms of the reactive power capability curve, different active power output will have different maximum reactive power output. The variation of active power curtailment $\Delta P_i(k)$ can be written as

$$\Delta P_i(k) = \frac{Q_i(k) - Q_{cap}^{'}(k)}{\rho_{ii}^{Q}} \rho_{ii}^{P}. \tag{3.27}$$

where $Q_{cap}^{'}(k)$ is the current maximum reactive power output in terms of current active power output. $\Delta P_i(k)$ is the active power variation that requires to be adjusted.

ρ_{ii}^{P} is the self node active power sensitivity coefficient.

Then, the current modified active power output $P_i^{'}(k)$ can be obtained.

$$P_i^{'}(k) = P_i(k) - \Delta P_i(k). \tag{3.28}$$

The active power curtailment only happens when the reactive power is not enough to reduce the voltage level. The right part of Fig 3.5 demonstrates if the active power output does not reach the maximum output value after active power curtailment, the active power enhancement can occur. The active power changes will affect the maximum controllable reactive power capability. Therefore, if the voltage level do not exceed the maximum value, the curtailed active power output can be adjusted. When the active power output is lower than the current maximum allowable output $P_{ma}(k)$, the active power can be regulated by increasing the voltage level. The voltage variation will be detected first. When the available voltage variation is not equal to zero, the active power output can be increased by enhancing the voltage level. Otherwise, the reactive power adjustment can be applied. The related active power adjustment expression can be shown as

$$P_i^{'}(k) = min(P_{ma}(k), P_i(k) - \Delta V_i(k)\rho_{ii}^{P}). \tag{3.29}$$

In terms of the voltage variation $\Delta V_i(k)$, it is clear to check how much voltage variation can be used to improve the active power output. If the active power increases to maximum allowable output $P_{ma}(k)$, it will apply to the DG directly. Otherwise, the reactive power adjustment will be taken into account.

$$Q_i^{'}(k) = Q_i(k) - \frac{\Delta P_i(k)\rho_{ii}^{Q}}{\rho_{ii}^{P}}. \tag{3.30}$$

where $\Delta P_i(k) = P_{ma}(k) - P_i^{'}(k)$ is the active power variation after the active power adjustment. The modified reactive power can decrease the voltage level. Then the active power will be increased again by increasing the voltage level. If the reactive power requirement is less than the reactive power capability, the requirement value $Q_i^{'}(k)$ will be used directly to DG, which can reduce the voltage level. Otherwise, the maximum capacity value $Q_{cap}(k)$ will be applied to calculate the voltage variation. The revised active power can be written as:

$$P_i'(k) = min(P_{ma}(k), P_i(k) - \frac{(Q_{cap}(k)-Q_i(k))\rho_{ii}^P}{\rho_{ii}^Q}). \tag{3.31}$$

where $Q_{cap}(k) - Q_i(k)$ is the maximum available reactive power variation when the requirement of reactive power variation is larger than the maximum capability.

Then the revised reactive power can be utilized to the DG to enhance the active power output. The proposed cooperative decentralized control strategy can effectively control the node voltage level compared to the independent DG control approach. In addition, this algorithm can reduce the possibility of active power curtailment. This novel voltage control approach can improve the efficiency of control method and optimize the allocation of reactive power. However, the proposed strategy still requires a certain limited information exchange. It is necessary to analyze the effect of time-delay on the algorithm.

3.4 Time-delay Analysis in Decentralized Control Voltage Method

The uncertainty of renewable energy output and energy demand can affect the voltage value. And the communication time-delay always exists during the information exchange. In order to implement the control in real time, the control strategy should adapt an effective and fast communication technology to improve the control speed. There are several kinds of communication technologies that can be chosen for enabling smart grid communications. The existing cellular network can be a good option. The 3rd Generation (3G) network can be considered as the backbone of a smart grid communication solution [104]. It has many advantages, such as mature technology, already deployed base stations, a wide coverage, low investment, and large capacity.

Using a coordinated control approach, the time-delay (including communication system delay and decision-making delay) among DGs or controllers could affect the effectiveness of the control algorithm. Without any time-delays, conventional control strategy can effectively regulate the voltage level within the operating range. However, when time-delay is applied, it becomes challenging to control the voltage level. The following part describes a simple communication time-delay model.

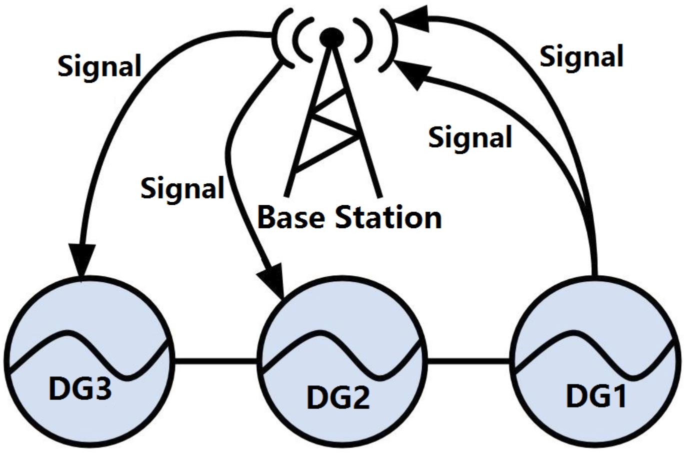


Figure 3.6: Exchange of control signals in a communication system.

Fig. 3.6 shows a basic communication system. First of all, if voltage level of DG1 is out of the operating range, the reactive power injection/absorption will be calculated by using sensitivity coefficients. Then the reactive power compensation signal will be sent to base station (BS), which could forward it to selected neighbouring MIGs, such as DG2 and DG3. Once the MIGs receive the control signal, they will modify the power factor to control. Meanwhile, the MIGs will also acknowledge DG1 to make sure that the control signal is received and operated.

According to the 3rd Generation Partnership Project (3GPP) Release 9 [105], the time-delay can be obtained as follows.

1. Set environment, network layout, and antenna array parameters: a) choose a scenario (Indoor, Micro cellular, Base coverage urban or High speed); b) determine the number of BSs and DG; c) determine the locations of BSs and DGs, or the distance of each BS and DG and relative direction of each BS and DG; d) determine BSs and DGs antenna field patterns and array geometries; e) determine BSs and DGs array orientations with respect to north (reference)

direction; f) determine speed and direction of motion of DGs; g) determine system centre frequency

2. Assign the propagation condition, i.e. line-of-sight (LOS) or non-LOS (NLOS).

3. Calculate the path loss for each BS-DG link in the system.

4. Generate other parameters, i.e. delay spread, angular spreads and shadow fading term.

5. Calculate the delays τ. Time-delay is drawn randomly from the delay distribution defined in [106], with an exponential delay distribution in DN scenarios as below:

$$\tau_{i,j}^{'} = -\sigma_{i,j} r_{i,j} ln(X_{i,j}). \tag{3.32}$$

where i and j are the transmitter index and receiver index, respectively. $\sigma_{i,j}$ is the delay spread, $r_{i,j}$ is the delay distribution proportionality factor, $X_{i,j} \sim$ Uni(0,1) and index $i = 1, ..., N, j = 1, ..., M$. With uniform delay distribution, the time delay values $\tau_{i,j}^{'}$ are drawn from the corresponding range.

The stochastic end-to-end delay over a fixed path mainly consists of two components: a deterministic delay (all routers processing delay) and a stochastic delay (assuming mainly caused by internet traffic). Normalise the delays by subtracting the minimum deterministic delay and sort the normalised delays to descending order:

$$\tau_{i,j} = sort\{\tau_{i,j}^{'} - \tau_{i,j}^{min}\}. \tag{3.33}$$

where $\tau_{i,j}^{min}$ is the deterministic delay which is a fixed minimum time for each path.

Equation (3.32) presents the random time-delay calculation. This equation explains that each communication time between DGs, which is not a fixed value for every information exchange, can reach a relatively high value. In practice, as measurements can be time stamped, it is convenient to know exact timedelay by comparing this time stamp with the received time of measurement signal.

Note: 3G has been an obsolete technology due to the explosive growth in cellular communications in past few years. Now, 4G technology is already on the verge of occupying the market and soon will revolutionize the existing systems [16]. The upcoming 5G will be an appropriate technology with less communication system time-delay. Besides this, there exists decision-making delay. When we consider the power system optimization, the decision-making time-delay may become dominant. In addition, it is also necessary to investigate the communication delay systems for different systems in different areas.

3.5 Case Study Results

3.5.1 IEEE 33 Bus Network Case

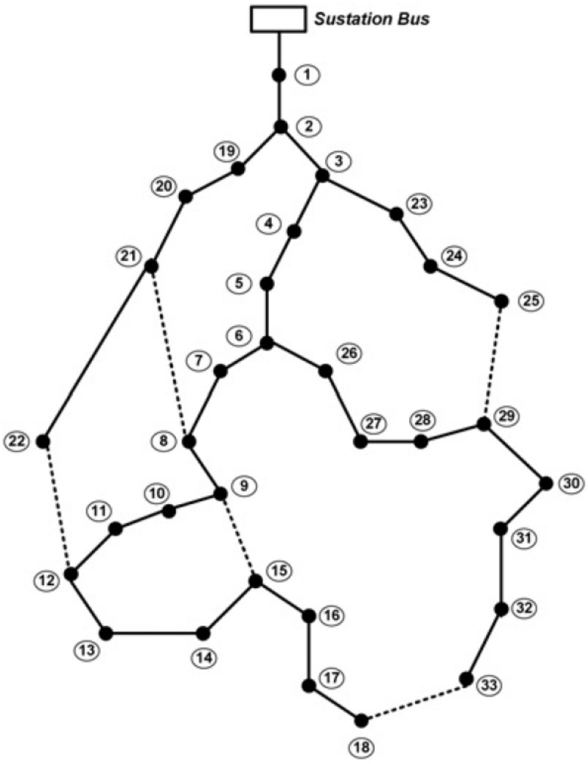


Figure 3.7: Single-line 33-bus distribution system diagram.

A medium-voltage (MV) distribution networks have been adopted as the case study network for the purposes of this research. This case study network represents an urban generic radial distribution system [13]. This network has 33 buses, 32 branches and 5 tie lines as can be seen from the single-line diagram depicted below in Fig. 3.7. The total real and reactive power loads on this system are 3750 kW and 2300 kVar, respectively. Then the original voltage profile can be obtained by NewtonRaphson method power flow which can be seen below in Fig. 3.8. For many power transformer applications, a supply interruption during a tap change is unacceptable, and the transformer is often fitted with a more expensive and complex On Load Tap Changer (OLTC, sometime Load Tap Changer, LTC). As can be seen, the voltage level of bus 1 is set by the primary substation transformer's OLTC which can be considered as a fixed value. Voltage levels in bus 18 and bus 33 are only 0.9141 p.u. and 0.9243, perspectively. The values are both lower than the minimum allowable voltage 0.95 p.u. because of the radial structure of the network. We set threshold value typically as 0.05 which means the maximum allowable voltage is 1.05 p.u. and the minimum allowable voltage is 0.95 p.u., following the ANSI C84.1-2006 standard [107]. Therefore, it is necessary to take measures to adjust the voltage level into the normal operation range.

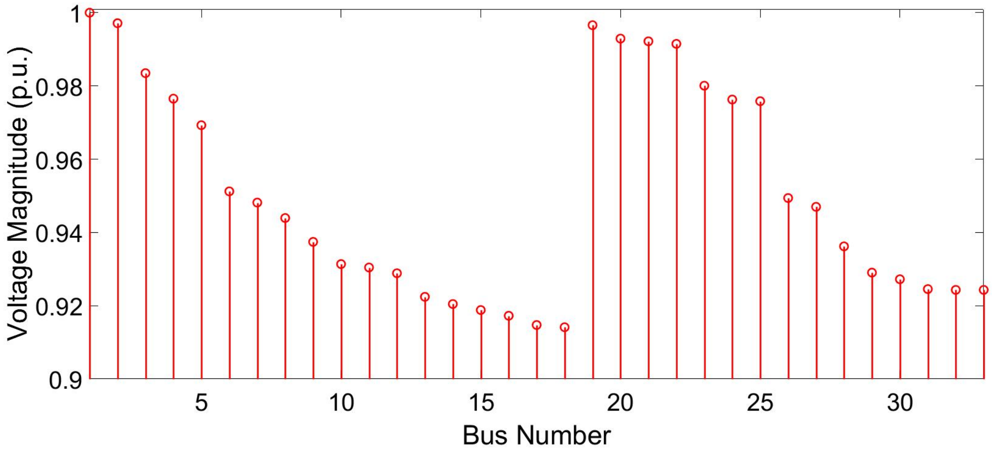


Figure 3.8: Voltage profile through Newton-Raphson method in 33-bus system.

In this section, we propose to utilize the reactive power of DGs to regulate the voltage level. There are two different types of DG which are applied under the test in order to obtain a general validation of the proposed decentralized voltage control approach, Wind Distributed Generation Unit (WDGU) and Photovoltaics

(PV). Four WDGUs and four PVs have been connected to the 33-bus network, respectively. The connection buses are also highlighted in Table 3.1 and Fig. 3.9, where the rated power value of the DGs are specified.

Table 3.1: WDGU and PV location and parameters

Parameters		
DG	Rated Power (MW)	Location (Bus)
$WDGU$	2.5	$2, 12, 15, 18$
PV	2.2	$23, 25, 27, 33$

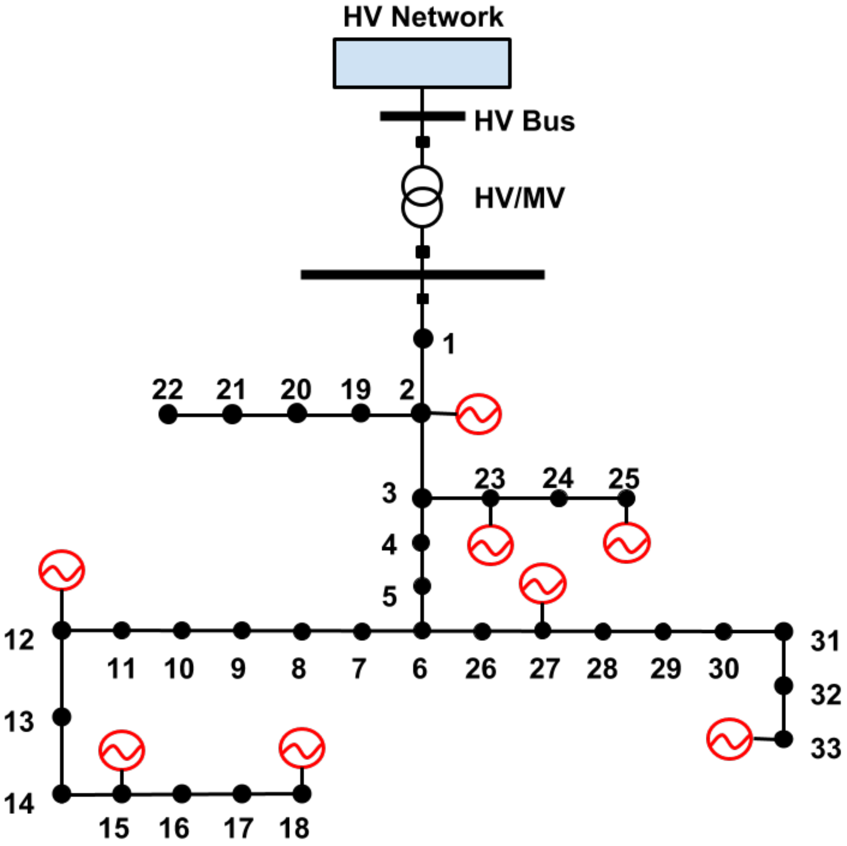


Figure 3.9: 33-bus system with distribution generators.

The single line diagram of the 33-bus distribution network with the DGs penetration is shown in Fig. 3.9. We assume that the WDGU and PV both have the same rated power, which are 2.5 MW and 2.2 MW, respectively.

Fig. 3.10 shows the wind and solar generation active power output profiles of one-day data in the UK in October 2015 from Solax Power Ltd. It is clear that the

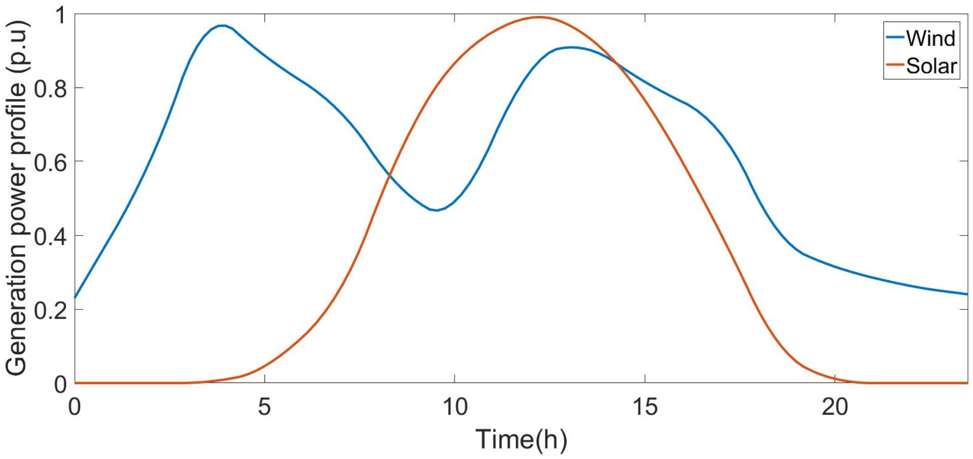


Figure 3.10: Generation active power output profiles for WDGU and PV.

solar power reaches the peak value around 2 pm in the daytime and almost no output for the whole evening. Contrarily, the wind energy can always maintain a certain output. When the DGs are applied into the DN, the simulation results of the power flow have been analyzed by Matpower/MATLAB, in order to investigate the assessment of the voltage profile.

3.5.2 Simulation Results without Considering Time-Delay

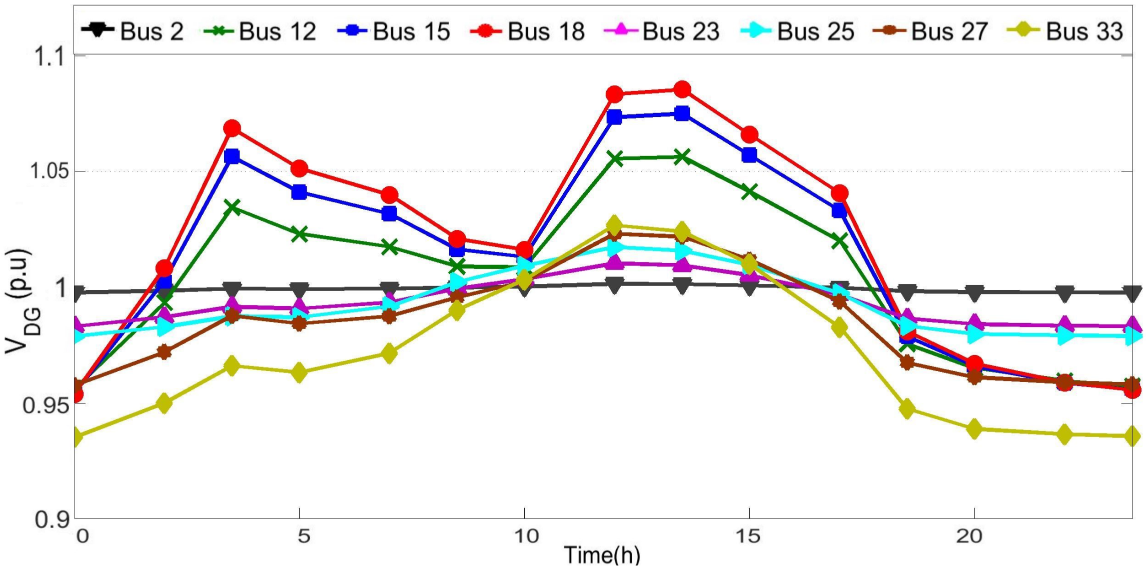


Figure 3.11: DG-bus voltage levels without any control action.

In the simulations, Fig. 3.11 depicts the voltage profile without any control actions

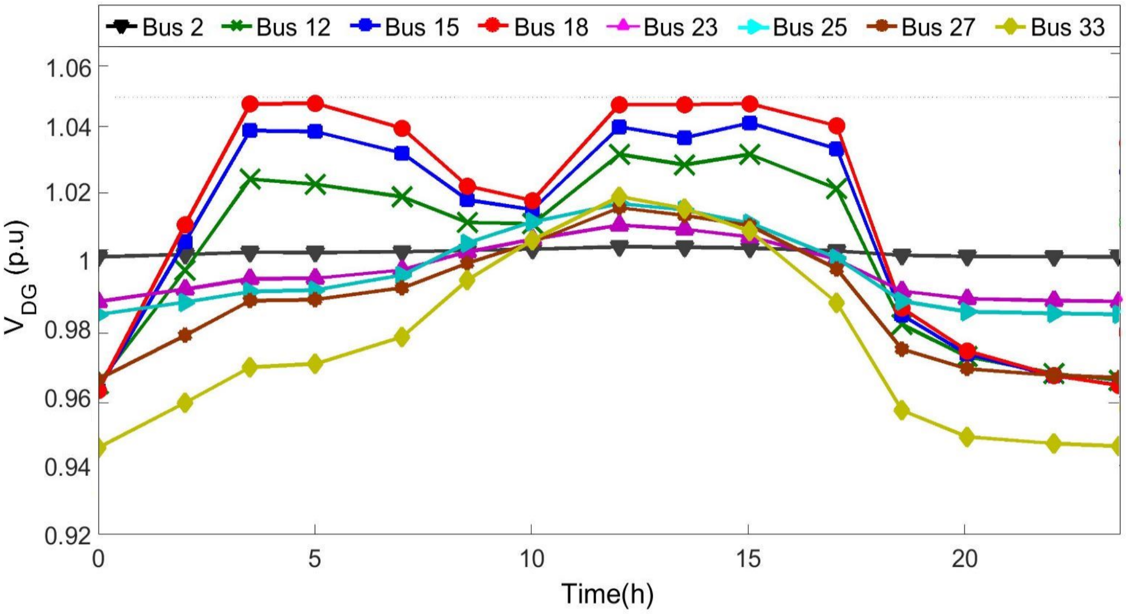


Figure 3.12: DG-bus voltage levels with control action.

when the DGs are installed to the DN. Without loss of generality and due to the infringement of upper operation range shown in Fig. 3.11, the control strategy has been run to optimize only the upper thresholds. It is clear that during two time periods (3:30 h to 5:00 h and 11:00 h to 16:00 h) voltage levels of some buses exceed the upper limited voltage value. Given the fact that nearly 90% of all power outages and disturbance are originated in the distribution system, the move towards the smart grid has to start at the distribution level of the power system. The maximum voltage is almost 1.09 p.u. which may lead to a series of issues and even cause the power outages. When the decentralized voltage control strategy is applied, the voltage level will be reduced to a normal operating range.

Fig. 3.12 presents the voltage level of DG buses after the control action. It is obvious that the voltage levels are under the regulatory limits after control action. As can be seen from Fig. 3.12, all the node voltages exceeding the maximum value are adjusted to 1.05 p.u. or less, which means that the proposed coordinated decentralized control approach can effectively control the voltage level within the variable generation power output. In addition, it is found that other two DGs (DG12 and DG15 who is close to DG18) have a large variation, in comparison to other DG buses in the same network. Consequently, It is worthwhile to emphasize that the control method using the reactive power variation and the sensitivity coefficients can be implemented for temporary over voltage mitigation (e.g., during emergency conditions, high energy demand or high active power injection).

The voltage oscillations (e.g., from 3:30 h to 5:00 h) depend on the wind generator power output. According to the sensitivity coefficients, we set DG18 as the MDG. DG15 is also more powerful than DG12 which means the sensitivity coefficient from DG15 to DG18 is greater (in absolute value) than the sensitivity coefficient from DG12 to DG18. Therefore, the reactive power of DG15 has the greatest impact on the voltage variation of the DG18, followed by the DG12. In contrast, when voltage variations of other DGs are considered, it is evident that the voltage variations of other DGs in Fig. 3.12 are much smaller than the voltage variations of DG12 and DG15. In this case, it is obvious that according to the radial structure of network, the DG12 with a small sensitivity coefficient value is farther than the DG15 with a large sensitivity coefficient value from DG18. Although some nodes are far from the MDG, they may have a greater impact on the voltage variation of MDG than those that are closer to the MDG. If it happens, the sensitivity coefficients table can be utilized exactly to choose the DGs which have the greatest impact to MDG.

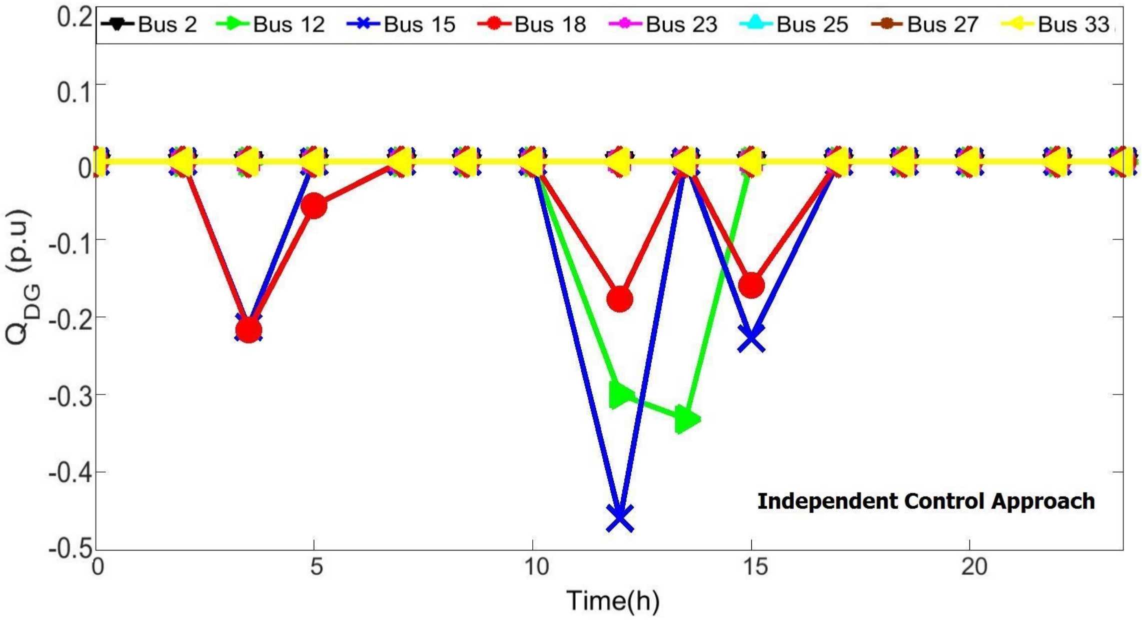


Figure 3.13: DG-bus reactive power injection without cooperative control.

Furthermore, compared with the independent approach, the coordinated approach can adjust the power factors of neighbouring nodes cooperatively in order to enlarge the total reactive power capability. To investigate the difference of reactive power absorption between two approaches, the reactive power absorption of independent control approach and cooperative control approach are shown in Fig. 3.13 and Fig 3.14, respectively. When the voltage rise occurs, Fig. 3.13 shows the reactive power compensation value after the operation of the independent control action. It shows that DG15 has the largest reactive power compensation value which is almost 0.45 p.u., in comparison to the compensation values of other DGs. Moreover, 0.45 p.u. is already 92% of the maximum capability. When the requirement of reactive power increases in case of some conditions, the reactive power compensation will not be enough to reduce the voltage level due to the maximum reactive power capability curve and the active power curtailment will be required in advance.

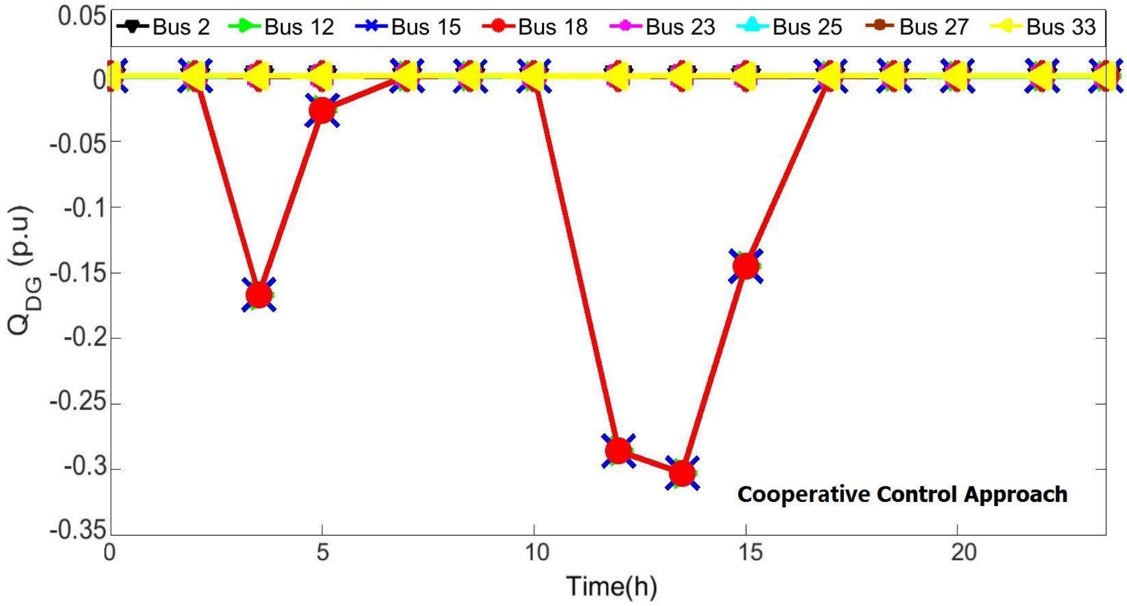


Figure 3.14: DG-bus reactive power injection with cooperative control.

On the contrary, the compensation performance of the cooperative approach is better than that of the independent approach, which is shown in Table 3.2 and Fig. 3.14. Meanwhile, the control results of voltage level for each node are the same as the independent control method. It is assumed that the WDGUs at bus 12,15,18

Table 3.2: Reactive Power Injection by Different Approaches

	Independent control Maximum output	Cooperative control Maximum output
Bus 12	0.33 *p.u.*	0.34 *p.u.*
Bus 15	0.45 *p.u.*	0.34 *p.u.*
Bus 18	0.18 *p.u.*	0.34 *p.u.*

have the same maximum capability. Comparing with the independent control approach, the cooperative control approach can decrease the maximum reactive power output from 0.45 p.u. to 0.34 p.u. as seen in Table 3.2. In addition, 0.34 p.u. can greatly reduce the possibility of active power curtailment occurrence even if the network loads are higher than usual. The normal maximum reactive power output is 0.49 p.u. for each DG according to (3.22). When the large requirement of reactive power compensation or load fluctuation happens, only 0.04 p.u. reactive power in the independent control strategy are available to regulate the voltage level without triggering an active power curtailment. In contrast, in the cooperative control approach, the MDG still has 0.15 p.u. of reactive power to regulate the voltage of MN, and neighbouring MIGs also have 0.15 p.u. that can be required to adjust the voltage of the MN. Meanwhile, the reactive power 0.45 p.u. in this case means the low power factor. Low power factor can significantly impact the DG performance. In the meantime, if the main DG is out of work, the neighbouring nodes can still adjust the voltage level of the MN through the reactive power adjustment of their own DGs. Consequently, the proposed cooperative voltage control strategy can not only control a wider scope of voltage fluctuation, but also enhance the robustness of the algorithm when an unexpected event occurs. However, it should be emphasized that this coordinated control strategy does not consider the optimization problem during the control action. It is possible to investigate the multi-objective optimization during the allocation of reactive power among neighbouring nodes in the future, such as the minimization of system power loss and voltage control.

3.5.3 Simulation Results Considering Time-Delay

In the preceding section, the control method does not consider the effect of the communication time-delay. However, in a real distribution system based on the cooperative control method, the communication time-delay always exist between neighbouring DGs and the normal algorithm with information exchange will always be affected by the time-delay.

To investigate the influence of communication time-delay, Fig. 3.15 demonstrates the voltage levels of DG buses when the control approach considers the communication time-delay. Without considering time-delay, the voltage level shown in Fig. 3.12 can be steadily controlled within the limited value. However, the voltage level is out of control which can be found in Fig. 3.15. This result is presented in one minute from 12:30 h to 12:31 h.

There are three different scenarios to show the effect of the time-delay, which all voltage levels will be affected. S1 stands for the sudden increased active power output of PVs, in which case the voltage level will increase. S2 stands for the sudden power generation caused by large wind speed changes, in which case the output of active power of DG will increase dramatically. S3 stands for the sudden power blackout of high power machine, in which case the excess active power will increase the voltage level. It shows that the voltage levels in all three cases will be out of control if the time-delay occurs. The reason is that delayed massage will make the control algorithm difficult to operate the control action in real time. Then at the beginning of each scenario, the voltage level will be always out of control. Power system stability could be affected by voltage collapse from a second to tens of minutes and transient voltage fluctuation is often the main concern [108]. According to Fig. 3.15, the voltage level is over the limited value 1.05 p.u. during the control action due to the emergency conditions. If it happens in real power systems, the system performance and electrical equipments would be damaged. If the voltage drop or rise is too large in few seconds, the power system even can not be restored again. Voltage stability is affected by various components in a wide time range. Therefore, it is necessary to consider the time-delay model and modify the control strategy to maintain the voltage level when time-delay or packet loss happens. The time-delay analysis can improve the control approach to maintain the voltage properly and reduce the incidence of system instability. Relevant investigation of modified cooperative control strategy to fit the time-delay could be a new research direction in future.

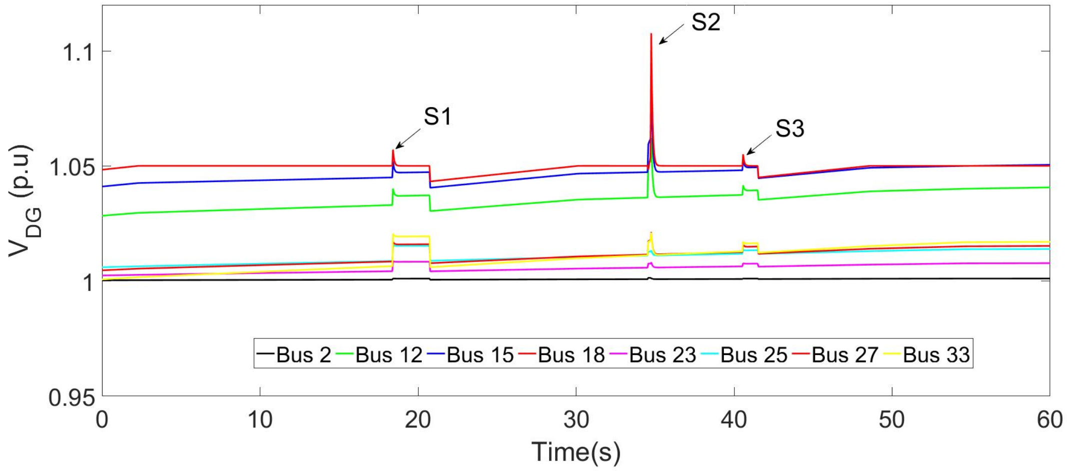


Figure 3.15: Voltage level with time-delay in three different scenarios.

3.6 Chapter Summary

This chapter has derived a cooperative decentralized voltage control approach. The widespread utilization of large number of DGs installed in MVDN can result in voltage fluctuation issues because of the uncertainty output. The voltage rise can induce loss of partial load and reduce the life span of equipment. The proposed decentralized voltage control approach, based on the sensitivity analysis coefficient, can regulate the voltage level into the operating range by choosing more than one generator to control the voltage level cooperatively.

The proposed control method is able to monitor the voltage level and compensate the reactive power into the DN effectively when time-delay is not significant and can be ignored. Meanwhile, the concept of MIGs could be applied to reduce the possibility of active power curtailment occurrence in advance and improve the DG power factor. The line resistance in MV network can not be ignored comparing with that in HV network. Therefore, the reactive power flow reduction can decrease the power loss.

The 33-bus MVDN is used to verify the proposed control method on smart grid development in the future without considering time delay. If the time delay is considered, the control method cannot control the voltage level effectively. A more effective control strategy should be proposed in order to fit the delay system. Due to greater complexity of electrical network with DGs, it is necessary to revise the control algorithm to regulate the voltage in real-time. Moreover, the cooperation with traditional reactive power compensator can also be applied into the system to control the voltage. In addition, the optimization problem can be considered both to regulate the voltage level and to optimize the system power loss during the decentralized control.

Chapter 4

Modelling of ADMM-Based Optimal Power Flow

4.1 Introduction

The future smart grid, which leverages advanced information and communications technology (ICT) to facilitate power system operation and control, is vulnerable to communication time-delay or packet loss [109–112]. The large penetrations of DGs in distribution grid could benefit to the power system, for example, increasing energy diversity, improving reliability and reducing environmental pollution. These DGs can provide a large quantity of ancillary services that are of great interest to the optimization of the grid [8, 113]. In order to realize the autonomous power systemin real-time, it is significant to migrate control strategy from traditional centralized approach to decentralized approach.

The ADMM approach, which is an augmented Lagrangian-based algorithm, is a popular choice due to the robust and fast convergence results both in theory and practice [114]. In literature, few papers discuss a fully decentralized OPF problem with stochastic communication delay in a distribution network. The main work in this chapter proposes a feasible fully distributed optimization approach to regulate the reactive power output of DGs. The majority of recent papers also have not investigated this particular decentralized OPF problem with both synchronous and asynchronous time-delay models. The asynchronous model means that each node could operate its own iterative step without considering the time synchronization of other nodes. For our work, we mainly concentrate on the medium-voltage distribution network, but the experimental results are also applicable to transmission network and low-voltage distribution network. The novelty of this chapter is to analyze the effect of communication time-delay on the performance of both synchronous and asynchronous algorithms. The main contributions of this work are as follows:

- The ADMM algorithm has been investigated for decades in power system, a fully decentralized reactive power optimization approach with a little coordination of neighbouring nodes is studied to solve the optimization problem. We develop the ADMM algorithm [14] to simulate the convergence result in optimization OPF problem. An improved iterative step is proposed to minimize the power loss which presents an efficient convergence result in this paper. The investigation of convergence speed could provide a reference to design a similar kind of algorithm.

- Both synchronous and asynchronous algorithms that consider communication time-delay are proposed in this chapter. By comparing with the results of the synchronous algorithm without delay, although the asynchronous algorithm has a larger time-delay tolerance on the iterative process, the proposed asynchronous algorithm without delay still has a better convergence speed and optimization results during the same wall clock time period. Compared to other decentralized OPF algorithms, this work not only adds the state-of-the-art communication delay model to the ADMM algorithm, but also explores the convergence performance of proposed synchronous and asynchronous algorithms with time-delay. Furthermore, the simulation results prove that the communication delay has a significant influence on the results of decentralized ADMM algorithm. When time-delay is considered, the traditional decentralized algorithm even cannot converge properly.

- As the fluctuation in experimental results with time-delay, we proposed four strategies, such as, skipping strategy (SS), previous value strategy (PVS), autoregressive (AR) strategy (ARS)and weighted AR strategy (WARS), to optimize the synchronous and asynchronous convergence results. The proposed weighted AR ADMM can effectively improve the convergence results for both synchronous and asynchronous algorithms and also dramatically reduce the fluctuation of the results significantly in the ADMM algorithm with different probabilities of time-delay.

This chapter is organized as follows. Section 4.2 briefly introduces formulation of problem in ADMM algorithm. Using the distributed consensus optimization theory, the sufficient improved ADMM recursive algorithm are proposed in Section 4.3. The stochastic communication delay model, which contain a deterministic delay and a stochastic delay, is discussed in Section 4.4.1. The message transmission mechanism of synchronous and asynchronous algorithms are introduced in Section 4.4.2. The proposed four optimized strategies are also discussed in Section 4.5 to assess the performance of the strategies. Simulation results are presented in Section 4.6, followed by discussions and conclusions in Section 4.7.

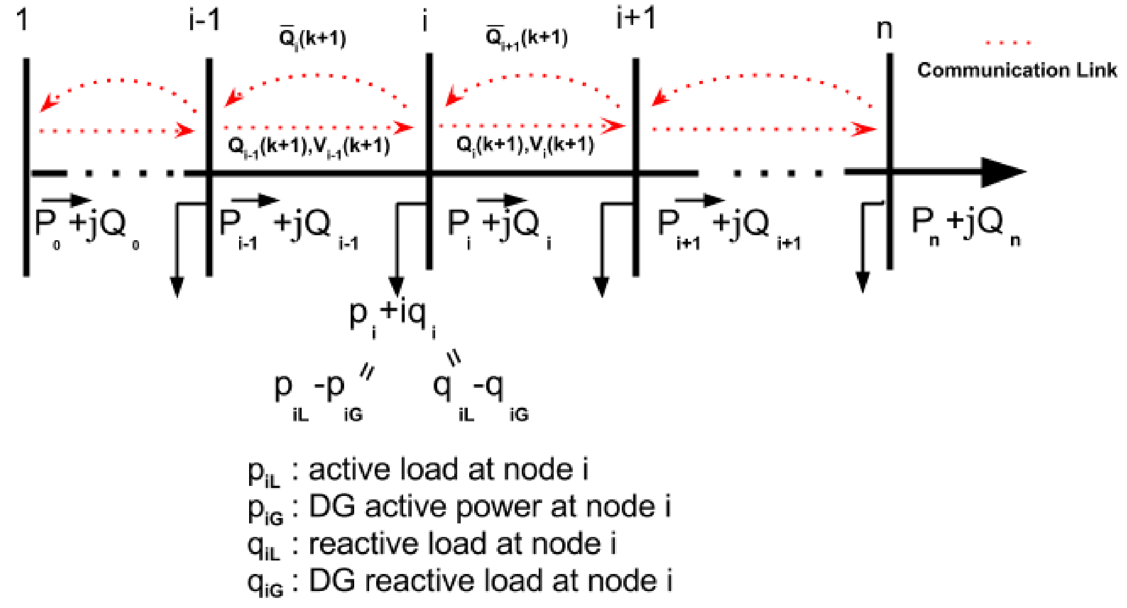


Figure 4.1: Single line diagram of a main distribution feeder.

4.2 Formulation of Problem

4.2.1 Distribution System Power Flow Formulation

Power flow in a distribution system always obeys physical laws, for example, Kirchoff laws and Ohm law [115], which become part of the constraints in the capacitor placement problem. In this section, we present power flow equations for radial distribution systems. The formulation is conductive to establish the effective solution methods. For pedagogic convenience, we first consider a special case where only one main feeder is presented in Fig. 4.1. The derived equation can also be applied to the general case including laterals. To simplify the presentation, the system is assumed to be a balanced three-phase system.

In Fig. 4.1, the voltage level in bus 1 represents the substation bus voltage magnitude and is assumed to be a constant value. The Lines are represented by a series impedance $z_i = r_i + jx_i$ and a power flow $S_i = P_i + jQ_i$, respectively. The loads can be treated as a constant power $s_i = p_i + jq_i$. The reactive power output of DG will be represented as variable reactive power source. Meanwhile, the communication links are displayed for the information exchange of iterative procedure. It is a bi-direction communication between neighbouring nodes. This network has $n + r$ nodes and $n + r - 1$ branches. We define ν as the set of nodes and β as the set of branches. $(i,j) \in \beta$ means nodes i,j are neighbouring nodes (because of lateral branches, some nodes may have two or more neighbouring nodes), and $\mathcal{N}_i$ denotes as the set of i's neighbouring nodes.

With this representation, the network will become a ladder network. If the power supplied $S_1 = P_1 + jQ_1$ from the substation is known, then the power and the voltage level at the receiving end of the first branch can be written as follows,

$$S_2 = S_1 - S_{loss} - s_2 = S_1 - z_1 \frac{|S_1|^2}{V_1^2} - s_2 \tag{4.1a}$$

$$V_2 \angle \theta_2 = V_1 - z_1 I_1 = V_1 - z_1 \frac{S_1^*}{V_1}. \tag{4.1b}$$

where θ_1 is the voltage angle. Repeating the same process will yield the following recursive formula for each branch on the main feeder.

$$P_{i+1} = P_i - r_{i+1}\frac{P_i^2 + Q_i^2}{V_i^2} - p_{i+1} \tag{4.2a}$$

$$Q_{i+1} = Q_i - x_{i+1}\frac{P_i^2 + Q_i^2}{V_i^2} - q_{i+1} \tag{4.2b}$$

$$V_{i+1}^2 = V_i^2 - 2(r_iP_i + x_iQ_i) + (r_i^2 + x_i^2)\frac{P_i^2 + Q_i^2}{V_i^2}. \tag{4.2c}$$

where P_i and Q_i are the active and reactive power flows from node i to node $i+1$. V_i is the bus voltage magnitude at node i.

Both p_i and q_i are composed of local consumption minus local generation due to the DG inverter, which can be found in Fig. 4.1.

$$p_i = p_{iL} - p_{iG} \tag{4.3a}$$

$$q_i = q_{iL} - q_{iG}. \tag{4.3b}$$

In terms of these four different parameters in (4.3), we assume that p_{iL}, p_{iG} and q_{iL} are uncontrollable parameters (i.e., driven by consumer load or instantaneous DG generation). On the contrary, the reactive power generated by the DG inverter, q_{iG}, can be adjusted within limits.

Note that we have the following terminal conditions:

$$V_1 = V_{cons} \tag{4.4a}$$

$$P_n = Q_n = 0. \tag{4.4b}$$

where V_{cons} is the constant voltage magnitude for substation voltage. And the active and reactive power flows at the end of the main feeder can be treated as zero.

The DistFlow equations can be generalized to include laterals. Consider a lateral branch out from the main feeder as shown in Fig. 4.2. For notational simplicity, the lateral branch out from node m will be referred to as the lateral m and the node m will be referred to as the lateral node.

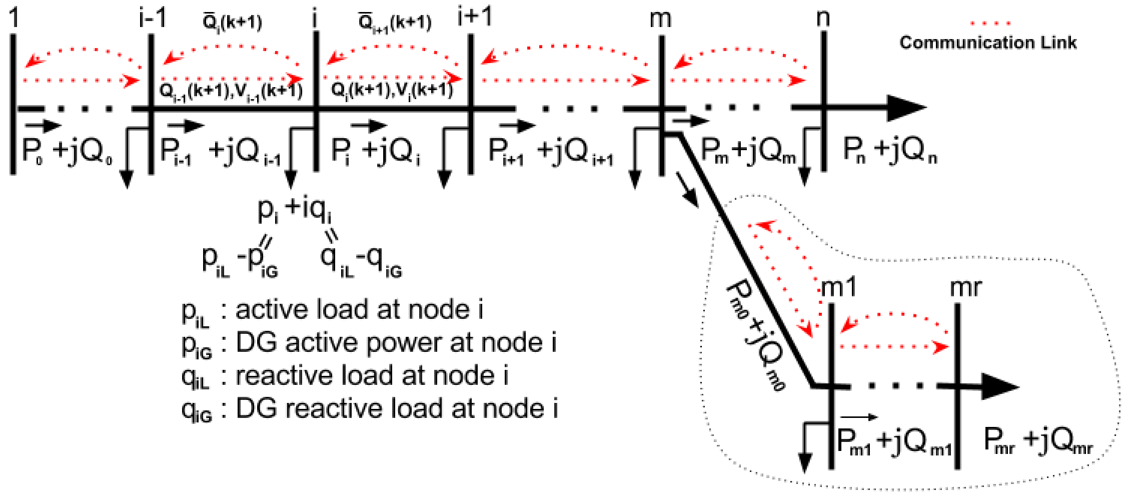


Figure 4.2: One-line main feeder with a lateral branching network.

The same process of DistFlow Equations of main feeder will be repeated for the lateral branch by using the formulas in (4.2) and the new terminal conditions can be set as $P_{mr} = Q_{mr} = 0$. The DistFlow equations can be utilized to determine the operating point. The special structure of the DistFlow equation can be used to develop a computationally efficient and numerically robust solution algorithm. Consequently, we prefer to use the ADMM algorithm over conventional optimization algorithm because the augmented Lagrangian-based ADMM algorithm has the robust and fast convergence results in theory and practice [114].

4.2.2 Global Optimization Problem

Our target in this chapter is to maximize the system operation efficiency, i.e., the minimization problem of power loss:

$$P_{los} = min \left\{ \overbrace{\sum_{i \in 1 \cdots \nu} (F_i(S_i))}^{power\ loss} \right\}. \tag{4.5}$$

where F_i is the power loss function of the ith node, ν is the total number of network nodes, and S_i is the complex power flow from node i to node $i+1$. S_i can also be written as $S_i = P_i + jQ_i$, where P_i and Q_i are the active and reactive power flow from node i to node $i+1$, respectively.

According to formula (4.2), the details of the power loss minimization function can be written as

$$\sum_{i\in 1\cdots\nu}(F_i(S_i)) = \sum_{i\in 1\cdots\nu}\left\{r_{i-1}\frac{P_{i-1}^2+Q_{i-1}^2}{V_{i-1}^2}\right\}. \tag{4.6}$$

Moreover, the power loss minimization function would be subject to multiple nominal operational constraints. We note that the active power P_i, determined by p_{iL} and p_{iG} from Fig. 4.2, can be viewed as a fixed constant during the iterative process. The DG's reactive power term q_{iG} will be treated as the control variable to optimize the objective function. The constraint formulas for all nodes are as follows

$$s.t. \quad \forall\ i \in 1, ..., \nu$$

$$\mid Q_i - Q_{i-1} - q_{iL} \mid \leq \overline{s}_i \tag{4.7a}$$

$$V_i^{min} \leq V_i \leq V_i^{max} \tag{4.7b}$$

$$V_i^2 = V_{i-1}^2 - 2(r_{i-1}P_{i-1} + x_{i-1}Q_{i-1}) + (r_{i-1}^2 + x_{i-1}^2)\frac{P_{i-1}^2 + Q_{i-1}^2}{V_{i-1}^2} \tag{4.7c}$$

$$\mid S_{i-1} \mid \leq S_{i-1}^{max}. \tag{4.7d}$$

where (2a) is the power balance constraints for each node, $\overline{s}_i$ is the inverter's maximum apparent power capacity of DG for node i [116]. (2b) is the node voltage level constraints. V_i^{min}, V_i^{max} are the minimum and maximum voltage magnitude for each node i, respectively. We set voltage threshold value to 0.05 (where $V_i^{min} = 0.95$, $V_i^{max} = 1.05$) according to the American National Standard ANSI C84.1-2011. (2c) is the voltage constraints between two adjacent nodes $i-1$ and i. r_{i-1} and x_{i-1} are the branch resistance and reactance from node $i-1$ to node i, respectively. (2d) is the transmission line capacity constraints, and S_{i-1}^{max} denotes the maximum limited apparent power of transmission line branch from node $i-1$ to i.

4.2.3 Linearisation of Objective Functions

The above objective function is a nonlinear programming problem. Under normal circumstances, the changes in voltage from node to node are relatively smaller than the normal voltage level and the power loss of active and reactive power are also smaller than the power flows from node to node. Therefore, equations (4.6) and (4.7) can be rewritten within a linear quadratic function with linear constraints. The individual generic power loss expression with constraints for each node i (power loss branch from node $i-1$ to node i) can be given by

$$F_i = r_{i-1}\frac{P_{i-1}^2 + Q_{i-1}^2}{V_1^2} \tag{4.8a}$$

$$\mid Q_i - Q_{i-1} - q_{iL} \mid \leq \overline{s}_i \tag{4.8b}$$

$$V_i^{min} \leq V_i \leq V_i^{max} \tag{4.8c}$$

$$V_i^{'} = V_{i-1}^{'} - 2(r_{i-1}P_{i-1} + x_{i-1}Q_{i-1}) \tag{4.8d}$$

$$\mid S_{i-1} \mid \leq S_{i-1}^{max} \tag{4.8e}$$

where F_i in (4.8a) is the power loss formula from node $i-1$ to node i. We assume that the $V_{i-1} \approx V_1$. $V_i^{'} = V_i^2$. Then, the objective function can be approximated as a linear quadratic function.

The LinDistFlow model (A linear branch flow model to model a radial distribution system) is well justified for a wide range of distribution circuits [117]. The observation in [117] is powerful because the LinDistFlow equations (4.8) is convex, which is a linear quadratic function with linear constraints. Convexity shows that this optimization problem can be solved efficiently. In this centralized optimization strategy, each node can communicate with a control center, which performs the computations and distributes the optimal variables to all nodes. By contrast, we will develop a decentralized optimization method, which can solve the objective function (4.8) only by exchanging the iterative messages between neighbouring nodes in the network.

4.3 Methodology

In this section, we will adopt a distributed ADMM algorithm to optimize the global power loss problem. A distributed ADMM method does not need any control center to gather the information to run the iteration steps. Without the control center, the algorithm can significantly reduce the optimization time. In addition, the communication delay model will be considered in the ADMM algorithm.

4.3.1 ADMM Consensus Distributed Algorithm

To solve (4.6) in a decentralized way, we propose to use the ADMM algorithm [25, 118]. In this algorithm, we rewrite the global objective function to a distributed consensus problem. Hence, each node has its own local objective function and local constraints associated with neighbouring nodes' variables, which can be easily handled as a decentralized problem. Moreover, information exchange with neighbouring nodes means all nodes are relatively interrelated. As (4.7a)-(4.7d) are the global variables, we take into account the local variables for each local function. Partial local variables are also equivalent to the global variables after each iteration. Let $X_i = \{\overline{Q}_i, \overline{Q}_i^+, y_i, y_i^+\}$ be the optimization variables of node i, $H(X_i) \leq 0$ is the inequality constraints and $E(X_i) = 0$ is the equality constraints, which are equal to constraints (4.7a)-(4.7d). The augmented Lagrangian expression can be defined as follows

$$\mathcal{L}_\rho = \sum_{i=1}^{\nu} \mathcal{L}_i(X_i) \tag{4.9}$$

where the detail of the individual augmented Lagrangian formula $\mathcal{L}_i(X_i)$ for node i can be given as

$$
\begin{aligned}
\mathcal{L}_i(X_i) = \quad & \overbrace{F_i(\overline{Q}_i)}^{power\ loss\ term} \quad + \overbrace{y_i(\overline{Q}_i - Q_{i-1}) + y_i^+(\overline{Q}_i^+ - Q_i)}^{reactive\ power\ term} \\
& + \overbrace{\frac{\rho}{2}(\parallel \overline{Q}_i - Q_{i-1} \parallel_2^2 + \parallel \overline{Q}_i^+ - Q_i \parallel_2^2)}^{ADMM\ penalty\ term}
\end{aligned}
\tag{4.10}
$$

where $\overline{Q}_i$ is the local variable of reactive power flow from node $i-1$ to i and $\overline{Q}_i^+$ is the local variable of reactive power flow from node i to $i+1$. Q_{i-1} and Q_i are the global reactive power flow from node $i-1$ to i and node i to $i+1$, respectively. y_i, y_i^+ are the Lagrangian multipliers for node i. And ρ is the penalty factor.

The ADMM penalty term in the objective function with $\frac{\rho}{2}$ represent penalties for the local variables being different from the global variables. This term does not impact the optimal result because the constraints demand that the local variables are equal to the global variables at the optimum. Note that (4.8b) is not included in the augmented Lagrangian expression because the algorithm will be minimizing $\mathcal{L}_i(X_i)$ by adjusting the reactive power variables Q_i within a feasible set (satisfy the condition given by (4.8b)).

The ADMM distributed consensus algorithm is an iterative algorithm, where the $k+1th$ iteration starts with values $\overline{Q}_i(k)$, $\overline{Q}_i^+(k)$, $y_i(k)$, $y_i^+(k)$, $v_i(k)$ for each node i. One iteration of the improved ADMM recursive algorithm will be written as follows:

1. Minimization step: For each individual node i, the following optimization problem is solved by:

$$
X_i(k+1) := \arg\min_{X_i(k)} \{\mathcal{L}_i(X_i(k)) : H(X_i) \leq 0, E(X_i) = 0\} \tag{4.11}
$$

This minimization step is a convex optimization problem with two local variables $\overline{Q}_i(k)$ and $\overline{Q}_i^+(k)$ and the constraints are also linear. The objective function can be solved analytically by evaluating the corresponding KarushKuhn-Tucker (KKT) conditions [119]. Given the fact that the expressions are bulky and we skip them here for sake of brevity. According to the consensus algorithm, each objective function can be minimized independently because the optimization process only uses the local variables at node i. The solution of the minimization problem are denoted as $X_i(k+1)$ which also means $\overline{Q}_i(k+1)$ and $\overline{Q}_i^+(k+1)$.

2. Global variables update step: For each node i, the global reactive power variable of node i will be updated associated with the neighbouring node's local variable $\overline{Q}_{i+1}$ of node i. The variable for each node is updated according to the following rules:

$$Q_i(k+1) = \frac{1}{2}(\overline{Q}_i^+(k+1) + \overline{Q}_{i+1}(k+1)) + \frac{1}{\zeta_i}y_i^+(k) \tag{4.12a}$$

$$Q_n(k+1) = 0, Q_1(k+1) = 0, V_{n+1} = 0 \tag{4.12b}$$

Since this update step contains the communication with neighbouring nodes. The variable $\overline{Q}_{i+1}(k+1)$ comes from node $i+1$, which means the node $i+1$ will send the local $\overline{Q}_{i+1}(k+1)$ to node i if the minimization step of node $i+1$ completes. Then the new local variable $Q_i(k+1)$, the average of local variables in self-node and forward neighbouring nodes, will be obtained and send to backward neighbouring nodes for initializing next iteration.

3. Lagrangian multipliers update step: The local Lagrangian multipliers will be stored by each node independently. The update rules for each node are the following:

$$y_i(k+1) = y_i(k) + \rho(\overline{Q}_i(k+1) - Q_{i-1}(k)) \tag{4.13a}$$

$$y_i^+(k+1) = y_i^+(k) + \rho(\overline{Q}_i^+(k+1) - Q_i(k)) \tag{4.13b}$$

All variables in this step have been communicated in the global variables update step. And the updated Lagrangian multipliers will be stored and prepared for next iteration.

The ADMM algorithm always requires information exchange to update the local variables between the neighbouring nodes. These local variables can influence each other and finally get the optimal feasible solution. The actual values of reactive power injection/absorption by local inverter can be obtained by each node from the global variables

$$q_{iG} = Q_i - Q_{i-1} + q_{iL} \tag{4.14}$$

It should be noted that q_{iG} will be within the allowed range given by the $\overline{s}_i$ in (4.8b). In addition, the addition of a communication system will inevitably impact the algorithm, for example by introducing a message delay or packet loss for an uncertain period of time. To analyze the effect of the communication time-delay model on the performance of the iterative results, we will develop a stochastic end-to-end time-delay model primarily.

4.3.2 Stochastic Time Delay Model in ADMM algorithm

4.3.2.1 Communication Delay Model

The components of the end-to-end delay can be divided into four categories: processing delay, transmission delay, propagation delay and queueing delay. From a measurement point of view, this end-to-end delay over a fixed path mainly consists of two components: a deterministic delay D_d and a stochastic delay D_s [54]. The deterministic delay is mainly caused by the physical delay (fixed part of the processing delay generated by the all routers). This delay D_d can be approximated by a probability density of the normal distribution,

$$\varphi_1(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\mu)^2}{2\sigma^2}} \tag{4.15}$$

where μ and σ are the mean value and standard deviation value, respectively. The mean value μ is larger than the minimum processing delay.

The random part of the processing delay is typically a stochastic value because it is not precisely the same for each probe-packet in the router. In [56], an extensive research was found to assess the distributions of on-period and off-period for Internet traffic between fixed source and destination pairs. There are three parametric models for the stochastic delay caused by Internet traffic, the exponential density model, the Weibull density model and the Polynomial (Pareto-like) density model. In this chapter, the exponential density model is adopted to analyze the stochastic delay D_s caused by the router processing delay and by interfering Internet traffic which originates from one alternating renewal process [22]. Hence

$$\varphi_2(t) = \lambda e^{-\lambda t} \tag{4.16}$$

where λ^{-1} models the mean length of the closure periods which correspond to the periods where the Internet traffic has an open period. The open period in the Internet traffic is the period during which the probe-packet is blocked. The independent sum of the deterministic delay and the stochastic delay has probability density function (PDF) [22]

$$\varphi(t) = p\varphi_1(t) + q\varphi_1(t) * \varphi_2(t),\ t \geq 0 \tag{4.17}$$

where $p + q = 1$ and $\varphi_1(t) * \varphi_2(t) = \int_0^t \varphi_1(u)\varphi_2(t-u)du$. In terms of (4.15) and (4.16), the PDF (4.17) can be rewritten as

$$\varphi(t) = \frac{p}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\mu)^2}{2\sigma^2}} + \frac{q\lambda}{\sigma\sqrt{2\pi}} e^{-\lambda t} \int_0^t e^{\lambda u - \frac{(u-\mu)^2}{2\sigma^2}} du \tag{4.18}$$

In order to calculate the time-delay probability of each communication for all nodes, the PDF (4.18) will be recalculated to derive the Cumulative Distribution Function

(CDF) of time delay model as [22]

$$\begin{aligned} P(t) &= \int_0^t \varphi(u)du \\ &= \frac{1}{2}\{erf(\frac{\mu}{\sqrt{2}\sigma}) + erf(\frac{t-\mu}{\sqrt{2}\sigma})\} \\ &+ \frac{p-1}{2}e^{\eta}\{erf(\frac{\lambda\sigma^2+\mu}{\sqrt{2}\sigma}) + erf(\frac{t-\lambda\sigma^2-\mu}{\sqrt{2}\sigma})\} \end{aligned} \tag{4.19}$$

where $\eta = \frac{1}{2}\lambda^2\sigma^2 + \mu\lambda - \lambda t$ and $erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}$ is the error function. The relative parameters can be set as $\mu = 5.3ms$, $\sigma = 0.078$, $p = 0.580$ and $\lambda = 1.39$. Consequently, the probability density curve can be found in Fig. 4.3. The red line is the probability density curve and the blue area is the probability density histogram, which shows the probability density histogram is consistent with the probability density curve. According to equation (4.19), we can obtain the different probabilities of time-delay for each communication procedure which will be added into the ADMM algorithm to analyze the performance.

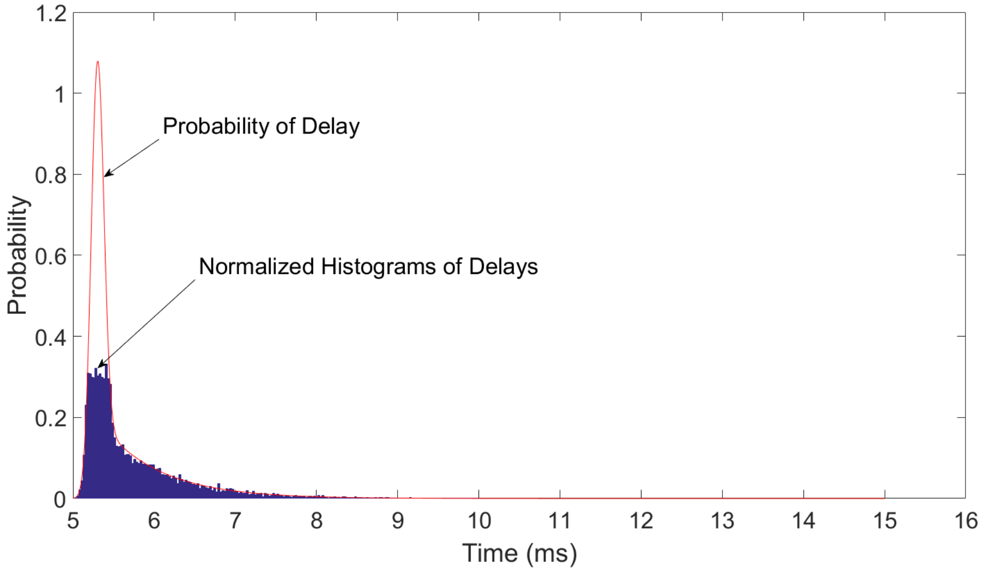


Figure 4.3: The probability density curve of communication delay.

4.3.2.2 Message Transmission Mechanism

The aim of this chapter is to investigate the decentralized OPF algorithm by applying the different probabilities of stochastic communication time-delay. In terms of the ADMM algorithm and communication delay model, we present the message transmission mechanism during the iterative procedure of the ADMM algorithm in detail. According to equations (4.11) to (4.13) and Fig. 4.2, we summarize the detailed iterative process for kth iteration as follow:

> (**Step 1**) Each node i would minimize the individual objective function first to achieve the updated local variables $(\overline{Q}_i(k+1), \overline{Q}_i^+(k+1), V_i(k+1))$ independently by using the equation (4.11).
>
> (**Step 2**) Node i will transmit the updated variable $\overline{Q}_i(k+1)$ to node $i-1$ when the minimization step achieves the updated variables. For node $i-1$, the received variable $\overline{Q}_i(k+1)$ from node i can be defined as $\overline{Q}_{i+1}(k+1)$ in (4.12a). Meanwhile, node i would receive the updated $\overline{Q}_{i+1}(k+1)$ from node $i+1$ when node $i+1$ completes the computation of minimization step. All the communications will begin immediately when the minimization step is completed.
>
> (**Step 3**) For node i, when the updated variables of neighbouring nodes are received, the new global variable $Q_i(k+1)$ can be obtained by using (4.12a) and the Lagrange multipliers $y_i(k+1)$, $y_i^+(k+1)$ can be updated by rules (4.13) immediately, which means that a full iteration calculation is accomplished. However, we still need to transmit the global updated variables to neighbouring nodes in order to begin the next iteration.
>
> (**Step 4**) Node i sends updated global variable $Q_i(k+1)$ and $V_i(k+1)$ to node $i+1$. At the same time, node i will receive the global variable $Q_{i-1}(k+1)$ and $V_{i-1}(k+1)$ from node $i-1$ when node $i-1$ completes the update step.

Then the iterative process will be repeated until the result satisfies a certain error condition. The above communication mechanism shows that each node will exchange the information with backward and forward neighbouring nodes for each iteration independently. Note that the backward links transmit the local variables $\overline{Q}_i(k+1)$ to backward neighbouring nodes and the forward links transmit the update global reactive power variable $Q_i(k+1)$ and $V_i(k+1)$ to forward neighbouring nodes. Although each iteration in the ADMM algorithm is decentralized, the proposed algorithm can still obtain the optimal feasible solution through the limited internal information exchange between neighbouring nodes.

Algorithm 1: Synchronous ADMM Algorithm

```
process for local node $i$, $i \in 1, ..., \nu$
  initialize local variables $X_i(0)$, k=0.
  repeat
      update to obtain $X_i(k+1)$
        wait $\leq t_{dm}$
      until all nodes complete the computation
      transmit $\overline{Q}_i(k+1)$ to backward nodes
      receive $\overline{Q}_{i+1}(k+1)$ from forward nodes
        wait $t_{ds}$
      until time reaches $t_{ds}$
      update to obtain $Q_i(k+1)$
      update to obtain $y_i(k+1)$, $y_i^+(k+1)$
        wait $\leq t_{du}$
      until all nodes complete the computation
      transmit $Q_i(k+1)$ to forward nodes
      receive $Q_{i-1}(k+1)$ from backward nodes
        wait $t_{ds}$
      until time reaches $t_{ds}$
      k=k+1
  untill satisfied the defined minimum error
 end process
```

According to the above description of the communication mechanism, it is easy to find that each iteration will have a fixed periodic time if the computation time and communication time are fixed. However, if the communication time is stochastic, the periodic time of each iteration will be always different for each node. When all nodes in the algorithm start to update the variables at the same time, it is necessary to discuss the synchronization issue here because the communication time of each transmission is always different. In this chapter, both synchronous (synchronization device installed) and asynchronous (no synchronization device installed) algorithms are proposed to analyze the performance of ADMM algorithm. When each node is equipped with an additional GPS synchronization interface, the synchronization issue may be solved easily. Otherwise, the algorithm can rely on the internal clocks to achieve the synchronization, but the effect is not as good as the GPS synchronization [120]. On the other hand, without any synchronization device, the algorithm can consider to utilize an asynchronous strategy to optimize the target. The details of both synchronous and asynchronous algorithms will be discussed in the following.

The synchronous distributed ADMM algorithm is outlined in Algorithm 1. In Fig. 4.4, we assume that the computation time t_{dm} (t_1 to t_2) and t_{du} (t_3 to t_4) are the constant values for all nodes. The red line is the backward link which means each node will send messages to the backward neighbouring nodes and the pink line is the forward link which means each node will send messages to the forward neighbouring nodes as shown in Fig. 4.2. Fig. 4.4 (a) is the synchronous algorithm timing diagram, where the maximum communication time in every iteration for each node is locked by the threshold time t_{ds} (assume t_2 to t_3 equals t_4 to t_5). For synchronous algorithm, each node will be equipped with an external synchronization interface, like GPS, to keep each step have the same clock. Specifically, after the step of minimization of objective function, each node must wait until all nodes receive the updated local variable $\overline{Q}_{i+1}(k+1)$ from backward node before proceeding step 3. We assume that each node starts calculating t_{ds} when the minimization step or update step is just completed. When the backward link communication time reaches the threshold time t_{ds}, each node will update its own local variables by (4.12) and (4.13) to obtain the new local variables and then send the new updated global variables to forward nodes. When time reaches threshold time t_{ds} in the forward link communication, each node will begin the next iterative procedure. This is the

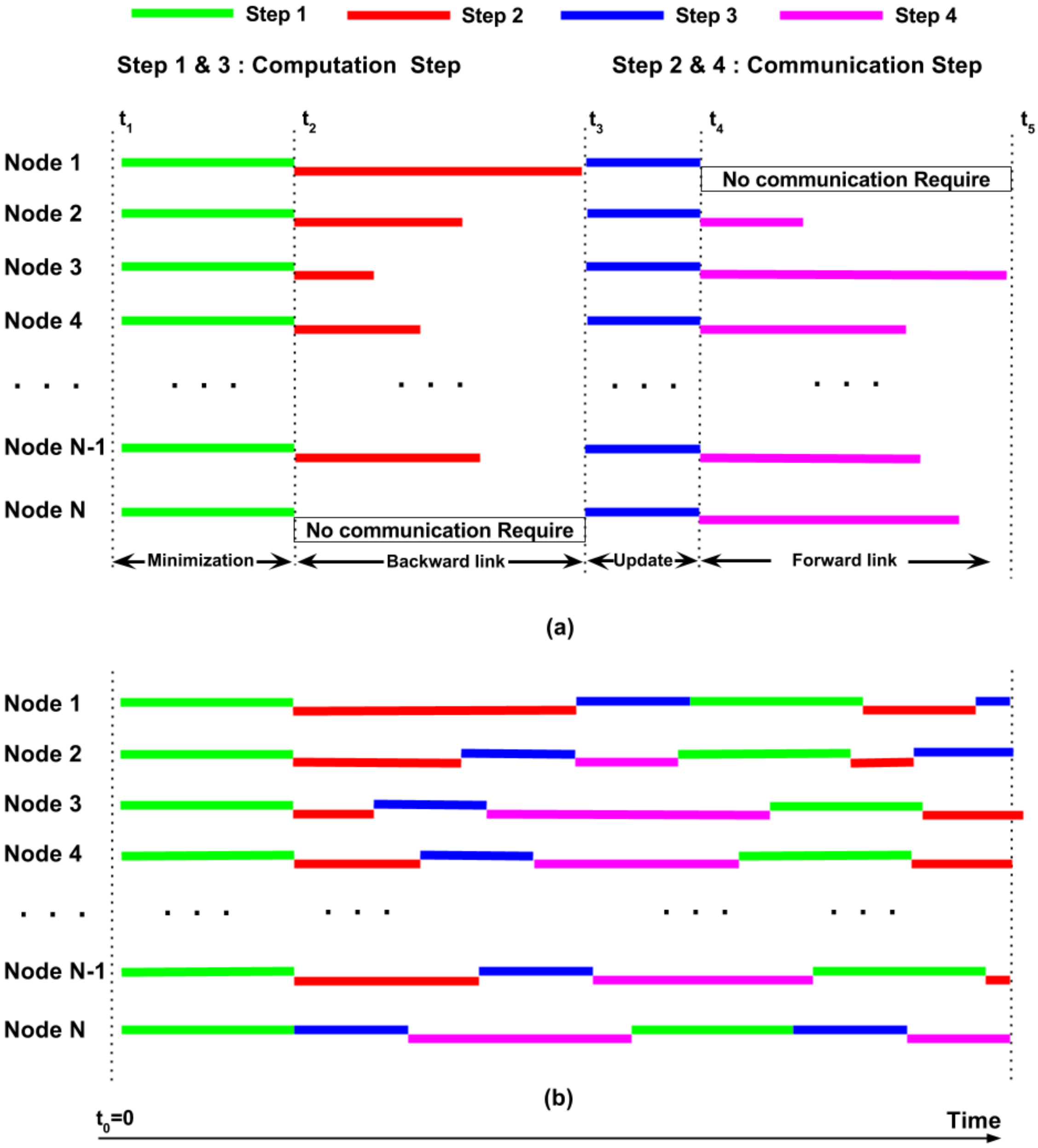


Figure 4.4: Illustration of synchronous and asynchronous distributed ADMM algorithm. (a) Synchronous distributed ADMM algorithm; (b) Asynchronous distributed ADMM algorithm.

detailed process of a complete iteration period for the synchronous algorithm.

Algorithm 2: Asynchronous ADMM Algorithm

```
process for local node $i$, $i \in 1, ..., \nu$
    initialize local variables $X_i(0)$, k=0.
    repeat
        update to obtain $X_i(k+1)$
        transmit $\overline{Q}_i(k+1)$ to backward nodes
        receive $\overline{Q}_{i+1}(k+1)$ from forward nodes
            wait $\leq t_{da}$
        until node $i$ receives or time reaches $t_{da}$
        update to obtain $Q_i(k+1)$
        update to obtain $y_i(k+1)$, $y_i^+(k+1)$
        transmit $Q_i(k+1)$ to forward nodes
        receive $Q_{i-1}(k+1)$ from backward nodes
            wait $\leq t_{da}$
        until node $i$ receives or time reaches $t_{da}$
        k=k+1
    untill satisfied the defined minimum error
end process
```

Compared with the synchronous algorithm, we also propose an asynchronous algorithm in detail. In the Fig. 4.4 (b), the timing diagram of asynchronous algorithm is presented in detail. We assume that each communication also has a bounded maximum transmission time t_{da}. In case of a larger delay or packet loss, the message may lead the algorithm to remain in the status of receiving the message which may endanger the algorithm convergence speed. However, it is obvious that we can enlarge the tolerance of maximum transmission time to reduce the probability of time-delay because the communication time-delay of each node will not affect the iteration process of other nodes. According to equation (4.19), we assume the time-delay probability of 0.1% as the bounded delay time t_{da} for the asynchronous algorithm. Each node i in this algorithm does not need to wait until all nodes have received the updated variable from the backward node before proceeding to the next step. Every node can execute the update steps to obtain the new local variables independently and immediately when it receives the message without considering whether the other nodes have received the messages. Under these circumstances, each node have no idle status and more iterations can be achieved by comparing to the synchronous algorithm at the same time interval. However, it should be noted that the communication message comes from neighbouring nodes, when node i starts calculating the communication time, neighbouring nodes sometimes may not complete the last computation step due to the asynchronous nature of the algorithm. It is possible that node i has not received any message from neighbouring nodes (perhaps the message is still in transit due to late transmission) when the communication time of node i reaches the threshold time t_{da}. Then we propose to update the variables by using the previous received message in order to keep the algorithm running without extra waiting time. As shown in Fig. 4.4 (b), without the limitation of synchronization problem, each node can update its own variables more frequently. The outline of asynchronous algorithm is listed in Algorithm 2.

In Fig. 4.4, during the same time interval, all nodes in synchronous ADMM algorithm just finish one iterative period, but some nodes in asynchronous ADMM algorithm almost completes one and a half iterative period. It is obviously that different nodes under different communication time-delay without extra waiting can shorten the iteration period and increase the number of iterations. Consequently, the asynchronous algorithm can speed up the convergence rate faster than the synchronous algorithm to obtain a high theoretical accuracy. The simulation results demonstrate convergence speed for both algorithms and the details will be discussed in result section. We also assume that each node can always receive the message in time for synchronous and asynchronous algorithms without time-delay. If some nodes do not receive the message from the backward node or the forward node within threshold time, the message will be considered as a packet lost. Then other improved measures will be taken to continue the next step.

4.3.3 Convergence Analysis for Asynchronous ADMM Algorithm

The convergence analysis of synchronous ADMM algorithm has been investigated in [24,25,47,119]. In this section, the convergence behavior of asynchronous ADMM algorithm will be studied. Some assumptions regarding the problem are made. Let ∇F_i be the gradient or subgradient of F_i in (4.8a). And we also define k_i^{τ} as a new sequence of node i, which implies that the gradient calculation may use old parameters due to the delayed message or lost message. x_i and $\overline{x}_i$ are the global and local variables for each node i, respectively. Then, the following assumptions are listed.

Assumption 1: For each node i, the individual function gradient ∇F_i is Lipchitz continuous, and there exists a constant $K_i > 0$, such that

$$\| \nabla F_i(\overline{x}_i(k+1)) - \nabla F_i(x_i(k+1)) \| \leq K_i \| \overline{x}_i(k+1) - x_i(k+1) \| \tag{4.20}$$

In addition, $\mathcal{X}$ is a closed, convex and compact set. The power loss function $F_i(x_i)$ is bounded from below over $\mathcal{X}$.

Assumption 2: The total delays are bounded. For each node i, there exists finite constant T_i such that $k - k_i^{\tau} \leq T_i$ for all k.

Assumption 3: For each node i, the stepsize ρ_i is chosen large enough such that:

$$\alpha_i = \rho_i - \frac{2\rho + 7K_i}{\rho_i^2} K_i(T_i+1)^2 - K_i T_i^2 > 0 \tag{4.21a}$$

$$\beta_i = \rho_i - 7K_i > 0 \tag{4.21b}$$

Assumption 1 is the standard in the context of non-convex optimization [121] and is satisfied for most problems of interest. According to assumption 2, when x_i is updated in asynchronous algorithm, the parameter used to update the variables should be the latest received parameter. The convergence of the asynchronous algorithm can be verified by the following lemma.

Lemma 1: Suppose that assumptions 1, 2 and 3 hold true. Then we have the following true for asynchronous algorithm.

(a) $\| y_i(k+1) - y_i(k) \|_2^2 \leq K_i^2(T_i+1) \sum_{\kappa=0}^{T_i} \| x(k+1-\kappa) - x(k-\kappa) \|_2^2$

(b) The augmented Lagrangian is lower bounded and satisfies

$$\mathcal{L}(\{\overline{x}_i(k)\}; \{x_i(k)\}, \{y_i(k)\}) \geq P_{los} - \sum_{i=1}^{\nu} \frac{Ki}{2} diam^2(\mathcal{X}) > -\infty \tag{4.22}$$

The proof of Lemma 1 can be found in Appendix A.1. Lemma 1(a) presents that there exists certain finite $k < \infty$ such that the augmented Lagrangian values are non-increasing after k iterations. Lemmas 1(b) presents that the Lagrangian is lower bounded. Then, we achieve that the augmented Lagrangian function is convergent.

The subsequent theorem proves the final convergence result and other properties.

Theorem 1: (a) The iterates generated by the asynchronous algorithm converges if the following is true

$$\lim_{k\to\infty} \| x_i(k+1) - x_i(k) \| = 0, \quad i = 1, ..., \nu \tag{4.23a}$$

$$\lim_{k\to\infty} \| \overline{x}_i(k+1) - \overline{x}_i(k) \| = 0, \quad i = 1, ..., \nu \tag{4.23b}$$

$$\lim_{k\to\infty} \| y_i(k+1) - y_i(k) \| = 0, \quad i = 1, ..., \nu \tag{4.23c}$$

(b) For each node i at k iterations, certain sequences $\{\{\overline{x}_i^*\}, \{x_i^*\}, \{y_i^*\}\}$ converges to the set of stationary solution of (4.5) and satisfies

$$\nabla F_i(\overline{x}_i^*) + y_i^* = 0, \quad i = 1, ..., \nu \tag{4.24a}$$

$$\overline{x}_i^* = x_i^*, \quad i = 1, ..., \nu \tag{4.24b}$$

The proof of Theorem 1 can be found in Appendix A.2. Note that it suffices to show that asynchronous algorithm converges to a stationary solution of (4.6) which is equivalent to (4.5). In other words, $\{x_i^*\}$ can be the solution of (4.5). It is emphasized that the asynchronous algorithm may not converge to a globally optimal solution.

4.4 Performance Assessment of Improved Strategies

In the previous subsection, we derived the mathematics and communication mechanism of synchronous and asynchronous ADMM algorithms. When the communication time-delay is added to both algorithms, the convergence performance of both algorithms will certainly be affected due to unreceived variables, for example, unstable results, low quality results and slow convergence. In this section, we will take different improved measures to assess the effect of time-delay of both synchronous and asynchronous algorithms for this OPF problem.

4.4.1 Strategy I-Skipping Strategy (SS)

In this strategy, we propose the skipping strategy that means if the communication message is not delivered within the threshold time, the unreceived node will ignore the delayed message and not update the local variables. Then the node will wait until the successful communication of the next step (other parameters will use data from last successful iteration). For every iteration, each node needs to obtain two messages, the backward link message and the forward link message. Both messages may have different degrees of influence on the iterative algorithm. Therefore, we may set different communication threshold times that relatively important communication link can be distributed a high bandwidth to increase the probability of receiving message. The simple expression for skipping strategy in (4.11)-(4.13) can be written as:

$$X_{is}(k+1) := \arg\min_{X_{is}} \{\mathcal{L}_{is}(X_{is}) : H(X_{is}) \leq 0, E(X_{is}) = 0\} \tag{4.25a}$$

$$Q_{is}(k+1) = \frac{1}{2}(\overline{Q}_{is}^{+}(k+1) + \overline{Q}_{is+1}(k+1)) + \frac{1}{\zeta_i} y_{is}^{+}(k) \tag{4.25b}$$

$$y_{is}(k+1) = y_{is}(k) + \rho(\overline{Q}_{is}(k+1) - Q_{is-1}(k)) \tag{4.25c}$$

where the subscript is means the set of nodes whose messages receive on time at kth iteration. For the backward link delay, we will only update the variable of the received node by using (4.25b) and skip unreceived nodes' update step. For the forward link delay, we plan to skip the update step for those nodes without receiving updated global variable Q_{i-1}. The variable update of other nodes will be calculated in accordance with equations (4.25a) and (4.25c). The skipping strategy not only reduces the update frequency of the algorithm, but also affects the neighbouring nodes' normal update of the algorithm due to the communication time-delay, which may lead to unstable convergence of the system. Therefore, we propose the previous value strategy, using the previous received message, to improve the convergence performance.

4.4.2 Strategy II-Previous Value Strategy (PVS)

The previous value strategy replaces the delayed or lost message by using the saved variables from the last successful communication. Each node can install a storage device to save the data generated from the previous normal iteration. When the communication delay occurs, the stored information can be invoked instead of the variables that have not be received within the threshold time. The update equations (4.11)-(4.13) can be modified as

$$X_{ip}(k+1) := \arg\min_{X_{ip}} \{\mathcal{L}_{ip}(X_{ip}) : H(X_{ip}) \leq 0, E(X_{ip}) = 0\} \tag{4.26a}$$

$$Q_{ip}(k+1) = \frac{1}{2}(\overline{Q}^{+}_{ip}(k+1) + \overline{Q}_{ip+1}(k)) + \frac{1}{\zeta_i} y^{+}_{ip}(k) \tag{4.26b}$$

$$y_{ip}(k+1) = y_{ip}(k) + \rho(\overline{Q}_{ip}(k+1) - Q_{ip-1}(k-1)) \tag{4.26c}$$

where the subscript ip is the set of nodes whose messages do not arrive on time as kth iteration. The variable update of unreceived nodes will exploit (4.26a)-(4.26c) and other nodes' variable update still follows equations (4.11)-(4.13). When time-delay happens in the forward link, the global reactive power variable Q_{i-1} in (4.26a) also will take advantage of the previous saved variables. This strategy may also decrease the convergence rate because the partial iterative processes using previous data without updated new variables may slow down the update speed of both self-node and neighbouring nodes in theory. For a real distribution network, this strategy is more suitable for certain scenarios that are prone to transmission delay or packet loss while the requirement of optimization accuracy is not very stringent. It is necessary to propose other measures to speed up the convergence rate. Therefore, we propose to use the predict value by autoregressive (AR) strategy to replace the message that does not arrive on time.

4.4.3 Strategy III-AR Strategy (ARS)

When the time reaches the threshold t_{ds} in the iterative process, if some nodes have not received any message from neighbouring nodes, we can use the predicted value in advance instead of the previous saved message in the previous value strategy. Estimating the correlation between past and present data is one of the effective approaches to understanding the behaviour of time series data. The predicted value can be closer to the original value than the previous saved value. Forecast can begin when the communication message was received in the last successful communication. The forecast can be made during the computation time and communication waiting time, which do not need extra forecasting time to predict the unreceived message. In order to understand the principle, this subsection will first provide the fundamental level of the theory and conceptual framework of the AR model to apply into the ADMM algorithm. Suppose the relationship between past successfully received messages and current unreceived message can be estimated using previous saved data. The general AR model $AR(\omega)$ of order ω is defined as [122]

$$\begin{aligned} a_t &= c + \sum_{i=1}^{\omega} \phi_i a_{t-i} + \epsilon_t \\ &= c + \phi_1 a_{t-1} + \phi_2 a_{t-2} + ... + \phi_\omega a_{t-\omega} + \epsilon_t \end{aligned} \tag{4.27}$$

where ω is the order of the AR model and $\phi_1, ..., \phi_\omega$ are the autoregressive coefficient which are constant parameters for the model, c is also the fixed value and ϵ_t is the stochastic parameter that we define as white noise, $\epsilon_t \sim T(0, \sigma^2)$. In addition, $a_1, a_2, ..., a_T$ are the previous values of time series data used to predict the current value. According to the autoregressive coefficient, the likelihood function of the AR model can be written as

$$p_l(\phi, \sigma^2) = \prod_{t=1}^{T} \frac{1}{\sqrt{2\pi\sigma^2}} exp\{-\frac{1}{2\sigma^2}(a_t - \sum_{i=1}^{\omega} \phi_i a_{t-i})^2\} \tag{4.28}$$

where the parameters of AR model can be obtained by using the Yule-Walker equations [123]. Taking a derivative of the logarithm of formula (4.28) by

$$\begin{aligned} -\frac{1}{\sigma^2}\sum_{t=1}^{T}(a_t - \sum_{l=1}^{\omega} \phi_l a_{t-l})a_{t-i} = 0 \\ \sum_{t-1}^{T}\sum_{l=1}^{\omega} \phi_l a_{t-l} a_{t-i} = \sum_{t-1}^{T} a_t a_{t-i} \end{aligned} \tag{4.29}$$

where $\sum_{t=1}^{T} a_{t-l}a_{t-i}$ is taken to be autocoveriance $C_{|i-l|}$.

Similarly, the derivative of each parameters $\phi_1, \phi_2, ..., \phi_\omega$ gives:

$$\begin{pmatrix} C_0 & C_1 & \cdots & C_{\omega-1} \\ C_1 & C_0 & \cdots & C_{\omega-2} \\ \vdots & \vdots & \ddots & \vdots \\ C_{\omega-1} & C_{\omega-2} & \cdots & C_0 \end{pmatrix} \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_\omega \end{pmatrix} = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_\omega \end{pmatrix} \tag{4.30}$$

All the autoregressive coefficients of the AR model can be obtained by the simultaneous formula in (4.30). The variance σ^2 can be written as:

$$\sigma^2 = \frac{1}{T+\omega}\sum_{t=1}^{T}(a_t - \sum_{i=1}^{\omega} \phi_i a_{t-i})^2 \tag{4.31}$$

The performance of autoregressive model is depended on the order. Next, the determination of the AR model order will be discussed. Decreasing the order against the time series data reduces the estimation performance of the AR model. However, increasing the order leads to more complex behavior and even fails to obtain appropriate estimations. This paper adapts the Akaike-Information-Criterion(AIC) as the evaluation function of the AR model to balance the size of order. The evaluation function of the AR model can be calculated as [124] by ϕ_i yields the following expression:

$$AIC = -2\sum_{t=1}^{T} ln\{p(a_t \mid \phi, \sigma^2)\} + 2\overline{\omega}. \tag{4.32}$$

where $\overline{\omega}$ is the order of the AR model and the value of $\overline{\omega}$ can be chosen from the order index 1,2,3...,ω. The evaluation function from AIC will be applied to the AR strategy to emulate the algorithm. If the node i do not receive the message from neighbouring nodes within a threshold value, the algorithm will adopt the predictive values to replace the unreceived $\overline{Q}^{+}_{i+1}(k+1)$ and $Q_{i-1}(k+1)$ in (4.11)-(4.13), respectively.

$$X_{ia}(k+1) := \arg\min_{X_{ia}}\{\mathcal{L}_{ia}(X_{ia}) : H(X_{ia}) \leq 0, E(X_{ia}) = 0\} \tag{4.33a}$$

$$Q_{ia}(k+1) = \frac{1}{2}(\overline{Q}^{+}_{ia}(k+1) + \overline{a}_{ia+1}(k)) + \frac{1}{\zeta_i} y^{+}_{ia}(k) \tag{4.33b}$$

$$y_{ia}(k+1) = y_{ia}(k) + \rho(\overline{Q}_{ia}(k+1) - a_{ia-1}(k)) \tag{4.33c}$$

where the subscript ia is the set of nodes whose message do not arrive on time. $a_{ia-1}(k)$ is the replacement value of the unreceived parameter $Q_{ia-1}(k)$ in Minimization step (4.11) and update step and (4.13), respectively. (4.33b) also use the predictive value $\overline{a}_{ia+1}(k)$ instead of unreceived data $\overline{Q}^{+}_{ia+1}(k+1)$ in (4.12) if the delay happens. Other nodes will continue to follow the original formulas (4.11)-(4.13) to update the variables. For brevity, we have not included the detail of the AR derivation process.

4.4.4 Strategy VI-Weighted AR Strategy (WARS)

The estimated value from AR strategy exists certain fluctuations and errors during the prediction. Therefore, we propose to add a weighted term into the ADMM algorithm to reduce the error caused by the prediction to improve the convergence results. The node update expression in (4.11)-(4.13) for kth iteration can be rewritten as

$$X_{iw}(k+1) := \arg\min_{X_{iw}}\{\mathcal{L}_{iw}(X_{iw}) : H(X_{iw}) \leq 0, E(X_{iw}) = 0\} \tag{4.34a}$$

$$Q_{iw}(k+1) = \frac{1}{2}(\overline{Q}_{iw}^{+}(k+1) + (1+\overline{\gamma}_i)\overline{a}_{iw+1}(k)) + \frac{1}{\zeta_i}y_{iw}^{+}(k) \tag{4.34b}$$

$$y_{iw}(k+1) = y_{iw}(k) + \rho(\overline{Q}_{iw}(k+1) - (1+\gamma_i)a_{iw-1}(k)) \tag{4.34c}$$

where the subscript iw is the set of nodes whose message do not arrive on time. γ_i, $\overline{\gamma}_i$ are the weighted factors. The weighted terms $\gamma_i a_{iw-1}(k)$ and $\overline{\gamma}_i\overline{a}_{iw+1}(k)$ are added to execute the iterative steps in (4.34) if delay happens. Other nodes will continue to use the original expression to update the variables. These weighted factors can improve the fluctuation caused by the uncertainty of the packet loss and predictive error and also optimize the predictive variables to obtain a better convergence result. The improved weighted AR iterative steps will enable the predicted value to be closer to the optimal value.

4.4.5 Connection between Weighted AR ADMM and Conventional ADMM

Generally, ADMM algorithms can rapidly converge to a local optimal value and slowly reach to the global optimal value [125]. In order to find the connection between the conventional ADMM and the weighted AR ADMM, it is necessary to observe the difference between two iterative steps. Reference [25] presents the traditional ADMM iterative form for consensus minimization problem.

$$X_i(k+1) := \arg\min_{X_i}\{\mathcal{L}_i(X_i) : H(X_i) \leq 0, E(X_i) = 0\} \tag{4.35a}$$

$$Q(k+1) = \frac{1}{N}\sum_{i=1}^{N}(\overline{Q}_i(k+1) + \frac{1}{\rho}y_i(k)) \tag{4.35b}$$

$$y_i(k+1) = y_i(k) + \rho(\overline{Q}_i(k+1) - Q(k+1)). \tag{4.35c}$$

where ρ is the ADMM penalty factor and also stands for the particular step size. Such a conventional ADMM algorithm follows normalise routine. The details of the routine are reported in [25]. The objective function for node i contains the variables of adjacent nodes j in N_i. Therefore, the local variables for each individual formula require the information exchange with neighbouring nodes.

Comparing (4.34) and (4.35), it is obviously that the traditional ADMM algorithm is a particular case of the weighted AR ADMM by setting $\overline{Q}_i(k+1) = \frac{\overline{Q}^+_{iw}(k+1)+(1+\overline{\gamma}_i)\overline{a}_{iw+1}(k)}{2}$, $Q_i(k+1) = (1+\gamma_i)a_{iw-1}(k)$ and $\frac{1}{\rho} = \frac{1}{\zeta_i}$. The same coefficient $\frac{1}{\rho}$ is set to all consensus constraints in the conventional ADMM. Contrarily, the weighted AR ADMM assign the different coefficient $\frac{1}{\zeta_i}$ instead of the same coefficient $\frac{1}{\rho}$ in the conventional ADMM algorithm. In addition, the proposed weighted AR ADMM adds different weighted terms $\overline{\gamma}_i\overline{a}_{iw+1}(k)$ and $\gamma_i a_{iw-1}(k)$ to each node i because of the forecast error by the evaluation function, which could reduce the volatility of convergence results theoretically.

These changes can make the weighted AR ADMM to achieve a better efficiency than the traditional ADMM. To begin with, the traditional ADMM requires to information exchange with all neighbouring nodes j in N_i for every communication that can update the global variable Q_i and the Lagrange multipliers y_i of node i. Therefore, the conventional ADMM requires a relative larger communication cost per iteration. In contrast, the weighted AR ADMM is able to decrease the communication cost by communicating with less neighbouring nodes, for example, backward link communication only communicates to backward nodes and forward link communication only communicates to forward nodes. Furthermore, when communication delay happens, the unreceived message not only affects the variable update of self-node, but also affects the variable update of neighbouring nodes. Using predicted value in proposed weighted AR ADMM can minimize the error caused by the delay or packet loss as much as possible compared that in the traditional ADMM. In addition, the adapted weighted predictive value may produce a certain deviation from the original value which can improve the results from a local optimization to a global optimization, just like the crossover in genetic algorithms [126]. Finally, the conventional ADMM can only optimize its convergence speed by adjusting the penalty factor ρ, since other parameters are fixed. Whereas, the weighted AR ADMM has the flexibility by adjusting both weighted terms $\overline{\gamma}_i \overline{a}_{iw+1}(k)$, $\gamma_i a_{iw-1}(k)$ and coefficient term $\frac{1}{\zeta_i}$. Consequently, the weighted AR ADMM has the potential to obtain a relatively smaller fluctuation result and a faster and better convergence result than that in the conventional ADMM.

Summing up, comparing to the conventional ADMM, the weighted AR ADMM can not only reduce the volatility during the iterations, but also accelerate the convergence speed to obtain a better optimization result. Therefore, this proposed weighted AR ADMM can theoretically obtain a better target solution while time-delay is considered. The similar analysis can be derived for other strategies, but we skip them here for space limitations. In the following section, we demonstrate the effectiveness through the numerical experiments.

4.5 Case Study Results

In order to verify the ADMM algorithm with communication, a 33-bus medium-voltage DN in chapter 3 has been used as a case study. The detail of the data can be found in [13]. This system is a 12.66 kV radial distribution network system. It contains 33 buses and 32 branches and we propose to install four wind DGs (2,12,15,18) and four solar DGs (23,25,27,33) in the network [127]. In the experiments, both partial penetration (8 DGs) and full penetration (full DGs) are discussed to perform the algorithms performance.

4.5.1 Partial DGs Penetration Optimization

The simulation results are based on the 8 DGs penetration of the DN which means only 8 DGs will regulate the reactive power to optimize the problem. The details can be shown as follows.

4.5.1.1 Observation of General Convergence Speed

In this section, we consider to maximize the convergence speed of the proposed ADMM algorithm without communication time-delay. As we know, the applied ADMM formula has two important parameters, the penalty factor ρ and the convergence tolerance ε which could affect the convergence speed in the augmented Lagrangian formula (4.10). Fig. 4.5 illustrates the general synchronous ADMM convergence speed with different penalty factor value ρ for 8 DG network. We have decreased the penalty factor ρ from 1 to 0.00001. The result of convergence speed is sensitive to the value of ρ. The high values of ρ typically have a relatively slow convergence speed and poor iterative results while the iterative results sometimes occur certain fluctuations. The best choice of ρ which provide the fastest convergence speed for this particular case is 0.001 in the early stage of the iteration process. Subsequently, the convergence speed of $\rho = 0.001$ is slower than the speed of $\rho = 0.0001$ after 200 iterations. In other words, the minimization results of $\rho = 0.0001$ is better than that of $\rho = 0.001$ after about 200 iterations. Intuitively the convergence speed is mainly dependent on the interaction between the reactive power term and ADMM penalty term in (4.10). In other different cases, sometimes a little higher or smaller value of ρ may result in a slightly better convergence speed.

Fig. 4.5 also shows the different iterations for different tolerance values. For the maximum error $\varepsilon < 0.1$ compared to conventional centralized OPF algorithm, the ADMM only needs 9 iterations to reach the tolerance goal of less than 10%. However, after 200 iterations, the error is only less than 5%. Then about 400 iterations later, the tolerance ε can reach 0.025. It is typically that the ADMM algorithm has a faster convergence rate at the beginning of the iteration process, then the convergence speed will come down dramatically. In some special cases, it also should be noted that setting a high tolerance value (e.g., $\varepsilon = 0.1$) may results in a relatively large fluctuation at the beginning of the iteration process. It is necessary to set an appropriate tolerance value for different cases. In this chapter, we set the tolerance value as $\varepsilon < 0.05$ which could also help to choose the penalty factor $\rho = 0.001$ with faster convergence rate. Summing up, the observations made in this subsection provide general guidelines to set up an appropriate parameter for similar optimization case.

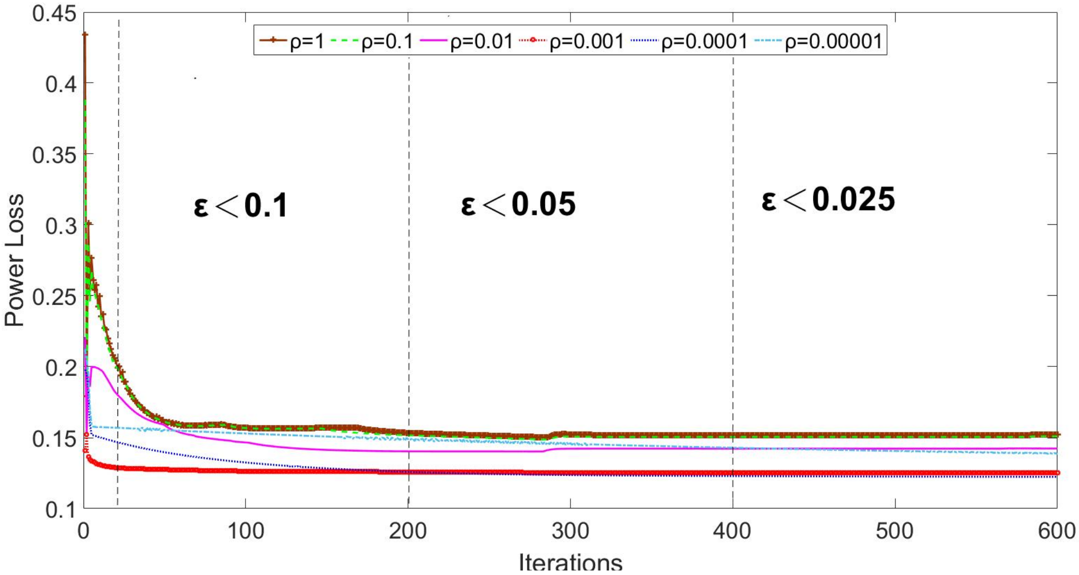


Figure 4.5: Illustration of convergence speed of distribution ADMM algorithm with different values of penalty factor ρ for 8 DG network.

4.5.1.2 Performance of Synchronous algorithm

In this section, we apply the communication delay to synchronous iterative algorithm to test the performance of the convergence results. According to equation (4.19), we set the time delay probability as 10% which the threshold time value t_{ds} can be calculated as 6.3363 ms. In the light of Fig. 4.2, each iteration requires twice information exchange, the backward link and the forward link. Hence, we divide communication into three different cases, the backward link case (only the backward link considering time-delay), the forward link case (only the forward link considering time-delay) and two-way link case (both links considering time-delay).

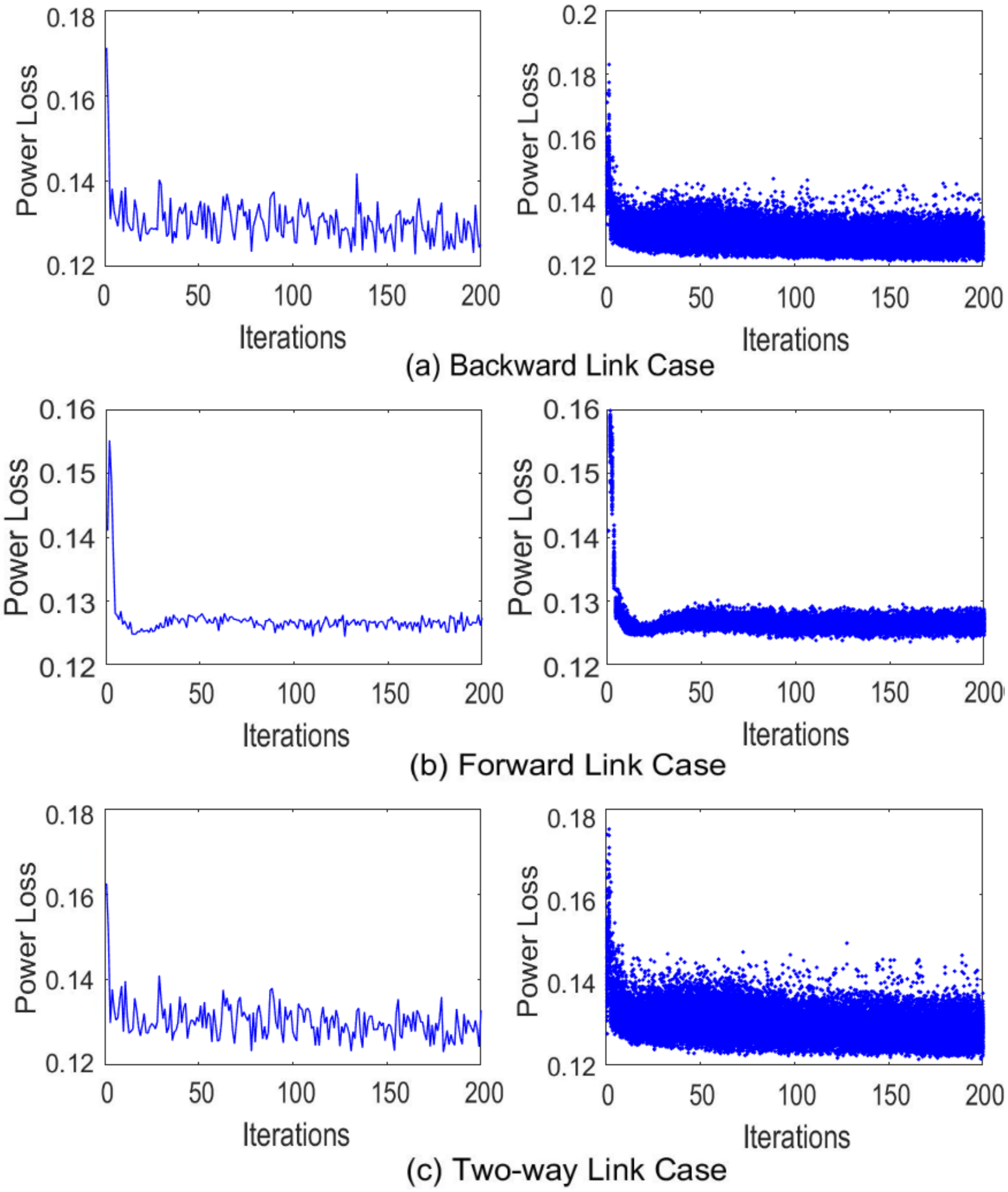


Figure 4.6: Comparison of convergence speed and statistic results of three different cases for synchronous skipping strategy.

Table 4.1: Statistical Results with 1000 Runs for Each Approach

	Synchronous			
	SS	PVS	ARS	WARS
$Mean$	0.1287	0.1298	0.1283	0.1243
$Variance$	$1.16E-5$	$7.12E-7$	$3.16E-7$	$6.20E-8$

Fig. 4.6 shows the effect of convergence speed and statistical results for different delay types compared to no-delay case in Fig. 4.5. When time-delay happens, the synchronous skipping strategy will be applied to deal with the update step of time-delay node. The left side of Fig. 4.6 presents the fluctuated convergence results in three cases under a fixed probability of time-delay. For the backward link, the optimization results always have a larger fluctuation during the iterations because the time-delay happens during the iterative process. For the forward link, the optimization results fluctuate less compared to the results of the backward link. On the other hand, two-way link case has the largest fluctuation because of the combination of backward link and forward link. The time-delay in backward link and two-way link both affect the update of global reactive power parameter in (4.12) which would significantly influence global reactive power update of both self-node and other neighbouring nodes of whole three terms in the augmented Lagrangian formulation (4.10). However, the forward link only affect the local reactive power variable of neighbouring nodes in (4.10). The right side of Fig. 4.6 demonstrates the statistical results for three cases (1000 stochastic time-delay runs each). The maximum fluctuation range is 0.1218 to 0.1474 (21.33% fluctuation) in backward link case, 0.1221 to 0.1355 (11.17% fluctuation) in forward link and 0.1214 to 0.1485 (22.58% fluctuation) in two-way link. Overall the results indicate that the convergence speed mainly depend more on the communication of step 2 in Fig. 4.4(a). When investigating the communication application for ADMM in such system, the bandwidth allocation should be studied to reduce the probability of packet loss during the backward link communication. From the results of these three cases, the synchronous skipping strategy cannot solve the fluctuations caused by the delay.

We next test the performance using previous value strategy. From this strategy, we only test the two-way link case as the space limitations. Fig. 4.7 shows the

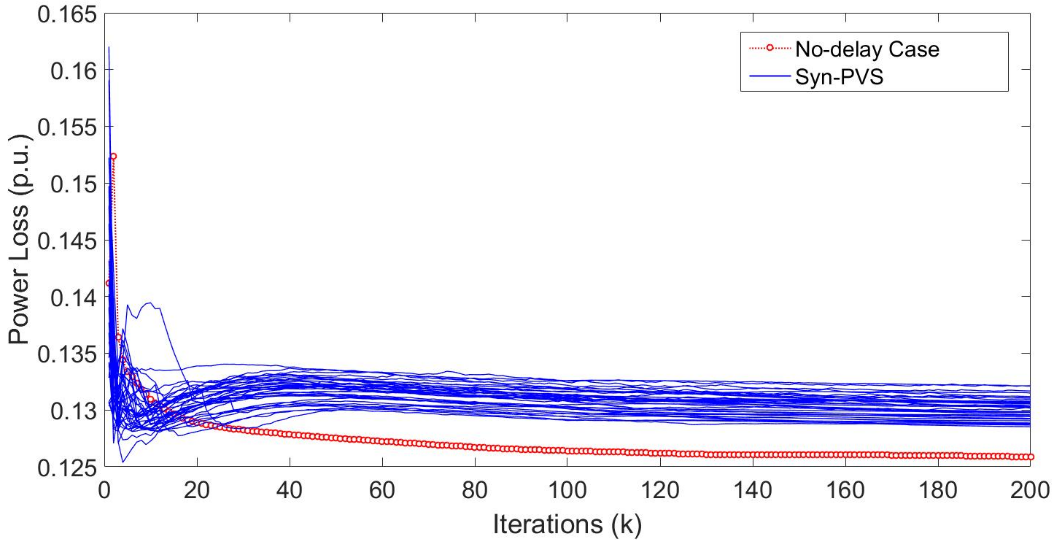


Figure 4.7: Comparison of convergence speed of synchronous no-delay case and synchronous Previous value strategy.

general optimization results of previous value strategy (100 stochastic time-delay runs) compared to the result of the no-delay case. It is clear that the results of using previous value strategy dramatically reduce the fluctuation range compared to the simulation results of skipping strategy in Fig. 4.6. In the early stages from 8 to 20 iterations, the convergence results appears to rise and one of the cases even rise to 0.1395 p.u.. Furthermore, the optimization result after 200 iterations still does not converge to a desirable value which only decreases to near 0.13 p.u.. The maximum 8.98% error after 200 iterations could be very inefficient for the ADMM algorithm. Therefore we have demonstrated that the proposed previous value strategy could only improve the fluctuation performance, but cannot speed up the convergence rate.

However, it should be noted that warm-starting the ADMM algorithm (e.g. forecast in advance) can be utilized to improve both the fluctuation in the skipping strategy and the convergence speed in the previous value strategy. In this subsection, the synchronous AR strategy is proposed to estimate the unreceived parameters which has a better simulation result compared with the previous value strategy. As shown in Fig. 4.8, we choose one typical fixed time-delay case to compare different synchronous strategies. The AR strategy speed up the convergence rate over the

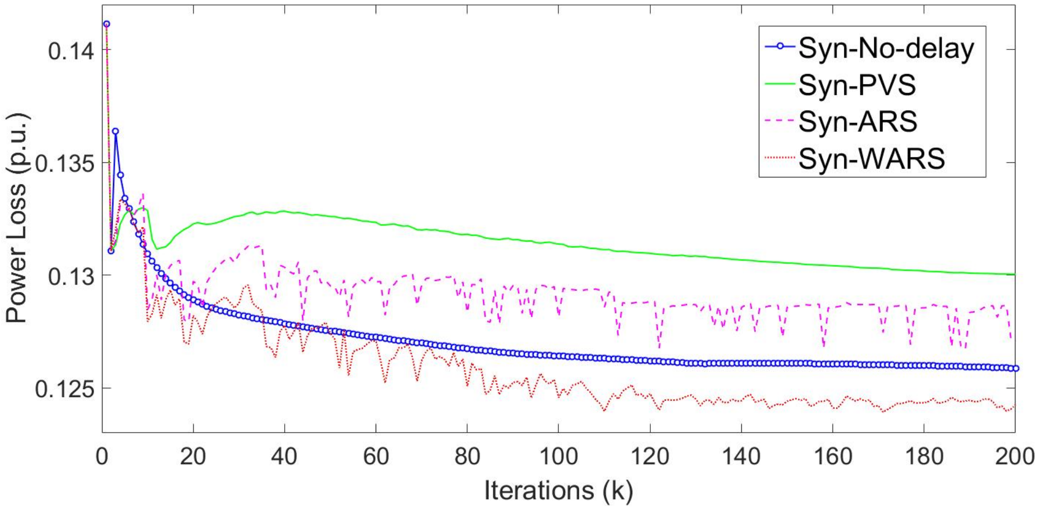


Figure 4.8: Comparison of convergence speed: Comparison of different synchronization strategies.

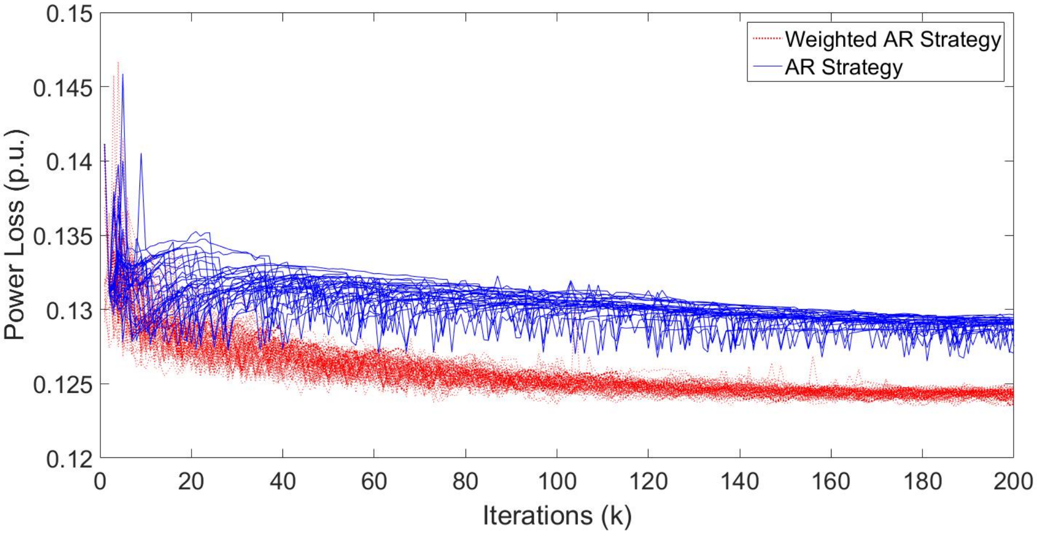


Figure 4.9: Comparison of convergence speed: Comparison of AR strategy and Weighted AR strategy (100 stochastic time-delay runs each).

previous value strategy but still has a large fluctuation because of the forecasting error. However, the good result is that this fluctuation is not very large compared to the synchronous no-delay case and the convergence result is also improved compared to the previous value strategy. The predictive parameter sometimes has a slight error fluctuation, we consider to modify the predictive values to decrease the estimation error to optimize the simulation results. Then the weighted AR strategy is proposed to improve the result of AR strategy. In Table 4.1, the peculiarity of weighted AR strategy with an appropriate weighted parameter, which the AR strategy do not modify the predictive value, is that due to a slight improvement of the predictive value there is an increased convergence speed, decreased fluctuation range and even significantly better optimization result than the result in the synchronous no-delay case. In Fig. 4.9, we also simulate 100 stochastic time-delay runs for each AR and weighted AR strategy. The modified global reactive power and Lagrangian multipliers can be more in line with the optimal values. At the beginning of the result between 10 to 30 iterations, the fluctuation range can be up to 12.5%. However, the results after 100 iterations only have a slight fluctuation and the final results at 200 iterations only have 1.0% fluctuation range. The original update parameters also have uncertainty in the early stage of iterative process, the AR prediction cannot be able to achieve an accurate value appropriately. The AR prediction values have better iteration results after 100 iterations because of the more predictable original update parameters. Comparing with the results 0.1258 p.u. of synchronous case without delay, the weighted AR strategy even can converge to mean 0.1243 p.u. which dramatically improve the local optimization result of the normal ADMM algorithm without delay.

It is well-know that the aggregators will be the fundamental part in the future smart grid [128]. The decentralized power system optimization scheme can really have a significant effect on the convergence rate in real-time OPF scheme. A distribution generator combined with distribution network aggregator could be a essential framework for smart grid in the future. As it is, our simulation results in synchronous weighted AR strategy with communication delay demonstrate that it is an efficient control strategy from a synchronous distributed optimization perspective.

Table 4.2: Statistical Results with 1000 Runs for Each Approach

	Asynchronous			
	SS	PVS	ARS	WARS
$Mean$	0.1239	0.1238	0.1237	0.1227
$Variance$	$4.96E-7$	$2.16E-7$	$1.15E-7$	$1.73E-7$

4.5.1.3 Performance of Asynchronous Algorithm

In this section, we proposed to apply the communication delay to an asynchronous ADMM algorithm. In this algorithm, we set 9.6146 ms (0.1% probability happens time-delay) as the bounded time delay threshold t_{da} for asynchronous algorithm which is larger than the threshold time 6.3363 ms in the synchronous strategy. Each node can update parameters using (4.11)-(4.13) without requirement of any synchronization devices. Under this circumstance, Fig. 4.10 demonstrates the iteration results of the proposed different asynchronous strategies compared to the results of synchronous strategy without delay case. The result is based on the wall clock time because the asynchronous algorithm do not require a synchronization device to wait in the process and have no specific iterative number. Although the asynchronous strategy has a much larger time-delay tolerance, the result in asynchronous strategy without delay still has a much better convergence speed and optimization result which can achieve 0.1231 p.u. compared to the 0.1258 p.u. in synchronous no-delay case at the same time interval. On the other hand, the synchronous strategy requires 1260ms to achieve 0.1258 p.u. of optimization result. However, the asynchronous strategy only needs 300ms to reach the same result, which means it is four times faster than the synchronous strategy. It also means we can decrease the ICT requirement of communication for asynchronous algorithm to achieve the results with same error tolerance if it is necessary. The increased convergence speed by the asynchronous algorithm mainly comes from the increasing number of the iterations and the reduction of the waiting time in the iterations.

In Fig. 4.11, the enlarged convergence performance in asynchronous algorithm with time-delay are displayed. The results of asynchronous skipping strategy show that the time-delay also brings a slight influence on the stability of the convergence per-

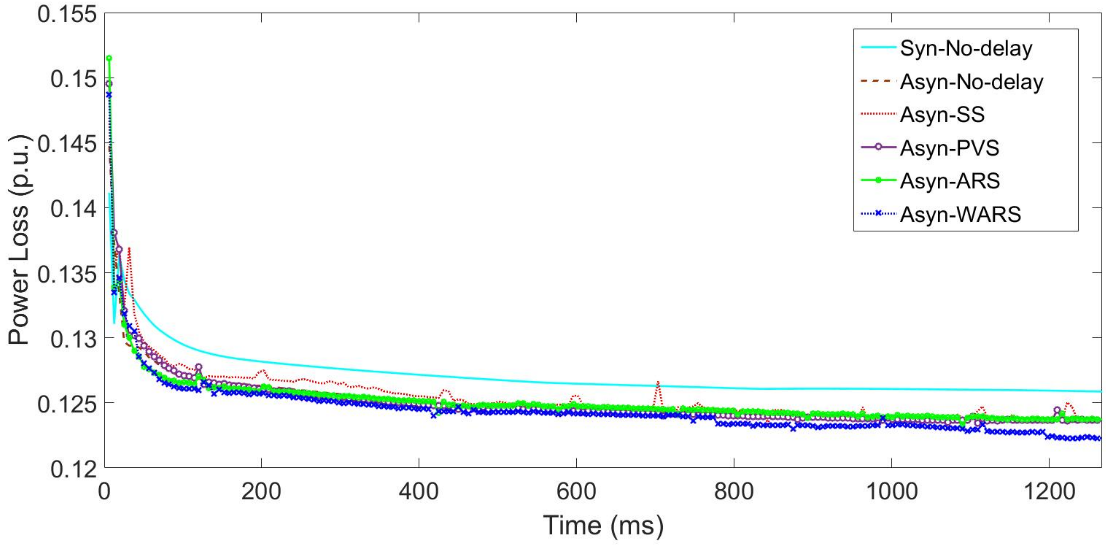


Figure 4.10: Comparison of synchronous no-delay case and different asynchronous strategies.

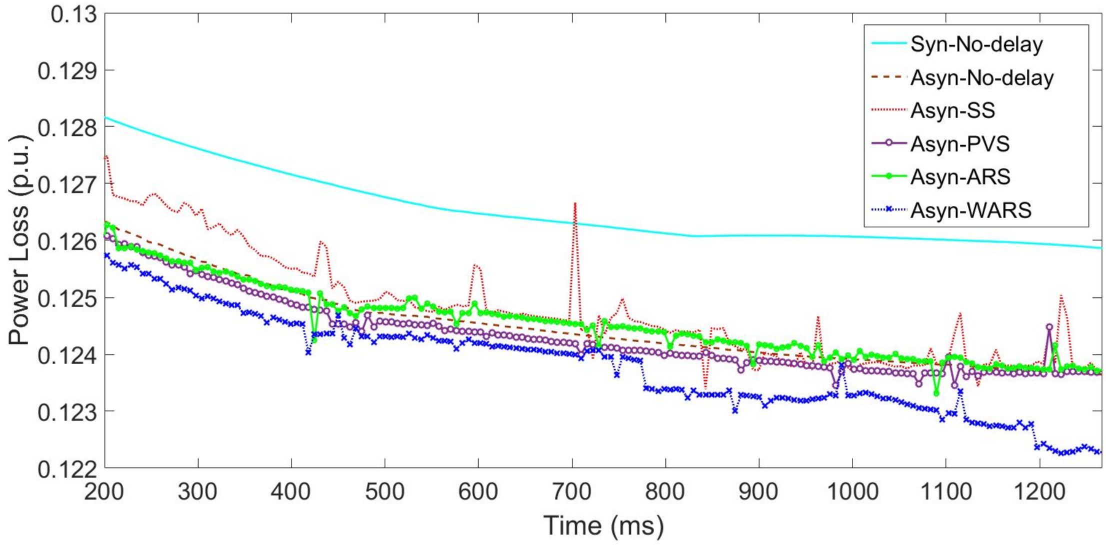


Figure 4.11: Enlarged convergence performance in asynchronous strategies.

formance even if the time-delay probability is only 0.1%, which indicates that the very low time-delay can induce a relative fluctuation in such an asynchronous algorithm. According to Table 4.2, the result of asynchronous weighted AR strategy utilizing the same time-delay probability presents that the optimization result can be improved to mean value with 0.1227 p.u. after 1000 runs. Meanwhile, the fluctuation performance can be improved effectively. In Table 4.2, we run 1000 simulations for each strategy. It should be noted that the asynchronous weighted AR strategy has a small fluctuation compared to the asynchronous skipping strategy. The uncertainty of the time-delay may reduce the predictability of the unreceived variables in the algorithm. The proposed weighted AR strategy can improve the optimization results, and also improve the accuracy of the forecast to reduce the fluctuation results. Relevant investigation of modified AR strategy with more accurate predictive value could be a new research direction in future.

4.5.2 Full DGs Penetration Optimization

The above simulation results are base on the partial DGs penetration (8 DGs). In this section, the results of full DGs penetration will be discussed.

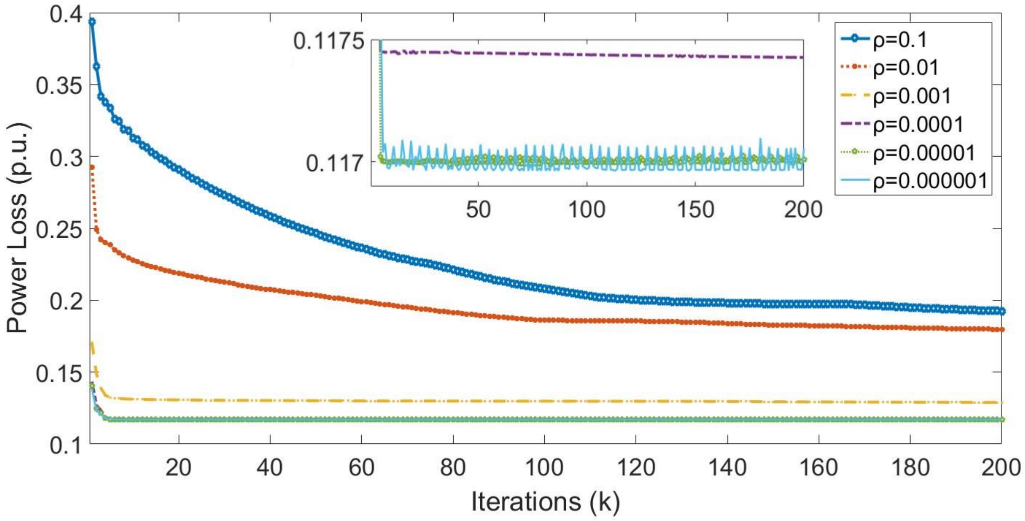


Figure 4.12: Illustration of convergence speed of distribution ADMM algorithm with different values of penalty factor ρ.

4.5.2.1 Observation of General Convergence Speed

As we know, the penalty factor ρ can affect the convergence speed in partial DGs penetration network. In this section, we also perform the different penalty factors to simulate the convergence speed. Fig. 4.12 shows the observation of convergence speed of full DGs penetration with different penalty factor ρ. The penalty factor ρ is tested from 0.1 to 0.000001. The best result of the convergence speed in this case is different from the result in 8 DGs case. It is obvious that when the penalty factor $\rho = 0.000001$, the iterative result has the fastest convergence speed. The full DGs penetration case has the different best penalty factor compared to the partial DGs penetration case. Meanwhile, the full DGs case has the faster convergence speed than the 8 DGs case, the result reaches the minimum value only after 5 iterations.

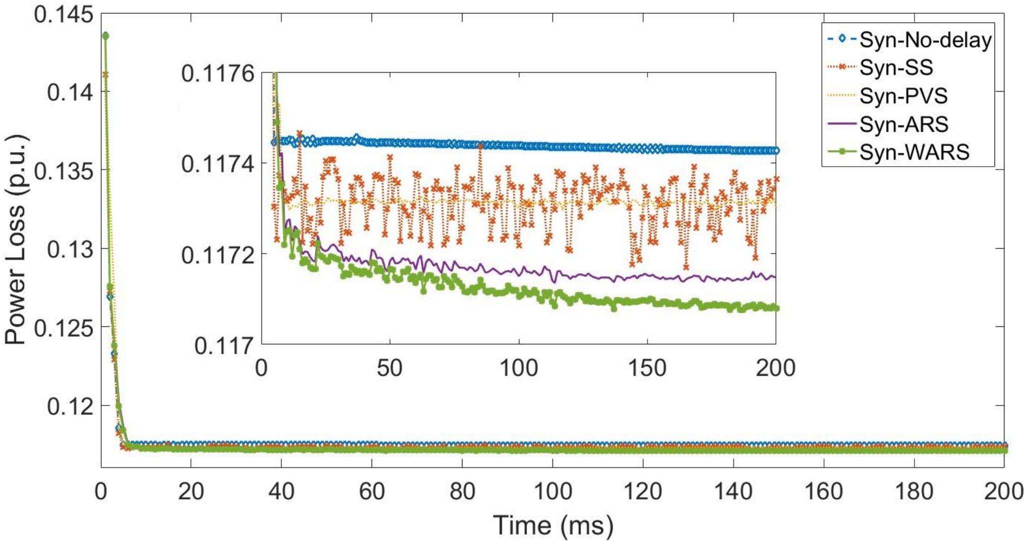


Figure 4.13: Comparison of convergence speed: Comparison of synchronous no-delay case and different synchronous strategies.

4.5.2.2 Performance of Synchronous Algorithm

According to the equation (4.19), we still set the time-delay probability as 10%. As depicts in Fig. 4.13, it presents different convergence results for no-delay case and different improved synchronous strategies under a fixed time-delay scenario. The simulation results show that the convergence speed does not change too much, which even can not distinguish their differences. Only when we enlarge the y-axial from 0.117 p.u. to 0.1176 p.u., the results can be clearly distinguished. It shows when the time-delay is considered in full DGs penetration case, the results still have a larger fluctuation during the iterations comparing to other strategies. However, the fluctuation range is relatively smaller than the partial DGs penetration case, s-ince the number of affected DGs in the full DGs penetration case (only affect 10% of the DGs) is small compared to the number of affected DGs in the partial DGs penetration case (affect more than 10% of the DGs). Whereas, when the synchronous previous value strategy is applied, it is clear that the results dramatically reduce the fluctuation range compared to the results of skipping strategy in Fig. 4.13. Compared with the result in no-delay case, both synchronous skipping and previous value strategies have a better convergence result after 200 iterations. Consequently, the proposed previous value strategy could only improved the fluctuation performance, but cannot speed up the convergence rate.

When the synchronous AR strategy is considered to estimate the unreceived parameters, the result with improved fluctuation range has a better convergence speed compared to the result in synchronous skipping strategy. It is obvious that the proposed AR strategy is an effective way to reduce the fluctuation range and also improve the convergence result when the time-delay is considered in the ADMM algorithm. Then we also consider to modify the predictive values to reduce the estimation error to optimize the simulation results. The result with green line can be found in Fig. 4.13. The simulation results of weighted AR strategy show that the the added weighted term can slightly improve the convergence results from 0.11715 p.u. to 0.11708 p.u.. As it is, our simulation results in synchronous weighted AR strategy demonstrate that it is also an efficient strategy in the full DGs penetration case.

4.5.2.3 Performance of Asynchronous Algorithm

The asynchronous ADMM algorithm with full DGs penetration is discussed in this section. The time-delay tolerance is much larger than that in the synchronous algorithm. When time-delay is considered in this asynchronous algorithm, the simulation

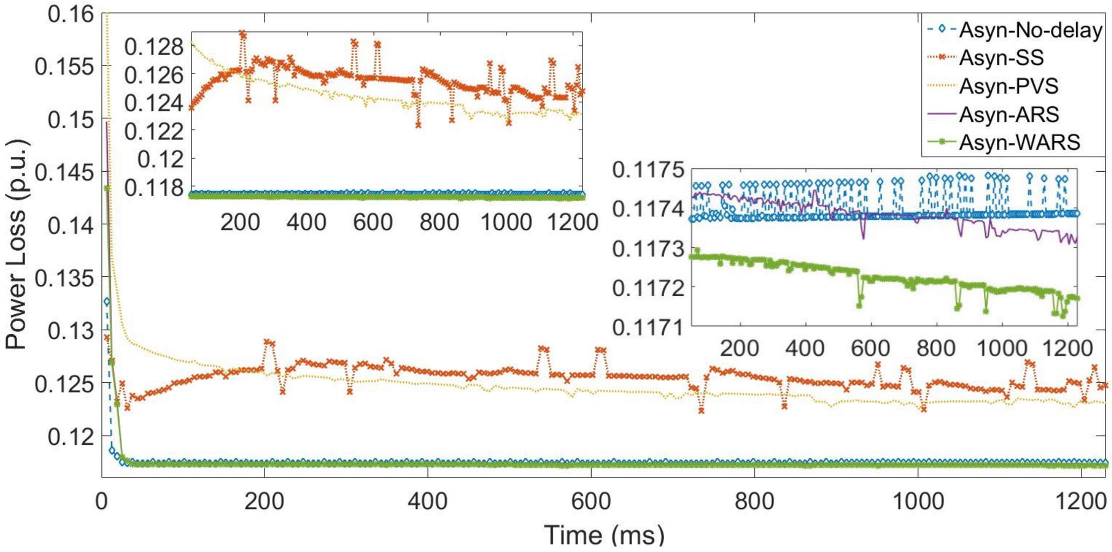


Figure 4.14: Comparison of convergence speed: Comparison of different asynchronous strategies.

results in Fig. 4.14 show that the skipping strategy can cause a larger fluctuation than the result in synchronous algorithm even if the time-delay probability is only 0.1%. It should be noted that the time-delay is more sensitive to the asynchronous algorithm than the synchronous algorithm. When the previous value strategy is adopted, the performance of fluctuation can be improved significantly. Whereas, the convergence result, which is 0.124 p.u., is still lager than the result in asynchronous no delay case. Hence, we propose to use the AR strategy to decrease the estimate error to improve the convergence result.

According to the simulation results in Fig 4.14, the convergence result under AR strategy can dramatically improved compared to the result of the skipping strategy. After 700ms, the simulation results will be better than the asynchronous algorithm without time-delay. The result of the experiment still has certain fluctuations, but it is too small to negligible. The result of asynchronous weighted AR strategy using the same time-delay probability scenario presents that the optimization result can be improved to 0.1171 p.u. which is better than any other strategies.

4.5.3 Performance of Loss Communication

The above simulation is based on the practical communication system which is low probability of communication delay. However, in case some nodes' communication devices are out of work, the normal convergence rate will have large fluctuation even if the probability of communication delay is low. The simulation results in Fig. 7 show the convergence results of different strategies both in synchronous and asynchronous algorithms. In this case, we assume that these nodes (node 15, 18, 23, 25) are out of work. Fig. 7(a) presents that the proposed WARS can effectively reduce the fluctuation of experimental results. In addition, the statistical results in Table II show that the mean value can be reduce to 0.1260 MW and the variance value is the smallest among the synchronous strategies. Comparing with the synchronous algorithm, the asynchronous algorithms can not only improve the mean value from 0.1260 MW to 0.1230 MW, but also demonstrate the lowest fluctuation of experimental results in Fig. 7(b) and Table II.

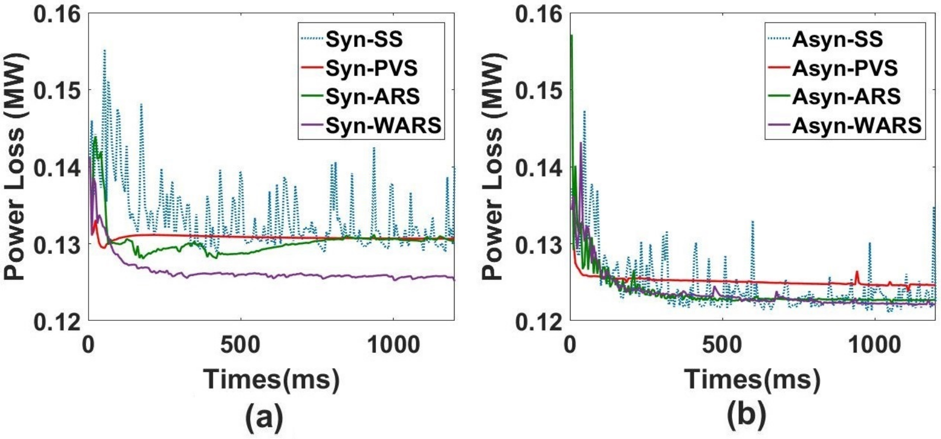


Figure 4.15: The convergence results for loss communication case.

4.5.4 Performance of 118-node System

We have expand an extra analysis in IEEE 118-node system. The results are based on the partial DGs penetration (25%). The proposed WARS can effectively improve the fluctuation in both synchronous and asynchronous algorithms and improve the convergence results. The simulation results are presented in Figure 4.16 and the

Table 4.3: Statistical results with 1000 runs for each strategies of loss communication case

	Mean	Variance
Syn-Skipping Strategy	0.1289	7.11E-6
Syn-Previous Value Strategy	0.1308	2.30E-5
Syn-AR Strategy	0.1299	1.53E-5
Syn-Weighted AR Strategy	0.1260	8.85E-6
Asyn-Skipping Strategy	0.1237	5.52E-6
Asyn-Previous Value Strategy	0.1250	1.02E-7
Asyn-AR Strategy	0.1231	5.16E-7
Asyn-Weighted AR Strategy	0.1230	6.62E-7

statistic results are listed in Table 4.4.

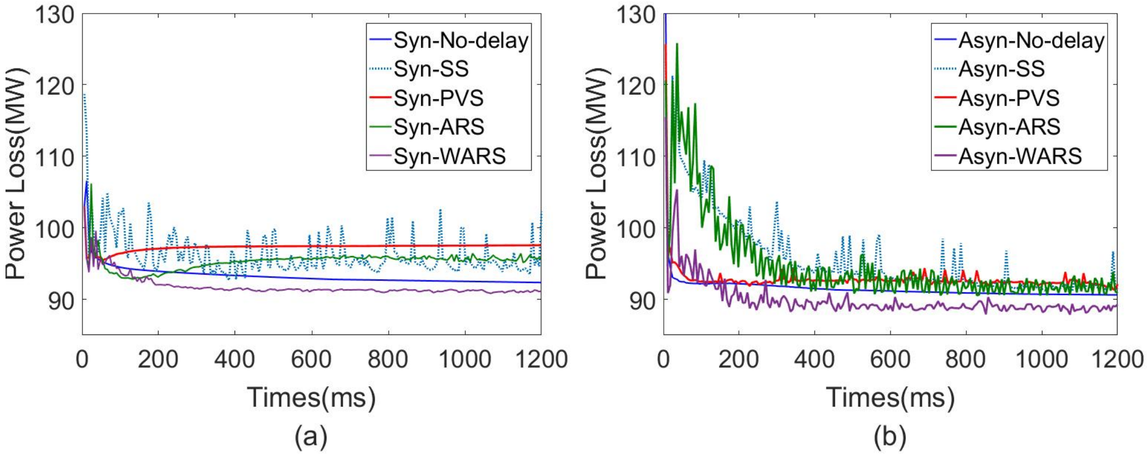


Figure 4.16: The convergence results for IEEE 118-node system.

4.6 Chapter Summary

The future power system will become more and more granular because of the increased penetration of renewable generators, distributed storage and electric vehicles. It is necessary to extend the current centralized operation and control strategies to be decentralized. In this chapter, the investigation considered communication delay model in reactive power OPF problem was studied. A parallel implementation of a fully decentralized ADMM algorithm has been adopted to solve the problem. Both synchronous and asynchronous algorithms combined with the communication model in partial DGs penetration case and full DGs penetration case are used to analyze

Table 4.4: Statistical results with 1000 runs of IEEE 118-node system

	Mean	**Variance**
Syn-Skipping Strategy	95.7956	4.5464
Syn-Previous Value Strategy	97.3927	0.0300
Syn-AR Strategy	95.2740	0.7273
Syn-Weighted AR Strategy	91.4291	0.2382
Asyn-Skipping Strategy	94.3714	11.8582
Asyn-Previous Value Strategy	92.5414	0.2140
Asyn-AR Strategy	93.2303	8.9628
Asyn-Weighted AR Strategy	89.2774	0.9600

the convergence results which have a large effect of the convergence rate compared with the no-delay algorithm. Extensive weighted AR strategy simulations showed that the fluctuation performance during the communication can be improved significantly in both algorithms. The optimization results also have been improved compared with the results of no-delay case for both synchronous and asynchronous algorithms.

Summing up the results, the convergence speed is largely dependent on the suitable value of the penalty factor and the tolerance. When time-delay is applied into the decentralized ADMM algorithm, the convergence performance would be significantly affected with a dramatical fluctuation. The proposed weighted AR strategy can largely reduce the fluctuation of the results in algorithm, and can also effectively improve the fluctuation in both algorithms although the unpredictability happened in both synchronous and asynchronous algorithms in DGs penetration case. Furthermore, both algorithms with weighted AR strategy can improve the iterative steps to achieve a better optimization result for no-delay cases.

It should be noted that this chapter is a first step to developing the communication model into the decentralized problem for power system and further research is necessary. Developing a more accurate communication, proposing novel and more effective strategy in asynchronous strategy in different DGs penetration case and investigating the cyber-attack would be very meaningful for future work.

Chapter 5

Cyber-attack in Voltage Control and ADMM Algorithm

5.1 Introduction

In the previous century, electrical power systems have evolved into the largest Cyber-physical (CP) network because of the emerging smart grid which integrates the power and energy systems with information and communication systems. In chapter 4, the optimization results can be obtained by a bi-direction communication link between neighbouring nodes. The secure and reliable communication through iterative algorithm is critical for stablility and economic target in smart grid. Therefore, the main purpose of this chapter is not only to analyze the effect of CP attack on the algorithm, but also to take certain defensive measures against CP attack.

Traditionally, the fundamental state estimation is a core function that processes the raw measurements of system topology and obtains accurate estimation of the state variables dynamically in power systems. In this chapter, we focus on the Time Delay (TD) attack and false data injection (FDI) attack scenarios which are based on the neighbouring nodes' information exchange without control center. The traditional state estimation model cannot be used to analyze the CP attacks through monitoring the measurement variations and state changes. We thus introduce a novel neighbouring monitoring scheme to detect the TD and FDI attacks. The scheme can detect the attacks by monitoring the exchange information of neighbouring nodes. There are two main contributions in this chapter:

1 We analyse two potential attack models, TD attack model and FDI attack model, in a fully decentralized OPF algorithm based-on the ADMM method. Both two attacks are discussed from the adversaries' perspective and we provides possible malicious attacks to simulate the final power dispatch results. The effects of both attacks are analyzed in this chapter. Since the attacks are not based on state estimation outcome by the control center, the information exchange will only be described between neighbouring nodes in this scenario.

2 The goal of the attack is to maximize system power loss and as a result the normal OPF algorithm with time-delay consideration will not take actions to alert the attacks. This chapter proposes a neighbouring estimate scheme to identify the misbehaving messages by using the local information to minimize the potential disruptions and damages. The weighted autoregressive (AR) strategy is utilized to mitigate the effects of attacks on the performance of the optimal results.

The rest of this chapter is organized as follows. Section 5.2 introduces the CP attacks model for the distributed OPF algorithm. The proposed defence mechanisms for detection of attacks are discussed in section 5.3. Section 5.4 demonstrates the effectiveness of the proposed method through simulations. Finally, the conclusions are provided in section 5.5.

5.2 Analysis of Cyber-attack Model in Smart Grid

In this section, we will demonstrate how the information exchange between neighbouring nodes could affect the final results of system power loss. In the previous research in chapter 4, we proposed an ADMM algorithm based on information exchange between neighbouring nodes and the stochastic end-to-end communication time-delay model is also applied to solve optimal power flow problems. The detailed information exchange mechanisms between neighbouring nodes can be found in section 4.3.2.2. All the information exchange is based on the proposed ADMM recursive algorithm in section 4.3.1. According to the simulation results in chapter 4, the optimization result is sensitive to the message delay or loss. As a consequence, a malicious cyber attacker can take advantage of vulnerabilities to compromise the distributed iterative algorithm. Two types of attack models, TD attack model and FDI attack model, are then defined.

5.2.1 Time-delay (TD) Attack Model

The distributed OPF algorithm, based on the ADMM recursive algorithm, only works under the assumption that all the nodes will only exchange the local information between neighbouring nodes. The wide-area wireless communication network can offer widespread access, moderate flexibility, wide coverage and low investment [62]. According to the previous work, it is clear that the time-delay or packet loss can often occur during the communication between neighbouring nodes. Under different environmental conditions, the wide-area wireless communication will have different degrees of delay or packet loss. Therefore, the attacker can take advantage of the stochastic probabilities of delay to induce the instability of optimization results in the transmission system. It is reasonable to model a type of attack by injecting time-delay during data transmission coming from telemeters measurements. The injected time-delay can be added into different parts of a control network, e.g., the feedback line, the referenced signal and the control signal. Here the time-delay attack in the wireless communication link is discussed during the distributed optimization power flow process. A simple cyber attack model can be seen in Fig 5.1. The attacker can attack the node by resending the control command after brief delay or directly modifying the control command to affect the normal operation of the algorithm. There are two time-delay attack models that will be discussed as follows.

Resend Time-delay (RTD) attack. TS and TS' donate the time stamping for backward link and forward link communication, respectively. First of all, the attacker will record the first message $\overline{Q}_i(1)$ from the sender and send the message to the receiver. Then the attacker will record and drop the second message $\overline{Q}_i(2)$ from

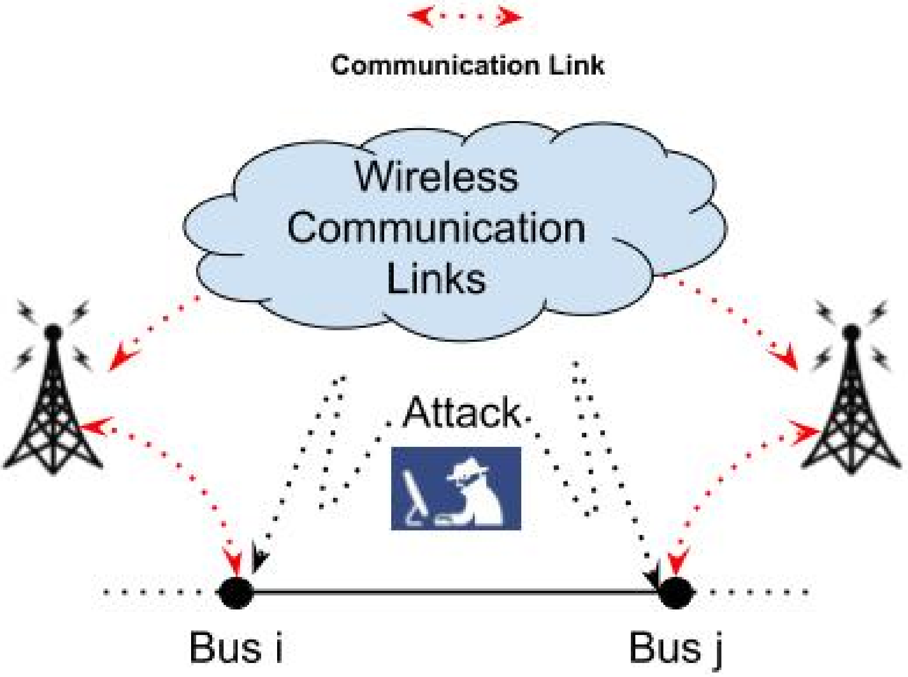


Figure 5.1: A simple cyber attack model between neighbouring nodes.

the sender. Subsequently, the attacker will send the first recorded message $\overline{Q}_i(1)$ to the neighbouring node instead of the second received message $\overline{Q}_i(2)$ from the sender. Furthermore, the attacker will send the second recorded message $\overline{Q}_i(2)$ to the receiver twice instead of the third message $\overline{Q}_i(3)$ and the fourth $\overline{Q}_i(4)$. Each message will be recorded and sent twice for the purpose of time-delay. The attacker can generalize the delay by sending one message twice within a certain delay (Normally in two iteration periods). Detailed steps of RTD attack can be found in Table 5.1. In the table, $Comm_{ji}$ means the backward link from bus j to bus i, and $Comm_{ij}$ means the forward link from bus i to bus j. This attack does not need to modify the packet before sending the message as it can be easily detected by the receiver. Next we will discuss a RTD attack mode based on the time stamping.

Time Stamping RTD attack. When the time stamping is not modified during the attack process, the resend packet can be easily detected by the time stamping detector. Hence, the adversary need to reconstruct the packet and fix the time stamping issue. If the adversary can decrypt the packet and reconstruct it with the wrong information, then the time stamping issue in the RTD attack model can

Table 5.1: The Scenario of The Resend TD Attack

Iteration	$Comm_{ij}$	$Comm_{ji}$
1	$\overline{Q}_i(1), TS_1$	$Q_j(1), TS_1^{'}$
2	$\overline{Q}_i(1), TS_1$	$Q_j(1), TS_1^{'}$
3	$\overline{Q}_i(2), TS_2$	$Q_j(2), TS_2^{'}$
4	$\overline{Q}_i(2), TS_2$	$Q_j(2), TS_2^{'}$
5	$\overline{Q}_i(3), TS_3$	$Q_j(3), TS_3^{'}$
$\vdots$	$\vdots$	$\vdots$

be fixed. In this way, the time stamping detector cannot detect the time-delay attack any more and the information will normally be accepted by the receiver. The attacker can receive the first message from the neighbouring node and copy the information in the buffer. Then, it can replace the information of the second message with the information of the first message and reconstruct the packet to send to neighbouring node. Then the controller will utilize the incorrect information to optimize the results. The subsequent message for each iteration will modify the time stamping issue in the same manner. Details about the steps of time stamping RTD attack can be found in Table 5.2, where the time stamping issue can be fixed with normal time stamping in each communication.

Table 5.2: The Scenario of The time stamping RTD Attack

Iteration	$Comm_{ij}$	$Comm_{ji}$
1	$\overline{Q}_i(1), TS_1$	$Q_j(1), TS_1^{'}$
2	$\overline{Q}_i(1), TS_2$	$Q_j(1), TS_2^{'}$
3	$\overline{Q}_i(2), TS_3$	$Q_j(2), TS_3^{'}$
4	$\overline{Q}_i(2), TS_4$	$Q_j(2), TS_4^{'}$
5	$\overline{Q}_i(3), TS_5$	$Q_j(3), TS_5^{'}$
$\vdots$	$\vdots$	$\vdots$

5.2.2 False Data Injection (FDI) Attack Model

As shown in Fig. 5.1, an attacker may launch a false data injection attack by hacking a few sensors to distort the exchange information or alter the correct information during the transmission in the wireless communication links.

In our previous study in chapter 4, all buses need to share the correct iterative information with neighbouring nodes in distributed OPF algorithm. During the iterative process, each node needs to know the updated variables of neighbouring nodes to optimize the allocation of reactive power. However, the attacker may exploit the vulnerability of the communication link and manipulate to send the incorrect information to affect the final power loss result. The attack method of the FDI attack at kth iteration is summarized in Table 5.3. It is assumed that the false data injection only occurs during the backward communication links in each iteration.

According to Table 5.3, it is obvious when the information during the backward communication link is manipulated, all the data updates based on the incorrect information will be incorrect. During the FDI attack, when the power balance is not fulfilled, the distributed generator will inject/absorb the reactive power to balance the power flow. As a consequence, the local distributed generator will be utilized to change the normal reactive power flow due to the false control information sent from the attacker. In this way, bus i will alter the optimal power flow and affect the final result of system power loss.

This attack could be exploited for an economic and stable issue in a distributed network. For example, a malicious attacker can manipulate the information and send to distributed generators which will increase or reduce the local reactive power output by controlling the electronic converter. In addition, this change will affect the stability of the voltage level directly, deviate from optimality, and break down in most cases.

Note: The colluding attack is not considered in this chapter. We assume that the adversary will only attack isolated buses without any two neighbouring buses being attacked at the same time. In addition, if the change amount of original data is too large, this attack could be detected by the system operator with a high probability because the system operator can detect the attack easily. Each bus usually has a

Table 5.3: The Strategy of FDI Attack in Distributed OPF Algorithm

Normal Operation	FDI Attacks
1. Bus i minimizes the equation (4.11) to update the local variables and sends the updated variable $\overline{Q}_i(k+1)$ to backward bus $i-1$. Meanwhile, it will receive the updated local variables from neighbouring bus j.	1. The updated reactive power variable $\overline{Q}_i(k+1)$ will be manipulated to be a false data: $\overline{Q}_i^f(k+1) = \overline{Q}_i(k+1) + \delta_{err}$. Then the false data $\overline{Q}_i^f(k+1)$ will be sent to bus $i-1$. In addition, bus i will receive the malicious data $\overline{Q}_j^f(k+1)$ from bus j.
2. After receiving the information from neighbour bus j, bus i update the global reactive power variable $Q_i(k+1)$ by equation (4.12) and then sent the updated $Q_i(k+1)$ to bus j. Subsequently, the Lagrange multipliers $y_i(k{+}1), y_i^+(k{+}1)$ will be updated by rules (4.13).	2. When the malicious data is received, the controller will utilize the false data $\overline{Q}_i^f(k+1)$ to update the global reactive power $Q_i^f(k+1)$ by equation (4.12) and send it to forward bus j. At the same time, the Lagrange multiplier $y_i(k+1)$ will be obtained by utilizing the modified global reactive power $Q_{i-1}^f(k)$ which is from the bus $i-1$.
3. According to the received updated global reactive power variables, bus i then will repeat the same steps for $k+1$th iteration to obtain the new local variables by (4.11).	3. Bus i will update the new local variables based on the updated incorrect data $Q_{i-1}^f(k+1)$ sending from backward bus $i-1$. It is clearly that the entire iterative process of node i will always be in the wrong calculation and affect the calculation of next iteration.

relative small amount of change in an iterative process compared to the previous iterative process.

5.3 Detection of Cyber-attack Model in Smart Grid

According to the above analysis, both TD attack and FDI attack could affect the final results of power loss. Without any countermeasures, the power system will be put into contingency condition or even worse. Therefore, any further modification of network or emergency condition could cause poor optimization results or even cascading failure. It is crucially important to have appropriate countermeasures to protect the system in advance or identify potential false data injection by observing the power system. Generic protection measures rely mainly on establishing a secured communication, protecting critical information and alleviating vulnerabilities against all possible cyber attacks. The bad data injection detection widely studied for centralized state estimation attack which is based on the entire system topology and dynamics to achieve estimation of the state variables at control center [78, 79]. However, the countermeasures for centralized CP attacks are not suitable for a decentralized cyber attack model in this chapter. The information exchange in this chapter only happens between neighbouring nodes and the state estimation function can not be applied. In this section, two kinds of countermeasures under local neighbouring nodes' information exchange are proposed to detect the TD attack and FDI attack, respectively.

5.3.1 Detection of TD attack

In this section, an effective defence mechanism scheme for the detection of TD attack is presented, which can be divided into three steps: protection, detection and mitigation. The details of generic defence strategy can be found as follows.

1. **Deployment of Phasor Measurement Units (PMUs)**: This is the protection stage to help against the cyber attacks in advance. A number of specific

protections can be utilized to reduce or even erase some certain cyber attacks. The deployment of secured or encrypted advanced measurement units, such as known-secure PMUs [129], is one of the secure ways to protect the optimization system from so as to be immune to the cyber attacks. Secured wireless network has provided trustworthy communication for the PMU and advanced metering infrastructure system. The known-secure PMUs can directly measure the variables of bus to verify the value of neighbouring nodes independently. However, the PMUs are too expensive to install them at all buses to protect the information in the network. The requirement of PMUs installation at all buses may not be able to implement, and it may be relaxed by installing at a few important buses, such as the DG buses in Fig. 3.9. The identification of important locations is left to be handled with in a future work.

2. **Real-Time Detecting Method**: Despite the effort of protection, the adversary may still have the ability to attack protected component by utilizing the vulnerability of the communication link. In case of this, a simple effective method is proposed to address a TD attack. Although the attacker can modify the time stamping of the packet, the encrypted information usually increases the challenge to decrypt the packet and increase the normal time of a complete communication process. This method uses a time-delay estimation (TDE) scheme, which contains a time-delay estimator and optimal controller, to alert the received bus for a TD attack if a long time delay communication is detected. In the meantime, the estimator has a buffer to store the history of controller commands and transmission time for each message which could help to estimate the time-delay in the communication channel for current information exchange. If the delay time is always over an acceptable time delay for three iterations (not too large comparing with normal communication time), it will send alarm signal to the bus controller and system operator. We set τ_n as the normal communication time and τ_a as the acceptable maximum time. If delay time is larger than τ_a and less than $\frac{5}{4}\tau_a$, the estimator give three chances to return to normal communication time. If the delay time is larger than $\frac{5}{4}\tau_a$, the estimator will report to system operator directly. Then the controller

will stop receiving the information from neighbouring nodes until the warning signal is released. Furthermore, the time-delay estimator will active the optimal controller to stabilize the iterative process. Moreover, the proposed time-delay estimator can also examine time stamping of the transmission message to determine if the control command has been maliciously modified or not.

3. **Mitigation of the cyber-attack**: When the attack is confirmed, it is necessary to mitigate the effects by the system operator to minimize the potential disruptions and damages. If the TD attack has been cleared from the communication system immediately, the restoration mechanisms can effectively resume the information exchange during the optimization process. However, if the TD attack has not been resolved in time, the bus operator needs to consider other appropriate countermeasures to prevent the malicious attack in the system. In this scenario, an optimal controller is proposed during the attack. When time-delay signal is received by the time-delay estimator during the information exchange process, the optimal controller can utilize the stored historical information received in the past to forecast a new value instead of the current manipulated message. The predictive value not only can stabilize the iterative process, but also accelerate the convergence rate to obtain a fast optimization result.

5.3.2 Detection of FDI attack

Different from the reduction of optimization speed during the TD attack, the FDI attack may change the entire power flow calculation and make the optimization results unstable or even lead to failure. In this section, an adaptive neighbouring monitoring strategy is proposed to detect and prevent false data injection. This strategy is inspired by the watchdog design in the security protocol for wireless Ad-Hoc networks [130]. It helps the iterative algorithm find a reliable way of detecting misbehavior information exchange and attempts to reduce the harm caused by FDI attack.

The proposed neighbouring monitoring strategy adds a reputation system against the misbehavior information exchange and takes advantage of the neighbouring local information to find out the dishonest nodes. Fig. 5.2 illustrates the framework of the proposed strategy box which contains three components: Monitoring Unit, Verification Unit and Protection Unit.

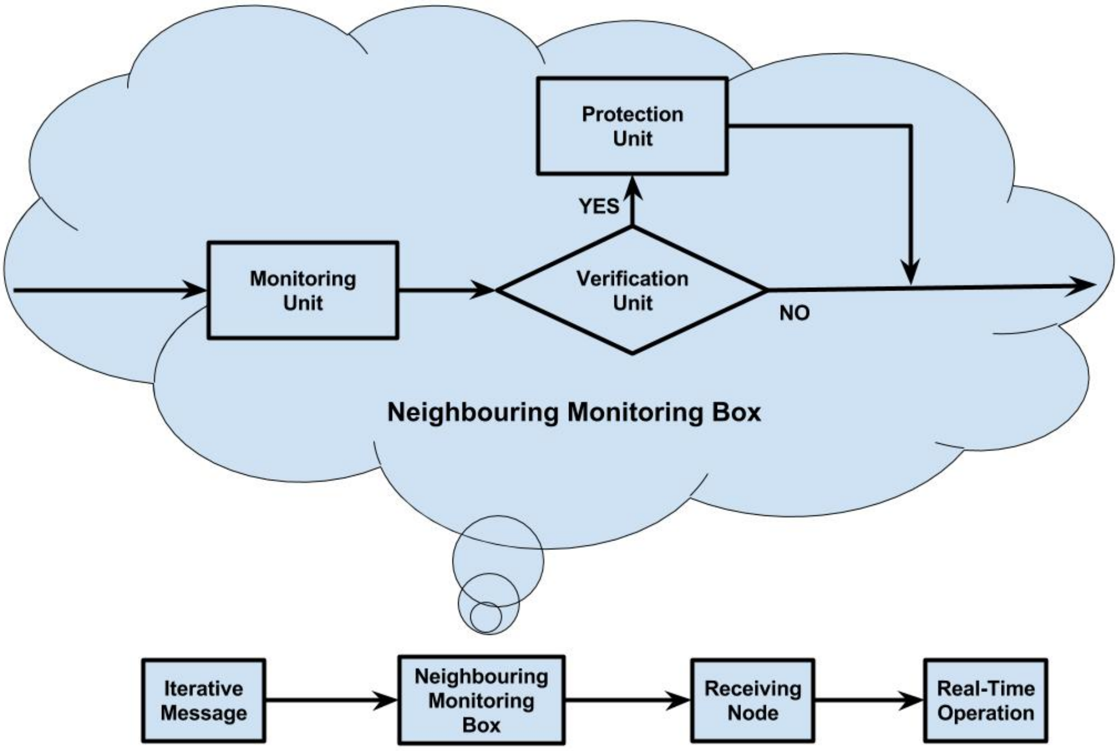


Figure 5.2: The diagram of the proposed neighbouring monitoring strategy.

Monitoring Unit

The monitoring unit holds the responsibility of receiving and monitoring the exchange information from neighbouring nodes. The time-delay estimator is also located in the monitoring unit. First of all, this unit will check the time stamping and estimate the communication time to detect the time-delay attack model. Second, this unit will receive all information from other nodes and use all saved historical data to predict the value of current received variables. The predictive value is based on the autoregressive (AR) model and a weighted coefficient is added to reduce the impact of predictive error. The detailed AR model can be found in subsection 4.4.3. The predictive value can be obtain by expression (4.32) in terms of the historical data. Then it will send the predictive value together with the received message to verification unit to detect if the received message is false data or not.

Verification Unit

The verification unit holds the responsibility of verifying the authenticity of the message. When a false information injection is confirmed, the control command will be transferred to activate the protection unit and a warning signal will be sent to the DG node to notify that a misbehavior of neighbouring node is detected. In wireless ad hoc networks, a detection and prevention of cyber attack is important. In order to surmount this issue, the verification unit will utilize a reputation rating mechanism to analyze the authenticity of the message.

Protection Unit

The protection unit holds the responsibility of utilizing the modified control instruction to mitigate the potential disruption or damage. When the protection unit is activated by the verification unit, it will utilize the forecast value to continue the iteration process instead of the manipulated variable by the attacker. The predictive value can effectively reduce the impact of the cyber attack on the iterative algorithm. Then the protection unit will terminate the false information communication and report the FDI attack to the system operator. After the FDI attack is released, the protection unit will be closed and wait to be activated again.

Notation for Mechanism I

- Ω is the total number of iterations.
- $\overline{Q}_i(k+1)$ is the normal received value from neighbouring bus.
- $\overline{Q}_i^{err}(k+1)$ is the predictive value for current receiving message by the evaluation function.
- $Rep_i(k+1)$ is the reputation index of node i for $k+1$th iteration.

- $rec_i(k)$ is the reputation count of node i for kth iteration.

- $\varepsilon_i(k)$ is the proper deviation threshold value of node i at kth iteration which is less than 1.

- $\varepsilon_i^{'}$ is the extra deviation threshold value of node i at kth iteration due to the error caused by the forecast.

- $err_i(k)$ is the error function estimating by the current received value and forecast value.

- $Rep_i^{ref}(k)$ is the reference reputation for each node i at kth iteration.

The reputation rating mechanism means that each bus will have its own local reputation value generated after each iteration. If the reputation value of node i belongs to the reference reputation index, then the exchange information will be considered as a trustworthy message. Otherwise, the exchange information will be treated as a false message. The details of the neighbouring monitoring strategy is presented in Table 5.4.

We initialize local deviation error index from the historical data. Then in order to identify whether the information from neighbouring node has been manipulated, the message of FDI attack from neighbouring nodes will be detected by calculating the deviation between the current data and forecast data. The reputation rating mechanism was introduced in step 3 which is based on the reputation index. When the reputation value $Rep_i(k)$ is smaller than the defined threshold value $Rep_i^{ref}(k)$ (we set as $k-1$), the system will determine the current information as a false information. The effective deviation error is updated based on the analysis of a set of historical data that a machine learning technique can utilize the historical data to update the proper range. However, part of the information exchange between neighbouring nodes may have various misbehavior results due to different reasons like transient link failure, larger prediction error by the predictor etc. The proposed trust range mechanism in Fig. 5.3 is utilized to give these buses a fair chance. As can be seen from step 3 and Fig. 5.3, if the deviation error is in the proper range, the reputation count $rec_i(k)$ will be set as 1; if the deviation error is in the trust range, the reputation count $rec_i(k)$ will be set as $\frac{2}{3}$ which means that the proposed trust

Table 5.4: Mechanism I: Reputation Rating Mechanism

Initialize: Each node i updates its own deviation error index through the saved historical local data
Start each iteration k: where $k \in \Omega$,

1. Each bus i communicates the updated variable $\overline{Q}_i(k+1)$ to the backward neighbouring bus.

2. After receiving the message from neighbouring bus, the neighbouring monitoring box of bus i will monitor and verify the authenticity of the information by estimating the message $\overline{Q}_i^{err}(k+1)$ from neighbouring bus $i-1$ using the evaluation function (4.32).

3. Then the verification unit will calculate the deviation error to check the reputation value $Rep_i(k)$ of bus i as follows:

$$Rep_i(k) = \frac{\sum\limits_{k=1}^{k} rec_i(k)}{k}. \tag{5.1}$$

   where $rec_i(k)$ can be written as

$$rec_i(k) = \begin{cases} 1, & if \quad err_i(k) \leq |\varepsilon_i(k)| \\ \frac{2}{3}, & if \;\; |\varepsilon_i(k)| < err_i(k) \leq |\varepsilon_i^{'}(k)| \\ 0, & if \quad err_i(k) > |\varepsilon_i^{'}(k)| \end{cases} \tag{5.2}$$

   where $err_i(k) = |\overline{Q}_i^{err}(k) - \overline{Q}_i(k)|$.

4. The introduced reputation value is controlled by the proper deviation threshold $\varepsilon_i(k)$ and extra deviation threshold $\varepsilon_i^{'}(k)$. When the calculated error is in different set ranges, the value of reputation count will be marked as 1 in the proper range, $\frac{2}{3}$ in the trust range, or 0 out of the trust range.

5. If $Rep_i(k)$ is less than the defined threshold value $Rep_i^{ref}(k)$, the verification unit will send the alarm signal to the receiving node and activate the protection unit to modify the control instruction instead of using the false information at the same time. Otherwise, the verification unit will inform the receiving node to continue using the received information from neighbouring nodes to perform the iterative algorithm.

6. When the protection unit is activated, the iteration variable will be replaced by the predicted value to continue the iterative calculation until the attack warning is released by the system operator.
7. If the attack warning is released, the protection unit will be closed and the current reputation value will also be reset to current reference reputation value $Rep_i^{ref}(k)$.
8. Repeat k=k+1 until satisfied the defined minimum error.

range mechanism gives the misbehavior nodes three opportunities to compensate for the large deviation due to the predicted error; if the deviation error is out of the trust range, the reputation count $rec_i(k)$ will be set as 0. Note that each bus may have a different reference deviation threshold value $\varepsilon_i(k)$ and extra deviation threshold $\varepsilon_i^{'}(k)$ due to the different stages of iterations. After a certain period of iterative process, the reputation count of misbehavior will be improved by the verification unit automatically to remove from the misbehavior list if the reputation value $Rep_i(k)$ is still larger than the defined threshold value $Rep_i^{ref}(k)$. Then the algorithm will have an additional three chances in case of new large deviation errors. Next, when the information is confirmed as a false information, the protection unit will use the predicted value instead of the false information and notify the system operator. The predicted value will always be adopted until the cyber-attack is released by the system operator. It is crucial for system operator to know that the predicted value can mitigate the efforts of attacks immediately on the procedure of iteration when the cyber-attack is detected.

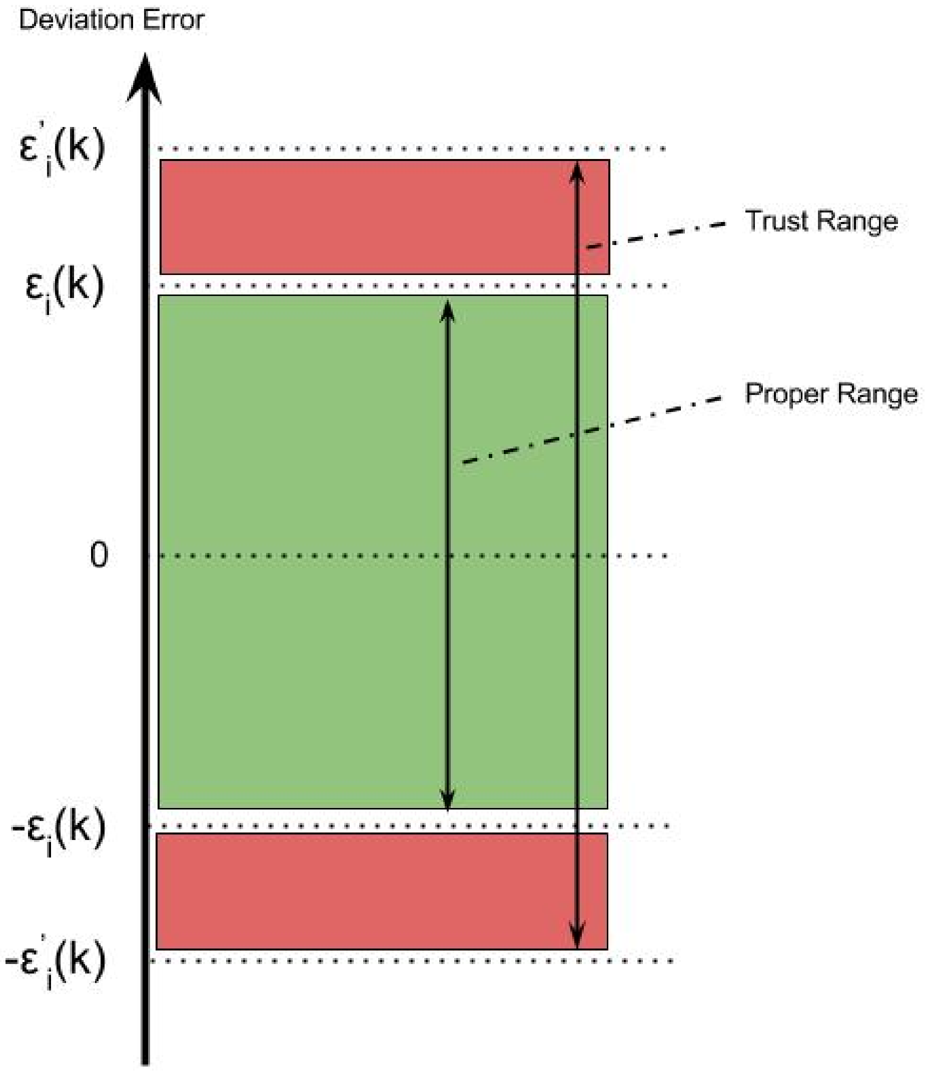


Figure 5.3: The operating condition of proper deviation range.

5.4 Case Study Results

In this section, we demonstrate the performance of proposed OPF algorithm against the cyber-attack. The 33-bus system with DGs in Fig. 3.9 will be applied and it is based on the configuration of the Future Renewable Electric Energy Delivery and Management (FREEDM) system [131]. The FREEDM system is a prototype of the smart grid, and there is an open-standard-based operating system called Distributed Grid Intelligence (DGI). The DGI is installed across all of the buses and can utilize the communication network to exchange information with neighbouring nodes. The Matpower/Matlab is utilized to simulate the performance of the algorithm in power system.

5.4.1 Results with TD Cyber-attack

Fig. 5.4 shows the normal iterative reactive power injection of one node compared with the predicted reactive power injection. It is demonstrated that the predicted value is very close to the normal iterative value to protect the packet loss or time-delay. In the early stages from 2 to 12 iterations, the predictive deviation is large which can be seen in the enlarged picture of Fig. 5.4. Then in the later iterations, the deviation between the predicted value and real value almost can be negligible. For brevity, we only present the comparison result for one special node 18, but the experimental results are also applicable to all other nodes. All the predicted values are close to the real values. Therefore, the proposed predicted parameter is very valuable to practical real-time optimal power flow calculation in such a smart grid.

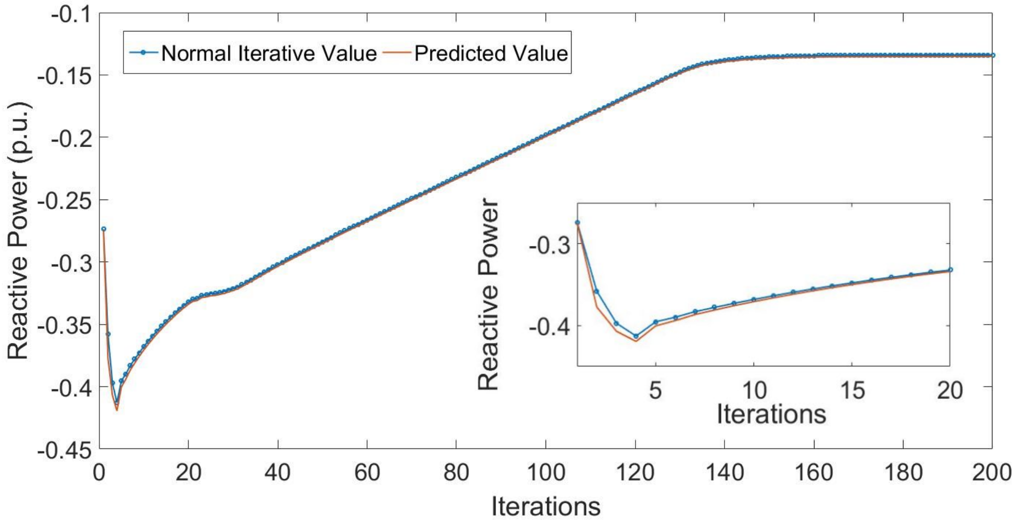


Figure 5.4: The comparison between the predicted value and real value for one node.

As for the TD cyber-attack case, the simulation result of partial nodes in TD attack case (nodes 2, 12, 15, 18, 23, 25, 27 and 33) can be found in Fig. 5.5. Assume that a TD attack only occurs in the first 100 ms. Without any defence countermeasures, when the TD cyber-attack happens, the simulation result presents that the convergence result has a large fluctuation in the early stage of iterations (42.3% variation). Although the convergence results do not fluctuate greatly in the later stage of iterations, the final experimental result still has a certain deviation error compared with the normal optimal result. Although the TD attack will not result in non-convergence of the optimal result, it reduces the convergence rate of the algorithm and needs more time to achieve the same convergence goal of the system power loss. If the TD attack can be detected, the predictive value can be used to replace the original modified message and mitigate the effects of TD attack and increase the convergence speed to minimize the potential disruptions. On the contrary, the result of weighted AR-based TD attack in Fig. 5.5 demonstrates the improvements of the iterative results when the proposed predictive value is used during the TD cyber-attack. The result presents that the iterative result can be improved dramatically and is close to the result in normal case without delay. Although the experimental result also has a certain fluctuation due to the prediction error, the fluctuation can be negligible compared with the fluctuation in the TD cyber-attack case. It can be anticipated that the proposed predictive value strategy is valuable in a practical iterative algorithm to mitigate the effects of the network TD cyber-attack.

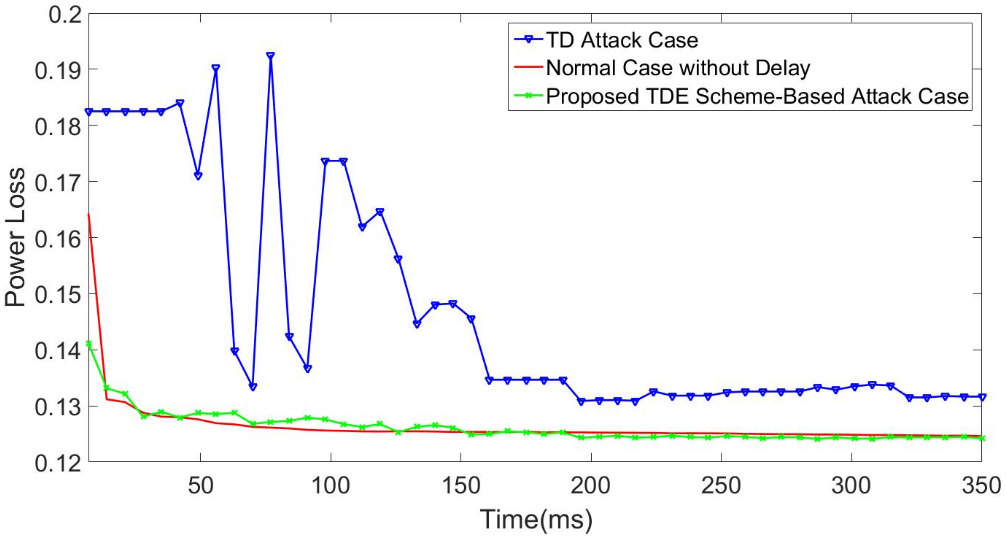


Figure 5.5: The comparison of iterative results among normal case, TD attack case and AR-based TD attack case.

5.4.2 Results with FDI Cyber-attack

The above simulation results are based on the TD cyber-attack. In this section, the results under FDI cyber attack model will be discussed. This simulation result considers the time-delay and will apply the weighted AR iterative algorithm during the iterative process as described in subsection 4.4.4. Compared with the TD cyber attack case, the FDI cyber attack case can send any control instruction to neighbouring node during the iterative process. If it could happen, the iterative results will not be able to converge completely. Fig. 5.6 shows the result under FDI cyber-attack between 100 to 120 iterations in a random attack scenario. When the attack happens without any defence countermeasures, the simulation result will be unable to converge completely. Fig. 5.6(a) shows that the result has a large fluctuation between 100-120 iterations, where the fluctuation range can even reach 8000. In the first 100 iterations, the experimental result can converge appropriately to 0.125 p.u. as shown in Fig. 5.6(b). When the FDI cyber-attack occurs without any defence countermeasures, the result shows a significant fluctuation during the attack in Fig. 5.6(c). If the result during the FDI attack is adopted, it will decrease the economic benefits and induce further and more intensive damages into the physical system. As can be seen from Fig. 5.6(d), although the attack is released after 120 iterations, the experimental result after 80 iterations still has a larger deviation error compared with the global optimal result.

When the proposed weighted AR-based neighbouring monitoring strategy is applied into the iterative algorithm, each node can check the authenticity of the received message by using the reputation rating mechanism. If the fake information is confirmed, the forecasting value will be used to execute the iterative algorithm. Fig. 5.7 presents the experimental result with the proposed AR-based neighbouring monitoring strategy after 100 iterations. It can be anticipated that the large fluctuation between 100 and 120 iteration has been improved dramatically compared with the results in Fig. 5.6(c). The results with weighted AR-based neighbouring monitoring strategy are very close to the iterative results of no-attack case, which means the proposed strategy shows a good performance in mitigating the impact by the FDI cyber attack.

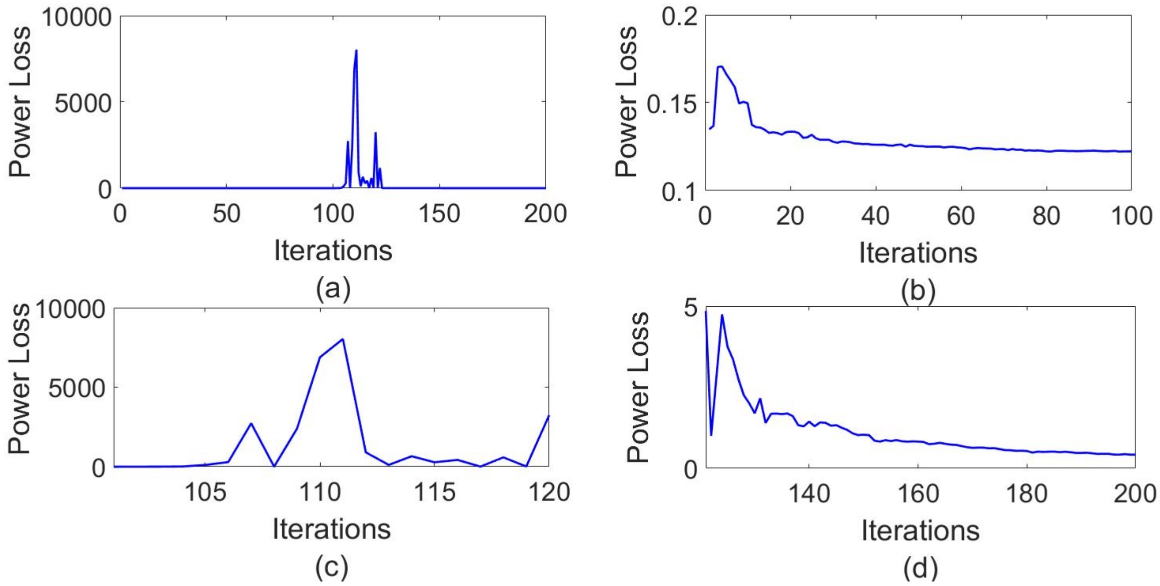


Figure 5.6: The iterative result under FDI cyber-attack between 100 to 120 iterations without any defence countermeasures. (a) is the entire results. (b), (c) and (d) are three separate parts of (a).

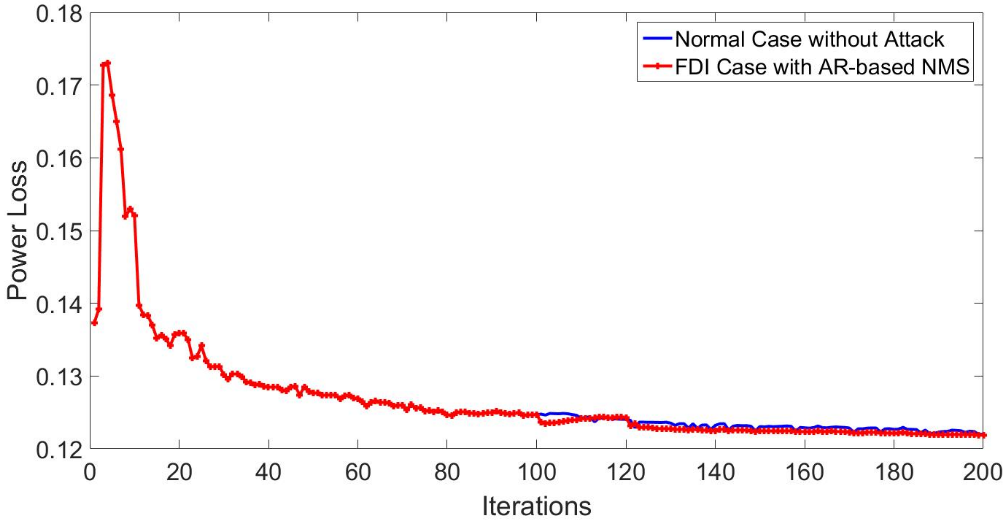


Figure 5.7: The comparison of iterative results between normal with no-attack case and AR-based neighbouring monitoring strategy with FDI attack case.

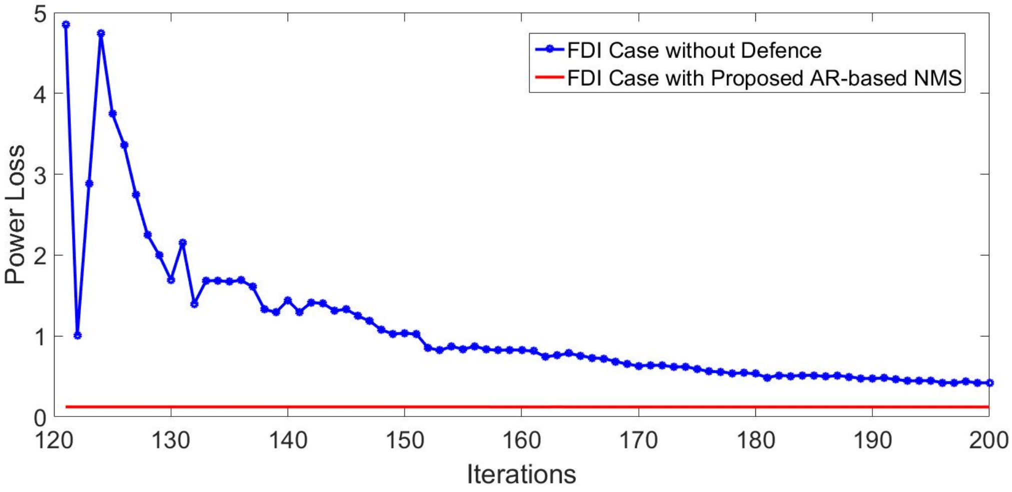


Figure 5.8: The comparison of iterative results between FDI case without attack and FDI case with AR-based neighbouring monitoring strategy after 120 iterations.

Comparing with the results in FDI cyber-attack case without defence, the performance of the proposed scheme after 120 iterations is shown in Fig. 5.8. Although the results in FDI case without defence are still convergent after 120 iteration, the final convergence result in 200 iteration has a large deviation error from the global optimal value, which is four times larger than the normal optimal result. As demonstrated in the Fig. 5.8, it can be anticipated that the proposed neighbouring monitoring strategy is able to mitigate the effect of the cyber-attack in OPF algorithm and obtain an improved convergence result.

5.5 Chapter Summary

In this chapter, we have discussed two potential cyber-attacks in distributed OPF algorithm. First, two cyber-attack models, time-delay attack model and false data injection attack model, are discussed during the OPF iterative procedure. Both two attacks can result in an increased power loss and the FDI attack can even lead to instability of the convergence result. Then two different detections are proposed to defend the TD attack and FDI attack. As for TD attack, the defence mechanism scheme, including protection, detection and mitigation, is proposed to detect the possible attack and mitigate the effect of the TD attack; as for FDI attack, an weighted AR-based neighbouring monitoring detection strategy with reputation mechanism is proposed to identify the misbehaving local information exchange to neighbouring nodes. The proposed strategy identifies the FDI attack by comparing the current received variables with the predicted value. The deviation error area can be set by relying on a set of historical data.

The simulation results have presented that the two proposed defance scheme is efficient can achieve improved convergence results during the cyber attacks. The time delay attack can only slow down the convergence speed, but the FDI delay attack may lead to a very large fluctuation in the convergence result. If the cyber attack is confirmed, system operators can use the predicted value to replace the manipulated information. By contrast, the simulation results indicate that the proposed mechanism can reduce the fluctuation of the results dramatically during 100 and 120 iterations and improve the final convergence results significantly. Future work will focus on considering other malicious scenarios, for example, neighbouring nodes collude with each other under multiple false data injection attack model.

Chapter 6

Discussion and Conclusions

In this chapter, we briefly summarize the performance evaluation of decentralized voltage control strategy combined with stochastic communication time-delay as well as the improved ADMM-based optimization algorithm in decentralized OPF model. In addition, the cyber-physical analysis is simulated to evaluate the performance of the efficiency on defensive strategy. In this concluding chapter, a brief summary of the key contributions from different chapters will be given in Section 6.1. Some limitations of work are discussed in Section 6.2. Several future directions of the research issues from current power system challenges are presented in Section 6.3.

6.1 General Conclusion of Different Chapters

Due to the increasing penetration of DGs, the reactive power allocation of DG is emerging to control system voltage level. In chapter 3, a decentralized voltage control method combined with time-delay model is proposed to analyze the performance of the control strategy. Compared with the independent control method, the coordinated control method can both effectively regulate the voltage level of each bus and improve the power factor of each node to enlarge the total reactive power capability. The maximum reactive power output could decrease from 0.45 p.u. to 0.34 p.u. which could drastically reduce the possibility of active power curtailment occurrence even if the total network loads have a higher demand than usual. This control strategy can effectively increase the range of voltage fluctuations that can be controlled. Despite the limitation of communication technology, the simulation results have shown that small time-delay still can affect the performance of decentralized voltage control method in real-time. Although the upcoming 5G can be an improved technology with less communication transmission delays, the impact on the decentralized control system with information exchange cannot be ignored. In the case of packet losses, such control strategy cannot even work properly without any control instructions. Therefore, it is necessary to analyze the impact of delay and propose an effective method to resolve this issue.

Chapter 4 presents a decentralized optimization algorithm, called ADMM algorithm, to minimize system power loss. One of the key advantages of the ADMM is that a fully centralized objective can be solved in a decentralized way that each local function can be handled by its own local parameters and processor. It can rewrite the objective function with local objectives by local variables. Each of these local objective function contains a selected variables of the global variables. In addition, the stochastic communication delay model is applied into the ADMM algorithm which can simulate the performance on the algorithm with time-delay consideration. In this chapter, both synchronous and asynchronous distributed ADMM algorithms are proposed to assess the convergence rate of the algorithm. In order to mitigate the impact of the time-delay, we assess four different strategies, skipping strategy (SS), previous value strategy (PVS), autoregressive (AR) strategy (ARS) and weighted AR strategy (WARS). The performance of WARS has been investigated and verified by simulation results. It has been demonstrated that the proposed WARS in both synchronous and asynchronous algorithm can achieve a better convergence results compared with other strategies when the stochastic time-delay occurs. If the probabilities of time-delay increase or communication devices of nodes are out of work, the convergence results will have great fluctuations. Therefore, the proposed ADMM algorithm is meaningful for decentralized algorithm in distributed power system with large penetration of DGs.

In order to analyze the effect of CP attack and reduce the threat from adversary, two attack models, time delay attack and false data injection attack, based on local information exchange are discussed in detail. Both attack models demonstrate how the malicious cyber attacks actually progress during the communication. In order to detect the attacks and reduce the impact of objective function, two countermeasures are proposed to detect the TD attack and FDI attack, respectively. For TD attack, a defence mechanism based on three steps is presented to protect, detect and mitigate the TD attack. For FDI attack, an AR-based neighbouring monitoring scheme is proposed to monitor and verify the information from other nodes. A predicted value is used to calculate the deviation error from the reputation index. Trust range mechanism is proposed in case of a major estimation error. According to the simulation results, when CP attack models are applied in the algorithm, simulation results demonstrate that attack can reduce the convergence rate or even fail to converge. However, the proposed countermeasures can improve the results strikingly. Moreover, the results with proposed AR-based NMS can be better than the results without attack.

6.1.1 Limitation of Work

In the reactive power control strategy to the voltage control problem, it should be noted that the coordinated control method only deals with the case of partial nodes. The application of whole nodes was not discussed in chapter 3. Meanwhile, the control strategy improved the power factor to maximize the capability of reactive power output but did not consider the optimization of reactive power allocation. Under the time-delay case, the reactive power control strategy did not perform well to mitigate the impact of time-delay. It is necessary to propose an appropriate way to reduce the possibility of a sudden voltage increase or decrease in voltage level. To further exploit the impact of time-delay, the combination of independent strategy and coordinated control strategy can be used as an effective way to mitigate the sudden fluctuation of voltage level. In addition, the time-delay model based on 3G technology is not perfect for delay analysis. The more specific delay time, such as decision-making delay, should be considered for power system optimization. The decision-making time-delay will become dominant while the new 5G technology can reduce the communication time-delay dramatically in the future smart grid communication.

In our existing work on the OPF problem, the adopted ADMM-based decentralized OPF algorithm can reduce the impact of time-delay on the convergence performance. The objective function is based on the improved linear quadratic function. However, in practice, it has certain limitations in the real power system. Besides, the stochastic time-delay model also needs to be updated for new communication technologies. The proposed AR model also contained certain predictive error, a new predictive model can be proposed to apply into the decentralized OPF problem. Due to time constraint and lengthy workload, we cannot undertake this in this chapter. The author will conduct an in-depth analysis in the next article.

Our work in chapter 5 has only introduced a general scheme to analyze the impact of CP attack on the convergence performance. The colluding attack is not considered during the attack. If the colluding attack happens, the proposed neighbouring monitoring strategy may fail to detect the attack due to the information change between nodes at the same time. The proposed neighbouring monitoring strategy is just the first step to analyze the cyber attack in the decentralized issue for power system. It should be noted that cyber attackers can take advantage of all vulnerabilities and contingencies in the network to damage the power system. The causes, processes and consequences across both cyber and physical spaces shall be comprehensively analyzed with consideration of all potential interdependence threats.

6.2 Future Directions of the Research

This thesis is the first in demonstrating decentralized control strategies combined with information and communication technology in the distribution power system network. There are a number of research gaps which have not been dealt with in this thesis. Some of them should be considered in a future work as listed below:

In chapter 3, the optimization problem should be considered to solve the voltage fluctuation issue cooperatively. In addition, the combination of independent and cooperative control strategies should be studied to avoid sudden fluctuation of voltage levels in an emergency. Another interesting direction of our work is to employ new communication technology to obtain the total processing time of delay and the probability of a delay in the framework of a distributed smart grid network.

In chapter 4, the framework of linear objective function can be transfer to a complex optimization problem, such as the non-linear problem. A relevant analysis of a non-linear problem could be an interesting research direction in a practical power system model. The multi-objective research can also be a meaningful area, e.g., minimization of power loss, maximization of economic benefit and the reactive power objective.

In chapter 5, in order to analyze all possible attack models, it is necessary to research all attack models including the practical attacks which may not be the worst cases. However, these cases can cause a chain reaction that may lead the system to a critical operation or a large blackout. To mitigate the potential threats in different scenarios, it is interesting to develop an effective defence scheme to deal with various threats.

Bibliography

[1] P. Kundur, *Power System Stability and Control.* New York: McGraw-Hill, 1994.

[2] H. M. Rustebakke, *Electric Utility Systems and Practices.* John Wiley & Sons, 1983.

[3] C. A. Gross, *Power System Analysis, Second Edition.* John Wiley & Sons, 1986.

[4] V. Gungor, B. Lu, and G. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Transactions on Indurtrial Electronics*, vol. 57, no. 10, pp. 3557–3564, Oct 2010.

[5] E. Parliament and of the Council, "Directive 2009/28/ec of the european parliament and of the council of 23 april 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing directives 2001/77/ec and 2003/30/ec," in *Official Journal of the European Union*, Brussels, Belgium, 2009.

[6] E. Parliament, "Directive 2009/28/ec of the european parliament and of the council," *Official J. Eur. Union*, pp. 16–62, 2009.

[7] K. R. C. Mamandur and R. D. Chenoweth, "Optimal control of reactive power flow for improvements in voltage profiles and for real power loss minimization," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 7, pp. 3185–3194, Jul 1981.

[8] N. D. Hatziargyriou and A. P. S. Meliopoulos, “Distributed energy sources: technical challenges,” *2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*, vol. 2, pp. 1017–1022, 2002.

[9] W. Y. Chiu, H. Sun, and H. V. Poor, “Energy imbalance management using a robust pricing scheme,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 896–904, Jun 2013.

[10] P. N. Vovos, A. E. Kiprakis, A. R. Wallace, and G. P. Harrison, “Centralized and distributed voltage control: Impact on distributed generation penetration,” *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 476–483, Feb 2007.

[11] N. Yorino, Y. Zoka, M. Watanabe, and T. Kurushima, “An optimal autonomous decentralized control method for voltage control devices by using a multi-agent system,” *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2225–2233, Sep 2015.

[12] V. Calderaro, G. Conio, V. Galdi, G. Massa, and A. Piccolo, “Optimal decentralized voltage control for distribution systems with inverter-based distributed generators,” *IEEE Transactions on Power Systems*, vol. 29, no. 1, pp. 230–241, Jan 2014.

[13] M. Baran and F. Wu, “Network reconfiguration in distribution systems for loss reduction and load balancing,” *IEEE Transactions on Power Delivery*, vol. 4, no. 2, pp. 1401–1407, Apr 1989.

[14] M. Huang, Y. Zhang, X. Zhang, and Z. Cai, “Reactive power coordinated control at the gateway between provincial and regional power grids,” in *processing 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Dec 2013, pp. 1–6.

[15] S. N. Salih and P. Chen, “On coordinated control of oltc and reactive power compensation for voltage regulation in distribution systems with wind power,” *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 4026–4035, Sep 2016.

[16] S. R. P and P. Sreejaya, “Coordinated voltage and reactive power control scheme for smart grids with distributed generation,” in *2015 International Conference on Control Communication Computing India (ICCC)*, Nov 2015, pp. 297–302.

[17] S. R. Islam, D. Sutanto, and K. M. Muttaqi, “Coordinated decentralized emergency voltage and reactive power control to prevent long-term voltage instability in a power system,” *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2591–2603, Sep 2015.

[18] F. Zhang, X. Guo, X. Chang, G. Fan, L. Chen, Q. Wang, Y. Tang, and J. Dai, “The reactive power voltage control strategy of pv systems in low-voltage string lines,” in *2017 IEEE Manchester PowerTech*, Jun 2017, pp. 1–6.

[19] N. Chen, M. Qian, L. Zhu, L. Yao, F. Wu, M. Chen, and N. Wang, “A coordinated reactive power and voltage control system for wind farm grid integration,” in *2012 IEEE International Conference on Power System Technology (POWERCON)*, Oct 2012, pp. 1–6.

[20] R. Anilkumar, G. Devriese, and A. K. Srivastava, “Voltage and reactive power control to maximize the energy savings in power distribution system with wind energy,” *IEEE Transactions on Industry Applications*, vol. PP, no. 99, pp. 1–1, 2017.

[21] W. Zheng, W. Wu, B. Zhang, and Y. Wang, “Robust reactive power optimisation and voltage control method for active distribution networks via dual time-scale coordination,” *IET Generation, Transmission Distribution*, vol. 11, no. 6, pp. 1461–1471, 2017.

[22] J. Zhang, S. Nabavi, A. Chakrabortty, and Y. Xin, “Admm optimization strategies for wide-area oscillation monitoring in power systems under asynchronous communication delays,” *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2123–2133, Jul 2016.

[23] R. Zhang and J. T. Kwok, "Asynchronous distributed admm for consensus optimization," *Proceedings of the 31 st International Conference on Machine Learning*, pp. 1701–1709, 2014.

[24] T. H. Chang, M. Hong, W. C. Liao, and X. Wang, "Asynchronous distributed admm for large-scale optimization part i: Algorithm and convergence analysis," *IEEE Transactions on Signal Processing*, vol. 64, no. 12, pp. 3118–3130, Jun 2016.

[25] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, 2011.

[26] J. W. Butler and C. Concordia, "Analysis of series capacitor application problems," *Electrical Engineering*, vol. 56, no. 8, pp. 975–988, Aug 1937.

[27] K. Tanaka, M. Oshiro, S. Toma, A. Yona, T. Senjyu, T. Funabashi, and C. H. Kim, "Decentralised control of voltage in distribution systems by distributed generators," *IET Generation, Transmission Distribution*, vol. 4, no. 11, pp. 1251–1260, Nov 2010.

[28] H. G. Yeh, D. F. Gayme, and S. H. Low, "Adaptive var control for distribution circuits with photovoltaic generators," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1656–1663, Aug 2012.

[29] X. Liu, A. Aichhorn, L. Liu, and H. Li, "Coordinated control of distributed energy storage system with tap changer transformers for voltage rise mitigation under high photovoltaic penetration," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 897–906, Jun 2012.

[30] S. H. Lee and J. J. Grainger, "Optimum placement of fixed and switched capacitors on primary distribution feeders," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 1, pp. 345–352, Jan 1981.

[31] M. Chis, M. M. A. Salama, and S. Jayaram, “Capacitor placement in distribution systems using heuristic search strategies,” *IEE Proceedings - Generation, Transmission and Distribution*, vol. 144, no. 3, pp. 225–230, May 1997.

[32] H. N. Ng, M. M. A. Salama, and A. Y. Chikhani, “Classification of capacitor allocation techniques,” *IEEE Transactions on Power Delivery*, vol. 15, no. 1, pp. 387–392, Jan 2000.

[33] R.-H. Liang and Y.-S. Wang, “Fuzzy-based reactive power and voltage control in a distribution system,” *IEEE Transactions on Power Delivery*, vol. 18, no. 2, pp. 610–618, Apr 2003.

[34] Y. Y. Hong and Y. F. Luo, “Optimal var control considering wind farms using probabilistic load-flow and gray-based genetic algorithms,” *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1441–1449, Jul 2009.

[35] T. Senjyu, Y. Miyazato, A. Yona, N. Urasaki, and T. Funabashi, “Optimal distribution voltage control and coordination with distributed generation,” *IEEE Transactions on Power Delivery*, vol. 23, no. 2, pp. 1236–1242, Apr 2008.

[36] T. Tsuji, T. Oyama, T. Hashiguchi, T. Goda, K. Horiuchi, S. Tange, T. Shinji, and S. Tsujita, “A study on autonomous decentralized voltage controller in distribution network considering control priority,” in *2011 International Conference on Clean Electrical Power (ICCEP)*, Jun 2011, pp. 749–754.

[37] Q. Zhang, J. He, and D. Zhang, “Coordinated control of energy storage devices and photovoltaic inverters for voltage regulation based on multi-agent system,” in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, Nov 2017, pp. 1–6.

[38] M. A. Laughton and M. W. H. Davies, “Numerical techniques in solution of power-system load-flow problems,” *Electrical Engineers, Proceedings of the Institution of*, vol. 111, no. 9, pp. 1575–1588, Sep 1964.

[39] B. Stott, "Review of load-flow calculation methods," *Proceedings of the IEEE*, vol. 62, no. 7, pp. 916–929, Jul 1974.

[40] S. Chatterjee and S. Mandal, "A novel comparison of gauss-seidel and newton-raphson methods for load flow analysis," in *2017 International Conference on Power and Embedded Drive Control (ICPEDC)*, Mar 2017, pp. 1–7.

[41] H. L. Nguyen, "Newton-raphson method in complex form [power system load flow analysis]," *IEEE Transactions on Power Systems*, vol. 12, no. 3, pp. 1355–1359, Aug 1997.

[42] Z. Zheng, L. Song, Z. Han, G. Y. Li, and H. V. Poor, "Multi-leader multi-follower game-based admm for big data processing," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Jul 2017, pp. 1–5.

[43] R. T. Rockafellar, *Convex Analysis.* Princeton University Press, 1970.

[44] D. P. Bertsekas, *Constrained Optimization and Lagrange Multiplier Methods.* Academic Press, 1982.

[45] D. Bertsekas, "On the method of multipliers for convex programming," *IEEE Transactions on Automatic Control*, vol. 20, no. 3, pp. 385–388, Jun 1975.

[46] A. Makhdoumi and A. Ozdaglar, "Convergence rate of distributed admm over networks," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 5082–5095, Oct 2017.

[47] F. Bach, *Learning with Submodular Functions:A Convex Optimization Perspective.* Now Foundations and Trends, 2013. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=8187292

[48] J. Eckstein and D. P. Bertsekas, "On the douglas—rachford splitting method and the proximal point algorithm for maximal monotone operators," *Mathematical Programming*, vol. 55, no. 1, pp. 293–318, Apr 1992. [Online]. Available: https://doi.org/10.1007/BF01581204

[49] D. P. Bertsekas and J. N. Tsitsiklis, “Parallel and distributed computation numerical methods,” *Prentice Hall*, 1989.

[50] K. Yokota, K. Sugiyama, J. Kurihara, and A. Tagami, “Rtt-based caching policies to improve user-centric performance in ccn,” in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Mar 2016, pp. 124–131.

[51] J. C. Bolot, “Characterizing end-to-end packet delay and loss in the internet,” *Journal of High-Speed Networks*, vol. 2, no. 3, pp. 289–298, Sep 1993.

[52] J. J. M. J. C. B. G. H. P. A. V. Moffaert, D. D. Vleeschauwer and P. Coppens, “Tuning the voip gateways to transport international voice calls over a best-effort ip backbone,” *9th IFIP CONFERENCE on PERFORMANCE MODELLING AND EVALUATION OF ATM & IP NETWORKS*, pp. 193–205, June 2001.

[53] D. G. Kendall, “Stochastic processes occurring in the theory of queues and their analysis by the method of the imbedded markov chain,” *The Annals of Mathematical Statistics*, vol. 24, no. 3, pp. 338–354, 1953.

[54] C. J. Bovy, H. T. Mertodimedjo, G. Hooghiemstra, H. Uijterwaal, and P. V. Mieghem, “Analysis of end-to-end delay measurements in internet,” *submitted to PAM*, 2002.

[55] K. Papagiannaki, S. Moon, C. Fraleigh, P. Thiran, F. Tobagi, and C. Diot, “Analysis of measured single-hop delay from an operational backbone network,” in *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, June 2002, pp. 535–544.

[56] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson, “Self-similarity through high-variability: statistical analysis of ethernet lan traffic at the source level,” *IEEE/ACM Transactions on Networking*, vol. 5, no. 1, pp. 71–86, Feb 1997.

[57] R. Smith, “Assault on california power station raises alarm on potential for terrorism,” *The Wall Street Journal*, pp. 1–7, 2014.

[58] T. Staff, “Steinitz: Israels electric authority hit by severe cyber-attack,” *The Times of Israel*, Jan 2016. [Online]. Available: https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/

[59] N. I. of Standards and T. (NIST), “Framework and roadmap for smart grid interoperability standards release v3.0,” *NIST Special Publication, Gaithersburg, MD*, 2014.

[60] I. Dumitrache and D. I. Dogaru, “Smart grid overview: Infrastructure, cyber-physical security and challenges,” in *2015 20th International Conference on Control Systems and Computer Science*, May 2015, pp. 693–699.

[61] U.-C. P. S. O. T. Force, “Final report on the august 14, 2003 blackout in the united states and canada: causes and recommendations,” *Office of Electricity Delivery & Energy Reliability*, Apr 2013. [Online]. Available: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[62] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” *IET Cyber-Physical Systems: Theory Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[63] L. Kotut and L. A. Wahsheh, “Survey of cyber security challenges and solutions in smart grids,” in *2016 Cybersecurity Symposium (CYBERSEC)*, Apr 2016, pp. 32–37.

[64] J. D. Glover and M. S. Sarma, *Power System Analysis and Design.* Cengage, 2012.

[65] M. Zeller, “Common questions and answers addressing the aurora vulnerability,” in *DistribuTECH Conference*, San Diego, California, Feb 2011.

[66] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar 2013.

[67] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar 2014.

[68] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “Cyber attack in a two-area power system: Impact identification using reachability,” in *Proceedings of the 2010 American Control Conference*, Jun 2010, pp. 962–967.

[69] A. J. Holmgren, E. Jenelius, and J. Westin, “Evaluating strategies for defending electric power networks against antagonistic attacks,” *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 76–84, Feb 2007.

[70] A. L. Motto, J. M. Arroyo, and F. D. Galiana, “A mixed-integer lp procedure for the analysis of electric grid security under disruptive threat,” *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1357–1365, Aug 2005.

[71] Y. Zhang, Y. Xiang, and L. Wang, “Power system reliability assessment incorporating cyber attacks against wind farm energy management systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2343–2357, Sep 2017.

[72] J. Yan, H. He, X. Zhong, and Y. Tang, “Q-learning-based vulnerability analysis of smart grid against sequential topology attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, Jan 2017.

[73] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” *Nature volume 464*, pp. 1025–1028, Apr 2010.

[74] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, Mar 2014.

[75] J. Hong, "Cybersecurity of substation automation systems," *PhD thesis, Washington State University*, 2014.

[76] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, Dec 2013.

[77] A. Abur and A. G. Expsito, "Power system state estimation: theory and implementation," *CRC Press*, Mar 2004.

[78] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul 2017.

[79] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep 2012.

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

[81] ——, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, Sep 2012.

[82] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, March 2013.

[83] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Crdenas, and J. G. Jetcheva, "Ami threats, intrusion detection requirements and

deployment recommendations," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2012, pp. 395–400.

[84] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319–1330, Jul 2013.

[85] L. Sankar, S. R. Rajagopalan, S. Mohajer, and S. Mohajer, "Smart meter privacy: A theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 837–846, Jun 2013.

[86] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 627–636, Mar 2014.

[87] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[88] D. H. Choi and L. Xie, "Sensitivity analysis of real-time locational marginal price to scada sensor data corruption," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1110–1120, May 2014.

[89] J. Giraldo, A. Crdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sep 2017.

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

[91] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun 2010.

[92] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3209–3223, Dec 2014.

[93] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, "Severe multiple contingency screening in electric power systems," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 406–417, May 2008.

[94] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. F. Wang, "Intrusion detection system for network security in synchrophasor systems," in *IET International Conference on Information and Communications Technologies (IETICT 2013)*, Apr 2013, pp. 246–252.

[95] R. Mitchell and I. R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sep 2013.

[96] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.

[97] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1000–1009, Aug 2011.

[98] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 4, pp. 712–718, Jul 2007.

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

[100] R. Bhisey, “Smart grid security market: Technological progress in energy & power industry trends 2025,” *The Edition Truth*, Aug. 2017. [online]. Available:http://www.editiontruth.com/smart-grid-security-market-technological-progress-energy-power-industry-trends-2025/.

[101] M. Brenna, E. D. Berardinis, L. D. Carpini, F. Foiadelli, P. Paulon, P. Petroni, G. Sapienza, G. Scrosati, and D. Zaninelli, “Automatic distributed voltage control algorithm in smart grids applications,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 877–885, Jun 2013.

[102] S. Corsi, “Wide area voltage regulation and protection,” in *2009 IEEE Bucharest PowerTech*, Jun 2009, pp. 1–7.

[103] E. N. GmbH, “Grid codehigh and extra high voltage,” Bayreut, Germany, Apr 2006.

[104] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, “Smart grid technologies: Communication technologies and s-tandards,” *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, Nov 2011.

[105] P. Kyosti, J. Meinila, and L. Hentila, “Winner ii channel models,” *European Commission, Deliverable IST-WINNER D1.1.2 ver 1.1*, Sep. 2007.[Online].Available:http://projects.celticinitiative.org/winner+/ WINNER2-Deliverables/.

[106] “3rd generation partnership project tr 36.814 v9.0.0 (release 9),” Mar. 2010.[Online].Available:http://www.qtc.jp/3GPP/Specs/36814-900.pdf.

[107] W. D. Caetano, P. R. S. Jota, and E. N. Gonalves, “Comparison between static models of commercial/residential loads and their effects on conservation voltage reduction,” in *2013 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, Aug 2013, pp. 1–6.

[108] J. Momoh, *Stability Analysis Tools for Smart Grid.* Wiley-IEEE Press, 2012, pp. 51–99. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6183638

[109] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home m2m networks: Architectures, standards, and qos improvement," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, Apr 2011.

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

[111] H. Liang, A. K. Tamang, W. Zhuang, and X. S. Shen, "Stochastic information management in smart grid," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1746–1770, Feb 2014.

[112] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar 2013.

[113] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1821–1831, Nov 2006.

[114] Y. Zhang, E. Dall'Anese, M. Hong, S. Dhople, and Z. Xu, "Regulation of renewable energy sources to optimal power flow solutions using admm," in *2017 American Control Conference (ACC)*, May 2017, pp. 3394–3399.

[115] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Transactions on Power Delivery*, vol. 4, no. 1, pp. 735–743, Jan 1989.

[116] M. Chinchilla, S. Arnaltes, and J. C. Burgos, "Control of permanent-magnet generators applied to variable-speed wind-energy systems connected to the grid," *IEEE Transactions on Energy Conversion*, vol. 21, no. 1, pp. 130–135, Mar 2006.

[117] S. Kundu and I. A. Hiskens, "Distributed control of reactive power from photovoltaic inverters," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS2013)*, May 2013, pp. 249–252.

[118] M. Kraning, E. Chu, J. Lavaei, and S. Boyd, "Message passing for dynamic network energy management," *Found. Trends Optimiz*, vol. 1, no. 2, pp. 70–122, 2013.

[119] S. Boyd and L. Vandenberghe, "Convex optimization," *Cambridge, U.K.: Cambridge Univ. Press*, 2004.

[120] M. Angjelichinoski, C. Stefanovic, P. Popovski, H. Liu, P. C. Loh, and F. Blaabjerg, "Power talk: How to modulate data over a dc micro grid bus using power electronics," *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, Dec 2015.

[121] S. Magnsson, P. C. Weeraddana, M. G. Rabbat, and C. Fischione, "On the convergence of alternating direction lagrangian methods for nonconvex structured optimization problems," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 3, pp. 296–309, Sep 2016.

[122] G. Hendrantoro, A. Mauludiyanto, and P. Handayani, "An autoregressive model for simulation of time-varying rain rate," *2004 10th International Symposium on Antenna Technology and Applied Electromagnetics and URSI Conference*, pp. 1–4, Jul 2004.

[123] M. G. Anderson, N. Zhou, J. W. Pierre, and R. W. Wies, "Bootstrap-based confidence interval estimates for electromechanical modes from multiple output analysis of measured ambient data," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 943–950, May 2005.

[124] H. Akaike, "Information theory and an extension of the maximum likelihood principle," *Springer Series in Statistics, Perspectives in Statistics.*, vol. 1, pp. 610–624, 1992.

[125] I. D. Schizas, A. Ribeiro, and G. B. Giannakis, “Consensus in ad hoc wsns with noisy links part i: Distributed estimation of deterministic signals,” *IEEE Transactions on Signal Processing*, vol. 56, no. 1, pp. 350–364, Jan 2008.

[126] M. Srinivas and L. M. Patnaik, “Genetic algorithms: a survey,” *Computer*, vol. 27, no. 6, pp. 17–26, Jun 1994.

[127] J. Xu, H. Sun, and C. Dent, “The coordinated voltage control meets imperfect communication system,” in *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Oct 2016, pp. 1–5.

[128] C. Guille and G. Gross, “A conceptual framework for the vehicle-to-grid implementation,” *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, 2009.

[129] J. Zhang, M. Momtazpour, N. Ramakrishnan, G. Welch, and S. Rahman, “Secure and adaptive state estimation for a pmu-equipped smart grid,” in *2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*, Jun 2015, pp. 1431–1436.

[130] V. Singh and M. Jain, “Analysis of trust dynamics in cyclic mobile: Ad hoc networks,” in *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, Feb 2015, pp. 400–406.

[131] A. Q. Huang, M. L. Crow, G. T. Heydt, J. P. Zheng, and S. J. Dale, “The future renewable electric energy delivery and management (freedm) system: The energy internet,” *Proceedings of the IEEE*, vol. 99, no. 1, pp. 133–148, Jan 2011.

[132] M. Hong, Z. Luo, and M. Razaviyayn, “Convergence analysis of alternating direction method of multipliers for a family of nonconvex problems,” *SIAM Journal On Optimization*, vol. 26, no. 1, pp. 337–364, 2016.

Appendix A

Basic and Auxiliary Results

A.1 Proof of Lemma 1

Proof of Lemma 1(a): According to the update of global variables (4.35), we can obtain that the following is true

$$\nabla F_i(x_i(k_i^\tau + 1)) + y_i(k) + \rho_i(\overline{x}_i(k+1) - x_i(k+1)) = 0, \tag{4.36}$$

Further, from (4.36), we have

$$\nabla F_i(x_i(k_i^\tau + 1)) = -y_i(k+1), \tag{4.37}$$

Similarly, it also have the following equality for iteration k

$$\nabla F_i(x_i(k_i^\tau)) = -y_i(k), \tag{4.38}$$

Therefore, when the new information is delayed or lost for each node i, it follows that

$$\nabla F_i(x_i(k_i^\tau + 1)) = \nabla F_i(x_i(k_i^\tau)), \tag{4.39}$$

According to (4.39), we have

$$\| y_i(k+1) - y_i(k) \|_2^2 = 0, \tag{4.40}$$

It means that Lemma 1(a) is true when message delayed or loss occurred. If the information arrives, we also have the following results by using triangle inequality.

$$\begin{aligned}
\| y_i(k+1) - y_i(k) \|_2^2 &= \| \nabla F_i(x_i(k_i^\tau + 1)) - \nabla F_i(x_i(k_i^\tau)) \|_2^2 \\
&\leq K_i^2 \| x_i(k_i^\tau + 1) - x_i(k_i^\tau) \| \\
&\leq K_i^2 (\sum_{\kappa=0}^{T_i} \| x_i(k+1-\kappa) - x_i(k-\kappa) \|)^2 \\
&\leq K_i^2 (T_i + 1) \sum_{\kappa=0}^{T_i} \| x_i(k+1-\kappa) - x_i(k-\kappa) \|_2^2 .
\end{aligned} \tag{4.41}$$

Subsequently, the desired result in Lemma 1(a) is achieved.

Proof of Lemma 1(b): According to the Lipschitz continuity of ∇F_i and triangle inequality, which implies that

$$\begin{aligned}
F_i(x_i(k+1)) &\leq F_i(\overline{x}_i(k+1)) + \nabla F_i(\overline{x}_i(k+1)) \parallel x_i(k+1) - \overline{x}_i(k+1) \parallel \\
&+ \frac{K_i}{2} \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2 \\
&= F_i(\overline{x}_i(k+1)) - \parallel \nabla F_i(\overline{x}_i(k+1)) - \nabla F_i(x_i(k+1)) \parallel \parallel x_i(k+1) - \overline{x}_i(k+1) \parallel \\
&+ \nabla F_i(x_i(k+1)) \parallel x_i(k+1) - \overline{x}_i(k+1) \parallel + \frac{K_i}{2} \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2 \\
&\leq F_i(\overline{x}_i(k+1)) + \nabla F_i(x_i(k+1)) \parallel x_i(k+1) - \overline{x}_i(k+1) \parallel \\
&+ \frac{3K_i}{2} \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2 .
\end{aligned} \tag{4.42}$$

Further, from (4.37), we have

$$\begin{aligned}
\mathcal{L}(\{\overline{x}_i(k)\}; \{x_i(k)\}, \{y_i(k)\}) &= \sum_{i=1}^{\nu} (F_i(\overline{x}_i(k+1)) + y_i(k+1) \parallel \overline{x}_i(k+1) \\
&- x_i(k+1) \parallel + \frac{\rho_i}{2} \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2) \\
&\geq \sum_{i=1}^{\nu} (F_i(\overline{x}_i(k+1)) + \frac{\rho_i - 3K_i}{2} \parallel \overline{x}_i(k+1) \\
&- x_i(k+1) \parallel_2^2 + \parallel \nabla F_i(x_i(k+1)) \\
&- \nabla F_i(x_i(k_i^{\tau}+1)) \parallel \parallel x_i(k+1) - \overline{x}_i(k+1) \parallel).
\end{aligned} \tag{4.43}$$

According to the Cauchy-Schwarz inequality on the last term in (4.43), it follows that

$$\begin{aligned}
&\mathcal{L}(\{\overline{x}_i(k+1)\};\{x_i(k+1)\},\{y_i(k+1)\}) \\
&\geq P_{los} + \frac{\rho_i - 3K_i}{2}\sum \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2 \\
&- \parallel \nabla F_i(x_i(k+1)) - \nabla F_i(\overline{x}_i(k_i^\tau + 1)) \parallel\parallel x_i(k+1) - \overline{x}_i(k+1) \parallel \\
&\geq P_{los} + \frac{\rho_i - 4K_i}{2}\sum \parallel \overline{x}_i(k+1) - x_i(k+1) \parallel_2^2 - \frac{K_i}{2} \parallel x_i(k+1) - x_i(k_i^\tau + 1) \parallel_2^2 \\
&\geq P_{los} - \sum_{i=1}^{\nu} \frac{Ki}{2} diam^2(\mathcal{X}) > -\infty.
\end{aligned} \tag{4.44}$$

where the last inequality follows the fact that $\mathcal{X}$ is compact in assumption 1 and $\rho_i - 7K_i > 0$ in assumption 3

A.2 Proof of Theorem 1

Proof of Theorem 1(a): According to Lemma 1, it is true that $\mathcal{L}(\{\overline{x}_i(k)\};\{x_i(k)\},\{y_i(k)\})$ converges as $k \to \infty$. Therefore, it holds from Lemma 1(a) that

$$\lim_{k\to\infty} \parallel x_i(k+1) - x_i(k) \parallel \to 0, \quad i = 1, ..., \nu \tag{4.45a}$$

$$\lim_{k\to\infty} \parallel \overline{x}_i(k+1) - \overline{x}_i(k) \parallel \to 0, \quad i = 1, ..., \nu \tag{4.45b}$$

Then, using (4.45) into (4.41), it follows that

$$\lim_{k\to\infty} \parallel y_i(k+1) - y_i(k) \parallel \to 0, \quad i = 1, ..., \nu \tag{4.46a}$$

$$\lim_{k\to\infty} \parallel \overline{x}_i(k) - x_i(k) \parallel \to 0, \quad i = 1, ..., \nu \tag{4.46b}$$

Proof of Theorem 1(b): According to (4.46), it is true that certain sequences $\{\{\overline{x}_i^*\},\{x_i^*\},\{y_i^*\}\}$ exist which follows that

$$\nabla F_i(\overline{x}_i^*) + y_i^* = 0, \quad i = 1, ..., \nu \tag{4.47a}$$

$$\overline{x}_i^* = x_i^*, \quad i = 1, ..., \nu \tag{4.47b}$$

Since $x_i(k+1) \in \mathcal{X}$, it holds that $x_i^* \in \mathcal{X}$. Once we can present that the primal feasibility gap goes to zero, the proof for stationary solution is straightforward. The details also can be found in [132]. Then the desired result is achieved..

A.3 Original publications

Conference Paper:

1. Jiangjiao Xu, Hongjian Sun, and Chris Dent, The coordinated voltage control meets imperfect communication system, 2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Oct 2016, pp. 1-5.

2. Jiangjiao Xu and Hongjian Sun, ADMM-based Coordinated Decentralized Voltage Control Meets Practical Communication Systems, IEEE International Conference on Communications (IEEE ICC'17): Bridging People, Communities, and Cultures. Paris, France, May 2017, pp. 906-910.

Journal Paper:

1. Jiangjiao Xu, Hongjian Sun, and Chris Dent, ADMM-based Decentralized OPF Problem Meets Stochastic Communication Delay in Smart Grid, IEEE Transaction on Smart Grid, submitted, major revision.