University of Wisconsin Milwaukee
UWM Digital Commons

Theses and Dissertations

December 2017

Reliability Evaluation and Defense Strategy Development for Cyber-physical Power Systems

Yingmeng Xiang
University of Wisconsin-Milwaukee

Follow this and additional works at: https://dc.uwm.edu/etd

Part of the Electrical and Electronics Commons

Recommended Citation

Xiang, Yingmeng, "Reliability Evaluation and Defense Strategy Development for Cyber-physical Power Systems" (2017). *Theses and Dissertations*. 1725.
https://dc.uwm.edu/etd/1725

This Dissertation is brought to you for free and open access by UWM Digital Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of UWM Digital Commons. For more information, please contact open-access@uwm.edu.

RELIABILITY EVALUATION AND DEFENSE STRATEGY DEVELOPMENT FOR CYBER-PHYSICAL POWER SYSTEMS

by

Yingmeng Xiang

A Dissertation Submitted in
Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
in Engineering

at

The University of Wisconsin-Milwaukee
December 2017

ABSTRACT

RELIABILITY EVALUATION AND DEFENSE STRATEGY DEVELOPMENT FOR CYBER-PHYSICAL POWER SYSTEMS

by

Yingmeng Xiang

The University of Wisconsin-Milwaukee, 2017
Under the Supervision of Professor Lingfeng Wang

With the smart grid initiatives in recent years, the electric power grid is rapidly evolving into a complicated and interconnected cyber-physical system. Unfortunately, the wide deployment of cutting-edge communication, control and computer technologies in the power system, as well as the increasing terrorism activities, make the power system at great risk of attacks from both cyber and physical domains. It is pressing and meaningful to investigate the plausible attack scenarios and develop efficient methods for defending the power system against them.

To defend the power grid, it is critical to first study how the attacks could happen and affect the power system, which are the basis for the defense strategy development. Thus, this dissertation quantifies the influence of several typical attacks on power system reliability. Specifically, three representative attack are considered, i.e., intrusion against substations, regional LR attack, and coordinated attacks. For the intrusion against substations, the occurrence frequency of the attack events is modeled based on statistical data and human dynamics; game-theoretical approaches are adopted to model induvial and consecutive attack cases; Monte Carlo simulation is deployed to obtain the desired reliability indices, which incorporates both the attacks and the random failures.

For the false data injection attack, a practical regional load redistribution (LR) attack strategy is proposed; the man-in-the-middle (MITM) intrusion process is modeled with a semi-Markov process method; the reliability indices are obtained based on the regional LR attack strategy and the MITM intrusion process using Monte Carlo simulation. For the coordinated attacks, a few typical coordination strategies are proposed considering attacking the current-carrying elements as well as attacking the measurements; a bilevel optimization method is applied to develop the optimal coordination strategy.

Further, efficient and effective defense strategies are proposed from the perspectives of power system operation strategy and identification of critical elements. Specially, a robustness-oriented power grid operation strategy is proposed considering the element random failures and the risk of man-made attacks. Using this operation strategy, the power system operation is robust, and can minimize the load loss in case of malicious man-made attacks. Also, a multiple-attack-scenario (MAS) defender-attack-defender model is proposed to identify the critical branches that should be defended when an attack is anticipated but the defender has uncertainty about the capability of the attacker. If those identified critical branches are protected, the expected load loss will be minimal.

© Copyright by Yingmeng Xiang, 2017
All Rights Reserved

To

my beloved parents,

and Uncle Guo.

TABLE OF CONTENTS

ABSTRACT ii

LIST OF FIGURES x

LIST OF TABLES xiv

ACKNOWLEDGEMENTS xix

1. Introduction 1
    - 1.1 Research Motivations 1
    - 1.2 Dissertation Objectives 3
    - 1.3 Dissertation Organization 4
2. Adequacy Evaluation of Power Grids Considering Substation Cyber Vulnerabilities 5
    - 2.1 Introduction 5
    - 2.2 Human Dynamics Analysis for Cyber Attacks 6
    - 2.3 Cyber Vulnerabilities of Substations 12
    - 2.4 A Game-Theoretic Approach 17
        - 2.4.1 The Markov Game 18
        - 2.4.2 The Static Game 21
    - 2.5 Power System Adequacy Evaluation 22
    - 2.6 Case Studies 27
        - 2.6.1 Influence of the Judgment of the Attack Type 29
        - 2.6.2 Influence of the Human Dynamics 30
        - 2.6.3 Influence of the Cybersecurity Parameters 31
        - 2.6.4 Influence of the Repair Time 33
    - 2.7 Conclusions 33

3. Power System Reliability Evaluation Considering Load Redistribution Attacks 35

3.1 Introduction 35

3.2 Intrusion Process Modeling for MITM Attack Against State Estimation 35

3.2.1 Attacks against Power System State Estimation 36

3.2.2 Attack against Non-encrypted SCADA Network 37

3.2.3 Attack against Encrypted SCADA Network 40

3.2.4 Calculation of MTTA 43

3.3 Regional Load Redistribution Attack Model 46

3.4 Power System Reliability Modeling 48

3.5 Case Studies and Simulation Results 51

3.5.1 MTTA of the Attack 51

3.5.2 Regional Load Redistribution Attack... 53

3.5.3 Reliability Modeling of Power System 55

3.6 Conclusions 57

4. Coordinated Attacks on Electric Power Systems in a Cyber-Physical Environment 58

4.1 Introduction 58

4.2 Power System Vulnerabilities and Coordinated Attacks 59

4.2.1 Analysis of Attacks against Power Systems.. 59

4.2.2 Power System Operation and Coordinated Attacks 61

4.3 Principle of Coordinated Attacks 66

4.4 LR Attack Coordinating with Attacking Generators 68

4.5 LR Attack Coordinating with Attacking Lines 71

4.6 Case Studies 73

4.6.1 LR Attack Coordinating with Attacking Generators 74

4.6.2 LR Attack Coordinating with Attacking Lines 78

4.7 Conclusions 81

5. A Robustness-Oriented Power Grid Operation Strategy Considering Attacks 82

5.1 Introduction 82

5.2 Attacks and Resultant Impacts 84

5.2.1 Attack Cases 84

5.2.2 Impact Analysis of Attacks 85

5.3 Problem Formulation 87

5.3.1 General SCOPF Formulation 87

5.3.2 Extended SCOPF Formulation Considering Attacks 89

5.3.3 Short-Term Post-Contingency Feasibility Check 90

5.3.4 Long-Term Post-Contingency Feasibility Check 91

5.3.5 Post-Attack Impact Analysis 91

5.4 Parallel Hybrid Solution Methodology 92

5.4.1 Computation Strategy 93

5.4.2 Computational Procedure 94

5.5 Case Studies 97

5.5.1 IEEE 14-bus System 98

5.5.2 IEEE 39-bus System 104

5.5.3 IEEE 118-bus System 108

5.6 Conclusions 111

6. An Improved Defender-Attacker-Defender Model for Transmission Lines Defense Considering Offensive Resource Uncertainties 112
6.1 Introduction 112
6.2 Problem Formulation 114
6.2.1 Conventional DAD Model 115
6.2.2 Modeling of Uncertainties 118
6.2.3 Proposed DAD Model Considering Uncertainties 119
6.3 Solution Method 122
6.3.1 Upper-Level Problem 123
6.3.2 Lower-Level Problem 125
6.3.3 Overall C&CG Algorithm 126
6.4 Case Studies 128
6.4.1 IEEE RTS79 system 128
6.4.2 IEEE 57-bus system 136
6.5 Conclusions 136
7. Conclusions and Future Work 138
7.1 Conclusions 138
7.2 Future Work 140
REFERENCES 141

LIST OF FIGURES

Figure 2. 1 Comparison between Poisson and power law distributions 7

Figure 2. 2 The occurrence pattern of the cyber attacks 8

Figure 2. 3 The relationship between probability and cyber attack intervals 9

Figure 2. 4 Simple illustration of the cyber attacker society 9

Figure 2. 5 The influence of social conformity psychology 11

Figure 2. 6 Power system cyber architecture 12

Figure 2. 7 An illustrative attack path.. 12

Figure 2. 8 Example of individual attacks 16

Figure 2. 9 Example of consecutive attacks... 16

Figure 2. 10 Sampling of the attack occurrence and the component statuses....................... 23

Figure 2. 11 Evaluation of system state 24

Figure 2. 12 A holistic adequacy assessment framework considering cyber attacks against substations.. 25

Figure 2. 13 Optimal mixed strategies for the players when all substations are up 29

Figure 2. 14 Comparison of attack type judgment... 30

Figure 2. 15 Influence of social conformity psychology on system adequacy..................... 31

Figure 2. 16 Influence of p_{aud} on system adequacy... 32

Figure 2. 17 Influence of p_{ad} on system adequacy 32

Figure 2. 18 Influence of individual substation cybersecurity on system adequacy 33

Figure 2. 19 Influence of MTTRA on system adequacy 33

Figure 3. 1 Attack tree for the state estimation.. 37

Figure 3. 2 Illustration of the attack... 37

Figure 3. 3 Semi-Markov model for attack against non-encrypted SCADA........................ 39

Figure 3. 4 Semi-Markov model for attack against encrypted SCADA 42

Figure 3. 5 Flowchart for power grid reliability assessment considering LR attacks........... 49

Figure 3. 6 The influence of attack time in the attack phases.. 52

Figure 3. 7 Regional load redistribution attack schemes with IEEE RTS79 system............ 53

Figure 3. 8 Regional attack results... 54

Figure 4. 1 Schematic overview of the chapter.. 59

Figure 4. 2 Attacks against electric power systems 60

Figure 4. 3 Power system operation and attacks... 62

Figure 4. 4 Coordinated physical attacks against lines 63

Figure 4. 5 Coordinated cyberattacks against substations 63

Figure 4. 6 Physically tripping a line coordinating with DDoS attack 63

Figure 4. 7 Cyberattack against a generator coordinating with false data injection attack .. 64

Figure 4. 8 Faulting a line coordinating with changing the relay’s setting........................... 64

Figure 4. 9 False data injection attack coordinating with tripping a line.............................. 65

Figure 4. 10 Bilevel modeling for the LR attack 67

Figure 4. 11 A bilevel model for the coordination of LR attack and other attacks 68

Figure 4. 12 Illustration of the LR attack coordinating with attacking generators............... 71

Figure 4. 13 Illustration of the LR attack coordinating with attacking lines 73

Figure 4. 14 Example of LR attack coordinating with tripping generators 75

Figure 4. 15 Sensitivity analysis for the cyberattack resource... 76

Figure 4. 16 Influence of load measurement attack magnitude limit τ................................. 77

Figure 4. 17 Example of LR attack coordinating with tripping a line with cyberattack resource of 25 79

Figure 4. 18 Example of LR attack coordinating with tripping a line with cyberattack resource of 45 80

Figure 5. 1 Resiliency construct of power systems 83

Figure 5. 2 Risk of attack against power system 86

Figure 5. 3 Cascading failure simulation flowchart 87

Figure 5. 4 Conventional SCOPF framework 87

Figure 5. 5 An extended SCOPF framework considering probable attack scenarios 89

Figure 5. 6 Procedure of the hybrid solution methodology 96

Figure 5. 7 Convergence of PSO for BAC-OPF in IEEE 14-bus system 100

Figure 5. 8 Load loss ratio in IEEE 14-bus system based on the N-1 SCOPF when two buses are attacked 102

Figure 5. 9 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF when two buses are attacked 103

Figure 5. 10 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF incorporating two attack cases when a bus is tripped 104

Figure 5. 11 Comparison of the impact of bus-isolating attack in IEEE 39-bus system 105

Figure 5. 12 Load loss ratio in IEEE 39-bus system based on N-1 SCOPF 107

Figure 5. 13 Load loss ratio in IEEE 39-bus system based on the proposed SCOPF considering attacks against one bus and one line simultaneously 108

Figure 5. 14 Comparison of the impact of bus-isolating attack in IEEE 118-bus system .. 109

Figure 6. 1 Conventional defender-attacker-defender model 115

Figure 6. 2 Proposed Multiple-Attack-Scenario defender-attacker-defender model.......... 118

Figure 6. 3 Overview of the C&CG algorithm 127

Figure 6. 4 Illustration of the attack and defense strategies for case 2 132

Figure 6. 5 Consequences for the sensitivity study of the attack scenario probabilities 133

Figure 6. 6 Consequences for the impact of the defensive resource................................... 135

LIST OF TABLES

Table 2. 1 Load curtailment caused by substation failure 27

Table 2. 2 Payoffs of static game when all substations are up 27

Table 2. 3 Payoffs of Markov game when all substations are up 28

Table 2. 4 System adequacy comparison with and without cyber attacks 29

Table 3. 1 Example time intervals for non-encrypted SCADA 52

Table 3. 2 Example time intervals for encrypted SCADA 52

Table 3. 3 Examples of regional LR attacks 54

Table 3. 4 Reliability evaluation with complete LR attack 55

Table 3. 5 Reliability evaluation with regional LR attack 56

Table 4. 1 Parameters of Generations 74

Table 4. 2 Comparisons of different attack strategies 75

Table 4. 3 Influence of the security factor 77

Table 4. 4 Load curtailment comparison for different attack strategies 79

Table 4. 5 Comparison with different attack strategies 80

Table 5. 1 Illustration of the solution method 93

Table 5. 2 Active power outputs based on N-1 SCOPF in IEEE 14-bus system 99

Table 5. 3 Loss for bus-isolating attack in 14-bus system under N-1 SCOPF 99

Table 5. 4 Loss for line-tripping attack in 14-bus system under N-1 SCOPF 99

Table 5. 5 Active power outputs based on BAC-OPF in IEEE 14-bus system 100

Table 5. 6 Loss for bus-tripping attack in IEEE 14-bus system under BAC-OPF 100

Table 5. 7 Active power outputs based on BAC-OPF without considering short-term feasibility in IEEE 14-bus system 101

Table 5. 8 Active power outputs based on LAC-OPF in IEEE 14-bus system 101

Table 5. 9 Loss for line-tripping attack in IEEE 14-bus system under LAC-OPF 101

Table 5. 10 Active power outputs in IEEE 14-bus system based on the proposed SCOPF considering attacks against two buses... 102

Table 5. 11 Active power outputs in IEEE 14-bus system based on proposed SCOPF considering two possible attack conditions.. 103

Table 5. 12 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF incorporating two attack conditions when two lines are tripped 103

Table 5. 13 Active power generation comparison for IEEE 39-bus system (MW)............ 105

Table 5. 14 Loss in line-tripping attack based on N-1 SCOPF in IEEE 39-bus................ 106

Table 5. 15 Loss in line-tripping attack based on LAC-OPF in IEEE 39-bus................... 106

Table 5. 16 Active power outputs in IEEE 39-bus system considering attacks against one bus and one line simultaneously... 108

Table 5. 17 Active power generation in IEEE 118-bus system 109

Table 5. 18 Loss in line-tripping attack based on N-1 SCOPF... 110

Table 5. 19 Loss in line-tripping attack based on LAC-OPF in 118-bus system 110

Table 6. 1 Simulation results for case 1 129

Table 6. 2 Comparative studies for case 1 130

Table 6. 3 Simulation results for case 2 131

Table 6. 4 Comparative studies for case 2 132

Table 6. 5 Defensive and offensive strategies for the sensitivity study of the attack scenario probabilities.. 134

Table 6. 6 Defensive and offensive strategies for the impact of the defensive resource 135

Table 6. 7 Comparative studies for IEEE 57-bus system 136

LIST OF ABBREVIATIONS

3-DES	Triple data encryption standard
BAC-OPF	Bus attack constrained optimal power flow
C&CG	Column-and-constraint generation
DAD	Defender-attacker-defender
DDoS	Distributed denial of service
DNP	Distributed network protocol
DoS	Denial of service
EENS	Expected energy not supplied
EMS	Energy management system
FACTS	Flexible alternating current transmission system
GSM	Global system for Mobile communications
HMI	Human machine interface
IDS	Intrusion detection system
IED	Intelligent electronic devices
KKT	Karush–Kuhn–Tucker
LAC-OPF	Line attack constrained optimal power flow
LLP	Lower-level problem
LOLP	Loss of load probability
LR	Load redistribution
MAS	Multiple attack scenario
MCS	Monte Carlo simulation
MILP	Mixed-integer linear programming

MTTA	Mean time to attack
MTTF	Mean time to failure
OPF	Optimal power flow
PSO	Particle swarm optimization
PDIP	Primal-dual interior point
RTS	Reliability test system
SCADA	Supervisory control and data acquisition
SCOPF	Security constrained optimal power flow
SHA	Secure hash algorithm
SMP	Semi-Markov process
SSL	Secure sockets layer
SSSA	Steady-state security assessment
ULP	Upper-level problem
VPN	Virtual private network
WAN	Wide area network

ACKNOWLEDGEMENTS

I would like to sincerely thank my advisor, Prof. Lingfeng Wang, for his insightful guidance, immense knowledge, valuable comments, various opportunities, great patience and continuous support during my PhD journey. His consistent enthusiasm on research always motivates me to aim higher and dig deeper.

I want to express my great gratitude to other committee members, Dr. Yi Hu, Dr. Chiu Law, Dr. Chao Zhu, and Dr. Xiao Qin for their support and advice. I greatly appreciate their time, effort and insightful comments.

I am very thankful to Yichi Zhang, Jun Tan, Zhu Wang, Rui Yang, and Prof. David Yu for all the discussions, guidance, help and encouragement, both academically and personally. Your help is of great value to me.

My great thanks are extended to my fellow colleagues Yunfan Zhang, Ming Wang, Ruosong Xiao, Zhilu Ding and Dandan Wang. Doing research with you is enjoyable and beneficial.

My sincere thanks also go to my good friends, including but not limited to, Hongjun Gao, Hongda Liu, Qingxue Lai, Bing Jin, Jizhou Tong, Zhongyue Sun, Qiang Fu, Meiling He, and Jiayan Nie. Without your help, encouragement and friendship, my life in Ohio and Wisconsin would not have been so colorful and fruitful.

This graduate research was in part supported by the National Science Foundation (NSF) under Award ECCS1128594. I am greatly grateful for the financial support.

Last, I own my deepest gratitude to my beloved parents and Uncle Guo for their immense love and invaluable support.

1. Introduction

1.1 Research Motivations

Due to the smart grid initiative, numerous emerging cyber and computer technologies are being applied in the modern power grid, such as wide area monitoring and control technologies [1], IEC 61850 based substations [2], flexible alternating current transmission system devices [3]-[4], distributed energy storage [5], and microgrid [6], etc. These changes can allow the cyber attackers to get access to the hierarchical control systems and exploit the vulnerabilities to gain the control privilege. Typical cyberattacks include denial of service (DoS) attacks, database modification, replay attack, and false data injection attack. In the physical domain, the power system is also vulnerable to both vandalism and terrorism activities. The power system spreads over a wide area, and numerous transmission lines travel hundreds of miles from power generation to utilization sites. And these lines could easily be the targets of attackers. The substations are distributed over vast land, and most of them are unmanned, and physically poorly protected. They can easily be broken into and be damaged.

Actually both the cyberattacks and physical attacks against the power grid are not pure speculations, but are serious realities. For example, in January 2015, a militant attack plunged more than 140 million people into darkness after a key power transmission line was disrupted [7]. In January 2003, the Davis–Besse nuclear power station was infected by slammer worms, which resulted in the nuclear power plant being out of monitoring for five hours [8]. Also, in April 2016 the Gundremmingen nuclear power plant in German was reported to be infected by computer viruses [9]. These incidents could evolve into serious nuclear disasters if not well managed.

Moreover, it was identified by the security agency that a cyberattack caused a power blackout outside the U.S. [10]. On December 23 in 2015, a Ukrainian electricity distribution company was hacked, seven substations were isolated for three hours, and the operators were forced to switch to the manual mode. This cyberattack induced incident caused severe power outages to approximately 225,000 customers for hours [11]. Up to 73 MWh of electricity demand was curtailed. Also, it was reported that Israeli electric power system suffered severe cyber attacks [12].

Due to security and privacy reasons, insufficient details regarding these attacks were disclosed to the public. But it is possible that many such cyber related incidents were not revealed to the public, and such attacks could occur more frequently in the future with the smart grid initiative. It was reported that the power grid is actually under cyberattack minute-by-minute [13].

Furthermore, great power failures could be triggered if the attacker launches coordinated attacks to compromise multiple parts or functions of the power grid in cyber and physical aspects. And in a report by North American Electric Reliability Corporation, the coordinated attack was identified as one of the three representative high impact low frequency threats [14].

There have been some research papers studying power system vulnerabilities and attacks [15]-[16]. The targets and attacking methods could differ greatly. For example, the false data injection attack on the power gird generation control was modeled in [17], and a mitigation strategy was developed. A strategy to develop false data injection attacks without sufficient system knowledge was proposed in [18]. In [19] a cyber-physical security assessment technique considering both failures and malicious attacks was proposed. In [20] the vulnerabilities in the substations and the related attacks were studied. In [21] the authors studied how to coordinately switch multiple breakers to destabilize the power grid and cause large-scale cascading failures. In

[22] the authors investigated the cascading failure initiated by sequentially disconnecting multiple substations, and an attack strategy based on the sequential attack graph was proposed. In [23] the joint substation-transmission line vulnerability was studied, and a component interdependency graph based attack strategy was proposed.

However, the influence of the attacks on cyber-physical power grid reliability and the efficient defense strategies are lacking and need to be further explored.

1.2 Dissertation Objectives

This dissertation aims to study the impact of attacks on power system reliability, including intruding the substations, false data injection attacks as well as coordinated attacks. Based on the modeling of the attacks, different defense strategies are proposed for securing the power grid when an attack is anticipated. Specifically, a novel power grid operation strategy is proposed, which can improve the power grid robustness in case of malicious attacks. Also, a novel trilevel model is proposed considering uncertainties regarding the attacker's capability, the most critical branches that should be defended with priority is identified.

The major contributions of this dissertation are listed as follows.

- Proposed a holistic power grid reliability evaluation framework considering human dynamics based event frequency analysis and game-theoretic modeling for different attack cases;
- Developed a reliability evaluation method incorporating the false data injection attacks against state estimation.
- Studied several coordinated attack scenarios, and the optimal coordination strategy is studied with bilevel optimization.

- Derived a novel power system operation strategy for improving the power system's robustness against man-made attacks.
- Developed a MAS defender-attacker-defender modeling for identifying the critical branches with uncertainties of the attacker's capability.

1.3 Dissertation Organization

The rest of this dissertation is organized as follows. Chapter 2 studies the occurrence frequency of cyber attacks against power system substations, and investigates the impacts of different attacks scenarios on power system reliability. Chapter 3 studies the influence of false data injections on power system reliability. Chapter 4 studies how different attacks can be coordinated to maximize the damage. Chapter 5 proposes a robust power grid operation strategy for defending against malicious attacks. Chapter 6 proposes a MAS defender-attacker-defender model considering uncertainties to identify the most critical lines. Chapter 7 summarizes the dissertation and discusses the future research work.

2. Adequacy Evaluation of Power Grids Considering Substation Cyber Vulnerabilities

2.1 Introduction

Power system adequacy evaluation aims to assess the power system's capability of supplying electric power to the customers without interruption while fulfilling the operational constraints. Currently in the field of power system adequacy assessment, the main focus is placed on investigating the influences of intermittent renewable energy resources [24] and the communication infrastructure failures [25]-[29]. In [25]-[27], the influence of the failure of phasor measurement units and their optimal placement on power system adequacy were studied. In [28]-[29], the reliability of wide-area measurement system was investigated and approaches to improve the reliability were explored. However, the accurate evaluation of power system adequacy requires taking into consideration all possible outages and uncertainties [30]. With the wider deployment of information technologies, it is possible that cyber attacks will happen more frequently in the future. Thus, it is highly necessary to incorporate the cyber attacks induced risk into power system adequacy evaluation.

This chapter aims to investigate the power system adequacy incorporating substation cybersecurity. This research focus is associated with quantifying the impact of malicious cyber attacks on the overall power supply adequacy, while most of the aforementioned reliability assessment studies were focused on adequacy evaluation due to hardware failures. The adequacy analysis incorporating cyber attacks is very different from that based on random hardware failures, which is thus a particularly challenging task as explained in the following.

First, it is required to study the occurrence frequency of the cyber attack contingencies. The contingencies caused by hardware failures are considered as physical contingencies, and similarly the contingencies caused by malicious cyber attacks can be considered as cyber attack contingencies. The frequency of physical contingencies is mainly determined by the hardware's physical characteristics and the influence of the environment. But the frequency of cyber attack contingencies is mainly determined by the behaviors of malicious attackers, which involves a number of uncertainties. While sophisticated methods such as those based on Poisson distribution and state transition have been developed to study the frequency of physical contingencies, very little work has been conducted to statistically study the occurrence frequency of cyber attacks over a long time span [31]. This is primarily due to the unavailability of historical data coupled with privacy concerns. In this chapter, human dynamics analysis is adopted to study the occurrence frequency of cyber attack contingencies.

Second, it is essential to study the consequence of each contingency. The influence of the physical contingencies is determined by the function and location of the hardware and the control strategy of the power system operator; simply speaking, it is unilaterally determined by the defender. However, the influence of the cyber attack contingencies is determined by the attacker/defender interaction. It is an interactive process and more uncertainties are involved, such as the strategies, rationality and available budget resources of the agents, i.e., the attacker and the defender. In this study, game theory is applied to model the attacker/defender's interactive behaviors, and then to investigate the influence of each cyber attack contingency.

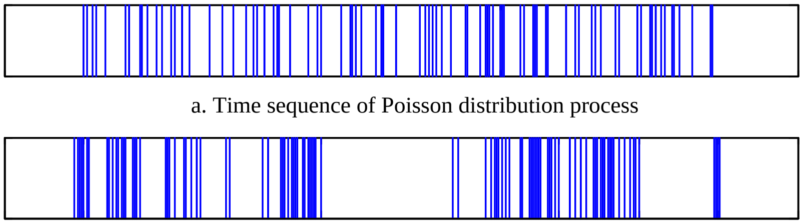
2.2 Human Dynamics Analysis for Cyber Attacks

In order to analyze the influence of a contributing factor of power outages on the long-term statistic power system adequacy, it is essential to study its occurrence pattern. Conventionally, the

Poisson distribution is adopted to model the failure of hardware components supported with the historical data. While it seems acceptable to assume that the cyber attack activities against power system could be simulated by Poisson distribution, many individual human activity temporal patterns were found to follow non-Poisson distributions, such as sending text messages, browsing webpages, and rating movies online [32], [33]. Similar temporal characteristics have also been captured in many collective social behaviors, e.g., wars and terrorism attack events [34], [35]. It is discovered that in these human activities the interevent intervals between two consecutive events are obviously not uniformly distributed. The time intervals are usually short, but there are also some non-negligible long intervals. By statistically analyzing the intervals τ, it is found that the probability $P(\tau)$ abides by the power law distribution:

$$P(\tau) \propto \tau^{-\alpha} \tag{2.1}$$

where α means the exponent, and it indicates the burstiness of the events. A larger value of the exponent indicates the burstiness of the event is more distributed.



a. Time sequence of Poisson distribution process

b. Time sequence of power law distribution process

Figure 2. 1 Comparison between Poisson and power law distributions

A comparison between Poisson distribution and power law distribution is illustrated in Fig. 2.1. Each vertical line in the figures represents a single event, and the mean values of the interval time are set to be the same. The sudden burst of a huge number of events in a short time period as well as inactivity within a long time period under power law distribution are more obvious than those in the Poisson distribution.

This study aims to develop appropriate methods instead of Poisson distribution to simulate the cyber attack occurrence pattern. However, until now very limited historical data about the cyber attacks targeting power grids are available to the public as the electric companies and utilities are concerned that the cyber attackers may take advantage of the data to increase their probability of launching successful cyber attacks. Also they have concerns on the loss of customers' confidence on their ability to provide high quality of service if these cyber incidents were released to the public. In this study, some real data [36] associated with the cybersecurity accidents are analyzed. These data record the detailed information on significant cyber attacks that occurred worldwide on a daily basis. The targets of attacks include electric power systems, governmental agencies, military units, finance sectors, transportation infrastructure, etc.

Since the exact occurrence moments of the attacks are missing, it is assumed that the attacks are randomly distributed over a day period if there are multiple attacks in a day. The occurrence pattern from April to September in 2012 is shown in Fig. 2.2 where each vertical line represents a single attack. It shows that the interval time between two successive attacks varies much. Sometimes multiple attacks may occur in a very short time period while there could be a long waiting period between two attacks.

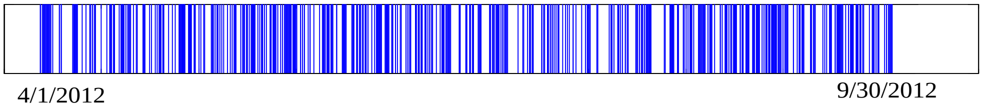


Figure 2. 2 The occurrence pattern of the cyber attacks

The probability and the interval time between attacks are shown in Fig. 2.3 based on the real-world data for cyber attacks from April 2012 to June 2014. It can be observed from Fig. 2.3 that the probability distribution of interval time between cyber attacks in real scenarios abides by the power law distribution. And the exponent can be obtained as α=1.68 using the curve-fitting technique with regression analysis.

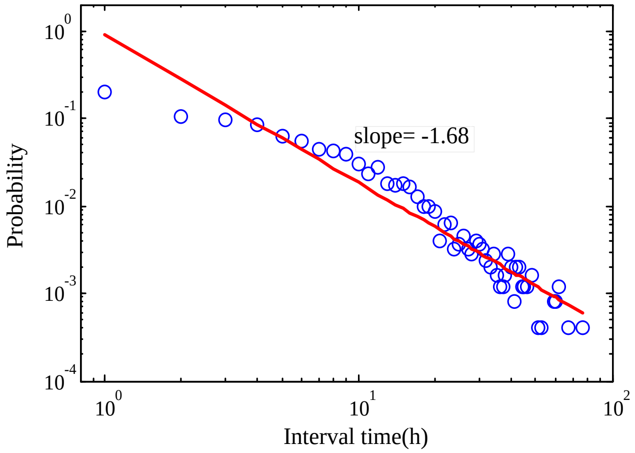


Figure 2. 3 The relationship between probability and cyber attack intervals

It is essential to investigate the social and psychological factors which drive the human behaviors. In order to interpret the statistical pattern of cyber attacks and to develop a mechanism for analyzing the cyber attack occurrence property, a human dynamics model can be built for cyber attacks, similar to those developed for mail communications based on queuing process in [37] and web access patterns using memory model in [38]. In [39], an opinion model considering memory effect was built to explain the pattern of terrorist attacks in Iraq and Afghanistan. Considering cyber attacks and terrorist attacks are both malicious attack activities to harm specific targets and cyber attacks initiated by the terrorists can also be seen as terrorist attacks, this study deploys the opinion model considering memory effect [34], [39] to model the pattern of cyber attacks against power system substations.

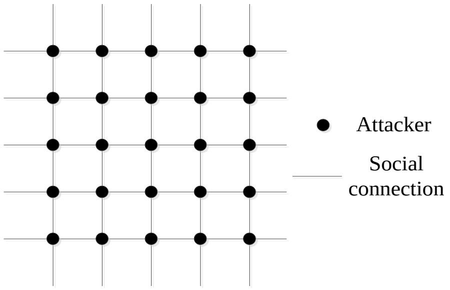


Figure 2. 4 Simple illustration of the cyber attacker society

As it is not possible to quantitatively model the complex human social network considering every detail, in this chapter a simplified graphical model is adopted to model cyber attacker society as shown in Fig. 2.4. The nodes represent attackers and the links represent social connections among them. Specifically, the attacker society is represented by an L×L two-dimensional lattice network, and every node at the conjunction represents an attacker. For the social connection, it is assumed that every node has certain social connections with its four neighboring nodes.

Just like different people have different opinions in a modern society, each individual in the cyber attacker society has an opinion about whether it is the right time to launch a cyber attack. At each moment, the individual opinion is represented by a parameter σ; and $\sigma = 1$ represents the supporting attitude while $\sigma = -1$ represents the opposing attitude. The opinions can change with time, which is influenced by two major factors, namely environmental effect and memory effect, due to the fact people's opinions or ideas are usually influenced by his/her own memory as well as others' opinions or ideas. The environmental effect is determined by the neighboring individuals, and at time *t* the environmental effect on the individual *i* is calculated by [34][39]

$$U_1(\sigma_{i,t}) = \sum_{j=1}^{4} \sigma_{i,t-1}\sigma_{j,t-1} (j = 1, 2, 3, 4) \tag{2.2}$$

Also, the memory effect is described by [34][39]

$$U_2(\sigma_{i,t}) = \begin{cases} 0.1 & \sigma_{i,t-1} \times \sigma_{i,t-2} \leq 0 \\ 1 & \sigma_{i,t-1} \times \sigma_{i,t-2} > 0 \end{cases} \tag{2.3}$$

The viewpoints of individuals can be updated as time goes on due to the influence of the environmental effect and the memory effect. The probability of changing ones' opinion is mathematically described as follows:

$$P(\sigma_{i,t}) = \begin{cases} \dfrac{1}{M}[\exp(-b_1 U_1) + \exp(-b_2 U_2)] & U_1 > 0 \\ \exp(-b_2 U_2) & U_1 \leq 0 \end{cases} \tag{2.4}$$

where b_1 indicates the social conformity psychology, and b_2 indicates the self-affirmation psychology, and M indicates the social chaotic degree.

Following the rules shown in (2.2)-(2.4), the cyber attacker society undergoes a self-organizing evolution. The collective opinion of the society is quantified by

$$m(t)=\frac{1}{L^2}\sum_{i=1}^{L^2}\sigma_{i,t},\quad \sigma_{i,t}\in\{-1,1\} \tag{2.5}$$

Analogous to the collective decision-making mechanism in the modern society, here it is assumed if *m* is higher than a critical set point m_c, the individuals in the cyber attacker society will reach a consensus to launch a cyber attack.

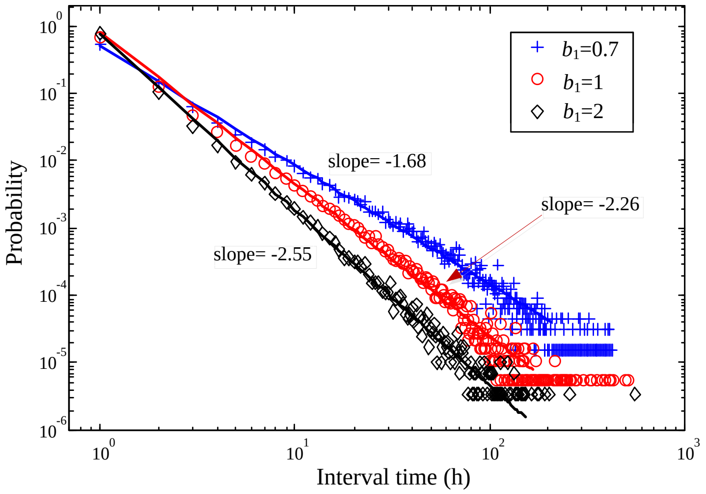


Figure 2. 5 The influence of social conformity psychology

Simulations are conducted to find the associated parameters for the real cyber attack data mentioned before. Since the social conformity psychology factor b_1 is a main factor influencing the power law exponent [39], specify L=10, M=2, b_2=0.7, m_c=0.7. And it is found when b_1 is 0.7, by applying curve-fitting the power law exponent it is obtained as 1.68, which matches the real data as shown in Fig. 2.5. It can be concluded that the increase of social conformity psychology factor b_1 leads to the increase of the power exponent α, which indicates that the cyber attacks occur more frequently.

To conclude, the main characteristics of the human society are incorporated in this human dynamics model, such as people, individual memory, social communication, and collective decision-making, etc. Although this model simplifies the cyber attacker society to some degree, it offers a quantitative way to statistically analyze the cyber attack occurrence pattern.

2.3 Cyber Vulnerabilities of Substations

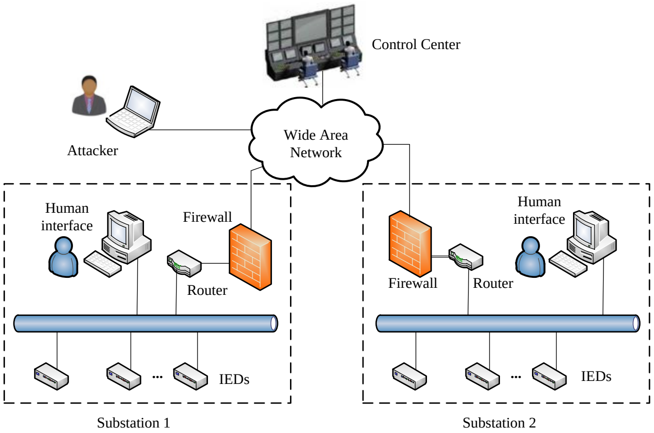


Figure 2. 6 Power system cyber architecture

A typical cyber architecture of a power system consists of control centers, SCADA network and substations, etc., as shown in Fig. 6. The substations and power plants are geographically distributed in a wide area, and they are connected with the control center. The power system dispatchers and operators working in control center monitors the operation statuses of field devices and control their operations.

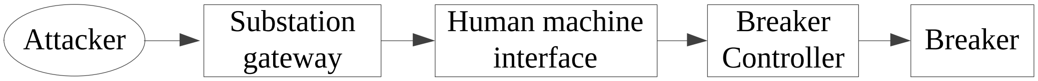


Figure 2. 7 An illustrative attack path

As substations are critical conjunction and control nodes in the power system network, they are usually well safeguarded from the malicious intrusions, and various countermeasures can be taken to further improve their cybersecurity level [40]. For example, firewalls and intrusion detection system (IDS) can be installed on the substation computers and the external gateways to detect the abnormal communication packets. Antivirus software can be installed to prevent the malware infection and propagation. Also, the vulnerabilities and holes in the operation systems, software, and system configurations are scanned and fixed. Password authentication, communication encryption and virtual private networks (VPNs) can be used to prevent unauthorized access and information leakage. As human is a critical part in the closed-loop system for enhancing the cybersecurity, employees should be trained to become more aware of the cybersecurity issues and strictly follow the stipulated cybersecurity regulations and policies. However, despite all these efforts cyber vulnerability induced risks remain in power system cyber networks. By exploiting the vulnerabilities in the operating system, passwords or protocols, a cyber attacker may successfully intrude into the substations and a possible attack path for controlling a breaker is presented in Fig. 2.7 [40], [41], and various detrimental activities could be performed such as tripping lines and shedding loads.

IDSs play a critical role in detecting and thwarting cyber intrusions. Generally, the performance gain of the IDS comes with the compromise of efficiency and it is difficult to achieve the high efficiency and high performance simultaneously. For example, an IDS could be capable of detecting malicious attacks or intrusion embedded in packet. However, continuously monitoring, recording and analyzing the packets consumes tremendous amounts of computational and storage resources, but the substation computers usually have limited memories and computing capabilities [42]. It is even more challenging to perform real-time monitoring and detection if the traffic load is heavy. And this is especially true when some faults or successful attacks occur, and in these cases the communication traffic between the substation and control center will increase tremendously, and the intensive monitoring of the traffic may cause the delay of transmitting critical operation commands and even incur serious consequence. And apparently, the operation of firewalls has the similar dilemma. So oftentimes an IDS features different operation modes: the lightweight mode and comprehensive mode. In the lightweight mode, only part of the packets is recorded and analyzed. In the comprehensive mode, all the packets in the traffic flow are analyzed. While the comprehensive mode features a higher probability of detecting the attack which is useful when an attack is ongoing, it may slow down the normal traffic for legitimate use and cause false positive alarms. So the IDSs usually work in the lightweight mode.

If a substation is under threat, in order to reinforce it the security operator could run the IDS of this substation in the comprehensive mode, while also enabling the IDSs in the SCADA network to focus on analyzing the traffic transmitted to/from the reinforced substation. Besides the IDSs, the security operator may remotely monitor and analyze the substation traffic, and even send staff to locally safeguard the substation if needed. All these actions could be taken so as to temporarily boost the cybersecurity level of the reinforced substation. Without loss of generality, denote the p_{aud} as the failure probability of a substation in the face of a cyber attack when the substation is not reinforced; similarly, denote p_{ad} as the failure probability of a substation in the event of attack when the substation is reinforced. It holds true that $0< p_{\text{ad}} < p_{\text{aud}} <1$ [42]. The specific values of p_{aud} and p_{ad} should be determined based on the evaluation of the experts or obtained from statistical cyber attack data.

Further, the consequence of a successful cyber attack will be quantified. The circuit breakers located in the substations can connect or disconnect a branch, a generator, and a load demand, etc. Undesired tripping or closing can directly impact the power flow, and may compromise the power supply reliability. The consequence will be disastrous if the attacker can take over the substation's human machine interface (HMI) and send false commands to trip all the breakers in the substation. In this case, all the lines, generators, and loads associated with the substation will be disconnected.

When a substation is down, the repair process will begin to recover the substation. And after a certain amount of repair time, the substation will recover. This repair process has an influence on the specific attack consequence, which is explained as follows.

The tripping of the substation circuit breakers can cause serious problems such as load loss, instability, or even complete system collapse. The specific consequence mainly depends on the system state at the time of the attack and the response of the system operator. Roughly, if the system is adequate in transmission and generation resources and the system operator responds in a timely manner and effective measures are taken, it is easy to prevent the system collapse. If the system is working in a marginal state and the system operator fails to take effective measures timely, the system would collapse.

From Fig. 2.1(b) and Fig. 2.2, it can be seen that in some cases certain attacks are individual ones as the intervals between them are quite long. A typical example of individual attacks is shown in Fig. 2.8. The interevent times between the attacks are more than the repair time. Prior to the next attack, the failed substations have recovered. At the moment of each attack, the system is operating with all the substations up. Also, it can be seen from Fig. 2.1(b) and Fig. 2.2 that in some other cases, multiple attacks burst in a short time and the interval times between them are quite short. These attacks are deemed consecutive attacks. A typical example of consecutive attacks is shown in Fig. 2.9. It can be found that the first attack occurs when no substation is down; and the second attack occurs when one substation is down before the down substation is restored; and at the moment of the third attack, two substations are down.

If the substation is disconnected and not recovered in time before the next attack occurs, the system will become increasingly vulnerable due to the loss of transmission and generation capacities, also the system operator will be under increasingly pressure and it is difficult for the operator to prevent system collapse at the moment of next attack. In summary, the consecutive attacks make the power system increasingly vulnerable to collapse. If this consecutive attack process goes on, the system will collapse at a certain time. The system collapse has been modeled by different methods in different studies, such as the convergence of the power flow analysis, the number of buses disconnected [43]. In this study, based on [43] assume that the power grid operator cannot prevent the system from collapsing if 10% of the substations are down.

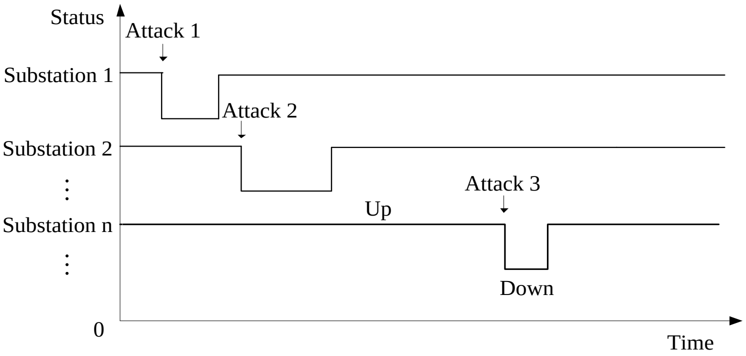


Figure 2. 8 Example of individual attacks

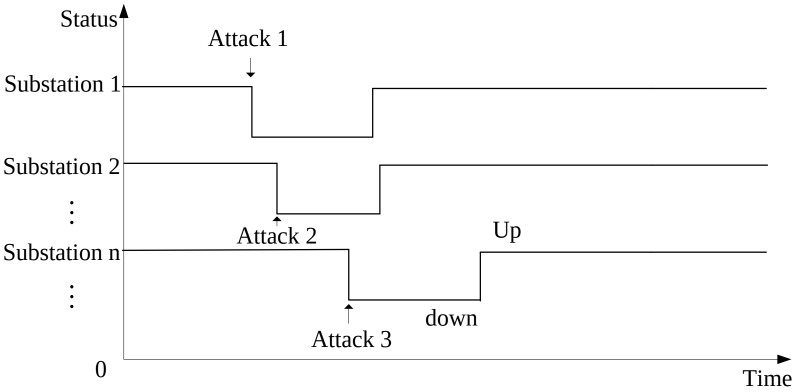


Figure 2. 9 Example of consecutive attacks

If the system does not collapse after one or more substations are brought down, the power system operator will take remedial measures to minimize the load curtailment in the remaining system. The minimum load curtailment l_m in the remaining network can be calculated by conducting the optimal power flow (OPF) analysis as described below:

$$l_m = \min \sum P_{c,i} \tag{2.6}$$

subject to:

$$P_{g\min} \le P_g \le P_{g\max} \tag{2.7}$$

$$0 \le P_{c,i} \le P_{d,i} \; (i \in N_B) \tag{2.8}$$

$$\sum_{i \in N_G} P_{g,i} + \sum_{i \in N_B} P_{c,i} = \sum_{i \in N_B} P_{d,i} \tag{2.9}$$

$$F = H \times (P_g + P_c - P_d) \tag{2.10}$$

$$|F| \le F_{\max} \tag{2.11}$$

where P_g is generation vector; P_c is the load vector; P_d is the load demand vector; N_B is the set of buses that have load demand; N_G is the set of buses that have generation; H is the connection matrix describing the relationship between branch power flow F and load/generation in the remaining network; $F_{\max}$ is the line transmission capacity vector.

If substation i is attacked successfully, the total load curtailment $l_s(i)$ is derived by

$$l_s(i) = l_d(i) + l_m(i) \tag{2.12}$$

where $l_d(i)$ is the load demand located in that attacked substation.

Similarly, the load curtailment can be calculated when more substations are down. Also, if the system collapses, the worst-case scenario will be considered where all loads will be curtailed.

2.4 A Game-Theoretic Approach

If the attack is launched in a time step, assume that with limited resources the attacker can only attack one substation because the contemporary power system is a critical infrastructure with enforced protection. Indeed it requires some level of intelligence and sophistication as well as adequate attack resources to attack the power network. On the defender's side, similarly assume that at each time step, the security operator can only choose a substation to reinforce as described in Chapter 2.3. Since each player needs to take into consideration the others' actions to maximize its payoff, the interactive optimal decision-making process is modeled based on game-theoretic approaches.

It should be noted that the attacker and defender interactions over a long period of time can be extremely complicated, so it is not realistic to model all these scenarios. In this study, two typical scenarios are modeled considering the cyber attack patterns. As shown in Fig. 2.9, the attack and protection interaction in this consecutive attack scenario could be a Markov process as the failed substation could not recover in time before the next attacks, and the next interactions could continue to cause the failure of other more substations. Since system collapse can bring great reward to the attacker, it is wise for the attacker to take into consideration the payoff of future attacks when making decisions in the current state, trying to cause system collapse with future attacks. Thus, the interactions in the sudden burst of consecutive cyber attacks should be modeled by a Markov game. For the individual attacks shown in Fig. 2.8, due to the recovery of the substations, the current attack will not coordinate with future attacks to cause system collapse, so a static game should be used to model the behaviors of the attacker and defender in this scenario.

2.4.1 The Markov Game

When the cyber attacker launches multiple attacks in a time period, the interaction between the attacker and the defender will continue with time, and this can generate a series of states which describes their respective optimized strategies. This series of interactions can be modeled by a Markov game, whose associated parameters are defined as follows [44], [45]:

- S: Set of the game states. Each single game state is a combination of the up/down statuses of all the related substations. When a substation goes down due to attack, it is denoted as 0; when it works normally, the status is denoted as 1. For example, if a small power system has 3 substations, the game state can be {1,1,1}, {1,1,0}, {1,0,1}, {1,0,0}, {0,1,1}, {0,1,0}, {0,0,1} or {0,0,0}. When the number of substations in a power grid is limited, the Markov game will be played in a finite state space.
- A: The player's action space. At each time step the attacker can attack one up-state substation, and the defender can reinforce one up-state substation. The attacker's attack action $a \in A_a$ indicates the substation chosen to hack. For the defender, the action $d \in A_d$ represents the substation that the defender chooses to reinforce.
- $MS(A)$: Mixed strategy set of the action set A. Each action $a \in A_a$ or $d \in A_d$ is assigned with a probability π_a or π_d with which the action a or d will be performed. For the attacker, $S(A_a) = [\pi_{a,1},\ \pi_{a,2}, \dots, \pi_{a,N_a}]$ and $\sum_{k=1}^{N_a} \pi_{a,k} = 1$ where N_a is the number of the up-state substations.
- T: State transition probabilities. p_{aud} is the failure probability of an unreinforced substation upon attack in a time step. p_{ad} is the failure probability of a reinforced substation when being attacked in a time step. These probabilities are modeled in Chapter 2.4. The cyber attack/defense interplay associated with the down-state substations is not considered.

The usual goal of a cyber attacker is to maximize the loss while a defender will try to minimize the damage. Thus, they have opposite goals and the attack/defense interaction should be modeled by a zero-sum game. A pair of actions $\{a, d\}$ in state s will result in an immediate payoff to the players due to the game state transitions. For the attacker, the reward is quantified as the curtailed load. Since the state transition exhibits probabilistic characteristics described by p_{ad} and p_{aud}, the immediate reward is also modeled in a probabilistic manner. An expected immediate reward of the attacker is defined as $R(s, a, d)$ when the attacker selects action a and defender selects action d in state s. The attacker's expected immediate reward is calculated by

$$R(s,a,d) = \sum_{s'} T(s,a,d,s') \times (l_s(s') - l_s(s)) \tag{2.13}$$

where s' indicates the possible next state; $T(s, a, d, s')$,T: $S \times A_d \times A_a \times S \rightarrow [0, 1]$ is the game state transition probability from s to s' when the attacker and defender take action a and action d, respectively. The transition probability is computed by the corresponding probabilities p_{aud} and p_{ad}, based on the pair of action $\{a, d\}$. The expected immediate reward of the defender is the opposite number of the attacker's expected immediate reward.

Every state transition will make the game move to a new state in which the game will continue. If a following state transition happens in the new state, another immediate reward will be given, and the game will continue. Thus, a pair of actions $\{a, d\}$ taken by the players in a game state can also have a long-term accumulated reward besides the immediate reward [44]. An expected long-term reward is defined as $Q(s, a, d)$ for the action pair $\{a, d\}$ in state s. Specifically, the attacker's expected long-term reward for the action pair {a, d} in state s is computed as follows:

$$Q(s,a,d) = \gamma \sum_{s'} T(s,a,d,s') \times V_a(s') + R(s,a,d) \tag{2.14}$$

where γ is the discount factor and satisfies $0 \leq \gamma \leq 1$, and a small value focuses on near-term reward while a large value emphasizes future long-term payoff; V_a (s) is the expected optimal long-term reward for the action pair $\{a, d\}$ in state s, which is defined as follows:

$$V_a(s) = \max_{\pi \in MS(A_a)} \min_{d \in A_d} \sum_{a \in A_a} Q(s,a,d)\pi_a \tag{2.15}$$

Similarly, the defender's expected optimal long-term reward in state s is represented as follows:

$$V_d(s) = \min_{\pi \in MS(A_d)} \max_{a \in A_a} \sum_{d \in A_d} Q(s,a,d)\pi_d \tag{2.16}$$

In zero-sum games, $V_a(s)$ and $V_d(s)$ calculated by (2.15) and (2.16) are the same, and it is denoted as $V(s) = V_a(s) = V_d(s)$. The optimal solutions computed independently by the attacker and the defender are the best strategies. In such Nash equilibrium, no players have the incentive to unilaterally change their strategies. The optimal mixed strategy obtained by (2.15) is a *maxmini* strategy considering Q which can be solved by linear programming [44]:

$$\max_{\pi \in MS(A_a)} V(s) \tag{2.17}$$

$$\text{s. t.} \quad \sum\nolimits_{a \in A_a} Q(s,a,d)\pi_a \geq V(s) \tag{2.18}$$

$$\sum\nolimits_{a \in A_a} \pi_a = 1 \tag{2.19}$$

$$\pi_a \geq 0 \tag{2.20}$$

A solution method named value iteration is adopted here to calculate the optimal Q and V as shown below [45]. The value iteration method is based on dynamic programming, and a *maxmini* problem is solved in each iteration as shown in step 7.

Algorithm 2.1 **Value iteration algorithm**

```
1: Initialize $V_0(s) = 0$ for all states $s \in S$
2: repeat
3:     for every $a \in A_a$, $d \in A_d$, $s \in S$
4:         update the value of $Q$ based on (2.14)
5:     end
6:     for every $s \in S$
7:         update the value of $V$ based on (2.15)
8:     end
9: until converge
```

2.4.2 The Static Game

When only considering the immediate reward in (2.13) and neglecting the future reward in (2.14), the game is a static game. For the attacker, it could be solved by

$$V_a(s) = \max_{\pi \in MS(A_a)} \min_{d \in A_d} \sum_{a \in A_a} R(s,a,d)\pi_a \tag{2.21}$$

Similarly, for the defender, it could be solved by

$$V_d(s) = \min_{\pi \in MS(A_d)} \max_{a \in A_a} \sum_{d \in A_d} R(s,a,d)\pi_d \tag{2.22}$$

For the solution of the static game, it should be noted that right after the first iteration of algorithm 1, the obtained mixed strategy is the optimal mixed strategy for the related static game without accounting for future rewards, and $V(s)$ is the reward in state s in static game.

2.5 Power System Adequacy Evaluation

Successful intrusion and undesired tripping of the breakers can seriously impact the power system operation. If such incidents happen frequently, the overall power system adequacy would be inevitably degraded. The impact of man-made cyber attacks on the long-term system adequacy is determined by the occurrence frequency of attacks over a long period of time and the consequence of each attack. The frequency of cyber attacks is simulated by human dynamics. The consequence of each attack is influenced by the defense/attack strategies and action of the defender/attacker, etc., which is modeled by game theoretic studies. When a cyber attack against the substation succeeds, the status of the components in the substation would go down due to the tripping of related breakers. If the attack causes a system collapse, the whole system could be down. When a substation becomes down due to the cyber attack, the repair process will begin and it will be up again after some repair time. The repair time mainly includes the time required for cyber forensics and the time needed for device restart [46]. The mean time to repair after attack is defined as MTTRA and used in the simulation in this study.

Two essential steps to incorporate physical failures and cyber attacks in power system adequacy evaluation are sampling states and evaluating the sampled states. The sampling process is shown in Fig. 2.10, where the top line represents the occurrence pattern of the cyber attacks based on the human dynamics described in Chapter 2.2, and each arrow indicates an attack is launched at that time step. The sampling of the generators and lines, etc. without the cyber attack is performed based on the reliability modeling of these physical components as in conventional adequacy assessment.

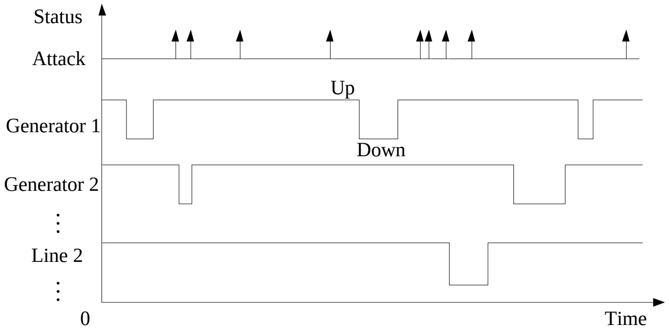


Figure 2. 10 Sampling of the attack occurrence and the component statuses

As shown in Fig. 2.11, the evaluation of a sampled system state is conducted considering the original components statuses, and the consequences of the attacks as well as the repair actions, etc. The consequence is determined by the attack/defense actions which are further determined by the attack/defense strategies. As described in Chapter 2.4, the attacker and the defender need to anticipate whether the attack is consecutive attack or static. The consecutive attack strategy modeled by the Markov game takes the future reward into consideration, while the static attack strategy modeled by the static game only accounts for the immediate reward. The judgment should be made by predicting whether sufficient amounts of attacks needed to cause system collapse will occur during the following repair time. For example, if the consecutive failure of three substations can cause a system collapse, the current attack should be judged to be consecutive attack if there are other two attacks in the following repair time. If there are only one or no attacks in the following repair time, it is not possible to cause system collapse, thus the current attack should be judged as individual attack. It is not an easy task for the attacker and defender to precisely predict future attack occurrence. These predictions could be made based on some social or political considerations.

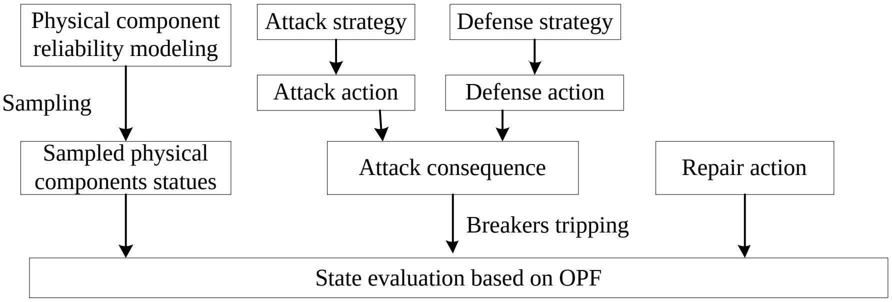


Figure 2. 11 Evaluation of system state

In this study, by extending conventional adequacy evaluation procedures [47], a holistic power system adequacy evaluation framework for integrating substation cyber vulnerabilities is proposed based on human dynamics analysis, game theoretic studies and sequential Monte Carlo Simulation (MCS). The major steps are depicted in Fig. 2.12, which are explained in more details as follows.

Step 1) Model the reliability characteristics of each physical component, including generators, transmission lines and loads, etc. Generate a time sequence of the status of each generator/line with sequential MCS.

Step 2) Generate a time sequence of cyber attacks using the opinion model considering the memory effect as described in Chapter 2.2.

Step 3) Model the cybersecurity of each substation. The cybersecurity of substations is modeled by p_{aud} and p_{ad}, as described in Chapter 2.3.

Step 4) Select an initial time step.

Step 5) For the current time step, check whether a cyber attack is sampled by examining the corresponding status in the time sequence of the cyber attack. If no attack is sampled, go to step 12.

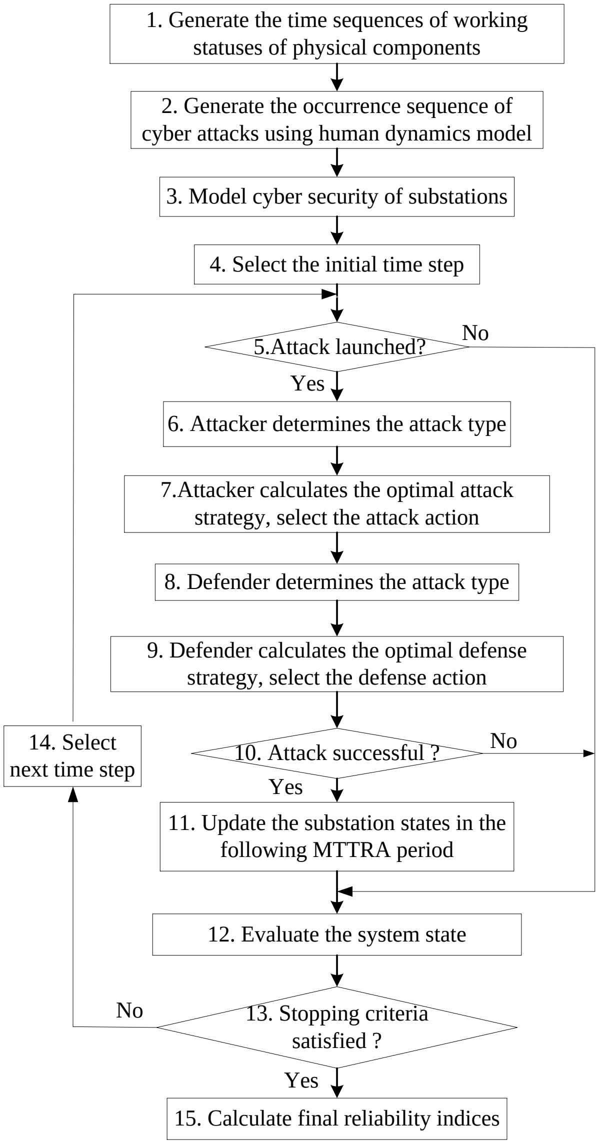

1. Generate the time sequences of working statuses of physical components
2. Generate the occurrence sequence of cyber attacks using human dynamics model
3. Model cyber security of substations
4. Select the initial time step
5.Attack launched?
No
Yes
6. Attacker determines the attack type
7.Attacker calculates the optimal attack strategy, select the attack action
8. Defender determines the attack type
9. Defender calculates the optimal defense strategy, select the defense action
14. Select next time step
10. Attack successful ?
No
Yes
11. Update the substation states in the following MTTRA period
12. Evaluate the system state
No
13. Stopping criteria satisfied ?
Yes
15. Calculate final reliability indices

Figure 2. 12 A holistic adequacy assessment framework considering cyber attacks against substations

Step 6) The attacker determines the attack type. If there are sufficient amounts of attacks within the repair time, the current attack should be considered as consecutive attack; or else the attack should be regarded as an individual attack. The attacker needs to predict future attacks and could make correct or wrong judgment.

Step 7) If the attack is judged to be consecutive, calculate the attacker's optimal strategy by equations (2.13)-(2.15); if it is judged to be the individual attack, calculate the attacker's optimal strategy by equations (2.13) and (2.21). The strategy can be a pure or a mixed one.

The attacker's action is implemented by using a random number generator to choose the target substation to attack.

Step 8) Similar to step 6, the defender makes predictions about future attacks and estimates the attack type. The defender could make a correct or wrong judgment.

Step 9) If the attack is judged to be a consecutive attack, calculate the defender's optimal strategy by (2.13), (2.14) and (2.16); otherwise, calculate the defender's optimal strategy by (2.13) and (2.22). A random number generator is utilized to choose the defense action.

Step 10) Check whether the attack is successful or not based on both the pair of action $\{a, d\}$ obtained in step 7 and 8 and the probabilities p_{aud} and p_{ad}. The attack can succeed with a probability, and thus a random number generator is used to decide consequence. If the attack is not successful, go to step 12, otherwise, go to the next step.

Step 11) Update the substation states corresponding to the game state. If a substation is hacked down, the worst-case scenario is considered, i.e., all the breakers are assumed to be tripped. Since a down-state substation generally requires a time period of MTTRA to recover, the statuses of the components affected by the down-state substation will be down in this time period.

Step 12) Evaluate the physical system state. This is accomplished by performing the DC OPF analysis aiming at minimizing the total load curtailment at all buses.

Step 13) Check whether the stopping criterion is met. In the simulation, the maximum number of iterations is used as the stopping criterion which should be adequately large to ensure the convergence.

Step 14) Select the next time step since the attack/defense and repair are sequential.

Step 15) Calculate the final adequacy indices. In this study, the adopted reliability indices are LOLP and EENS.

2.6 Case Studies

Simulations studies are carried out on the IEEE RTS79 system [48]. The RTS79 system has 32 generators and 38 transmission lines. The total generation capacity is 3,405 MW and the peak load demand is 2,850 MW. For simplicity, it is assumed that each substation is related to one bus. There are 24 substations in the RTS79 system. Since some substations are relatively more important than others, they could be the main targets for the attack/defense action. In order to reduce the number of Markov game states and alleviate the computing burden, the top 10 substations are chosen as the attack/defense target substations. The computational accuracy is not significantly affected by this because the probabilities of attacking the relatively less important substations are very low, which will be shown later in Fig. 2.13. The load curtailments in the substation are listed in Table 2.1.

Table 2. 1 Load curtailment caused by substation failure

Substation number	3	6	8	9	10	13	14	15	18	19
Load curtailment (MW)	180	136	171	175	195	265	194	317	333	181

In this simulation, the parameters for modeling the cybersecurity of all the substations are chosen as follows: p_{aud}=0.15 and p_{ad}=0.1. Game payoffs are calculated based on these probabilities. For example, when all the substations are in the up state, the payoff matrix of the static game in terms of MW is shown in Table 2.2 and the payoff matrix for the Markov game is illustrated in Table 2.3 where γ =0.7. The discount factor γ prefers a large value as the Markov game aims at causing system collapse.

Table 2. 2 Payoffs of static game when all substations are up

		Attacked Substation									
		3	6	8	9	10	13	14	15	18	19
Reinforced Substation	3	18	20.4	25.7	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	6	27	13.6	25.7	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	8	27	20.4	17.1	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	9	27	20.4	25.7	17.5	29.3	39.8	29.1	47.6	49.9	27.2
	10	27	20.4	25.7	26.3	19.5	39.8	29.1	47.6	49.9	27.2
	13	27	20.4	25.7	26.3	29.3	26.5	29.1	47.6	49.9	27.2
	14	27	20.4	25.7	26.3	29.3	39.8	19.4	47.6	49.9	27.2
	15	27	20.4	25.7	26.3	29.3	39.8	29.1	31.7	49.9	27.2
	18	27	20.4	25.7	26.3	29.3	39.8	29.1	47.6	33.3	27.2
	19	27	20.4	25.7	26.3	29.3	39.8	29.1	47.6	49.9	18.1

Table 2. 3 Payoffs of Markov game when all substations are up

		Attacked Substation									
		3	6	8	9	10	13	14	15	18	19
Reinforced Substation	3	18	20.4	25.7	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	6	27	13.6	25.7	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	8	27	20.4	17.1	26.3	29.3	39.8	29.1	47.6	49.9	27.2
	9	27	20.4	25.7	17.5	29.3	39.8	29.1	47.6	49.9	27.2
	10	27	20.4	25.7	26.3	19.5	39.8	29.1	47.6	49.9	27.2
	13	27	20.4	25.7	26.3	29.3	26.5	29.1	47.6	49.9	27.2
	14	27	20.4	25.7	26.3	29.3	39.8	19.4	47.6	49.9	27.2
	15	27	20.4	25.7	26.3	29.3	39.8	29.1	31.7	49.9	27.2
	18	27	20.4	25.7	26.3	29.3	39.8	29.1	47.6	33.3	27.2
	19	27	20.4	25.7	26.3	29.3	39.8	29.1	47.6	49.9	18.1

The strategies of the attacker and defender under different scenarios are shown in Fig. 2.13. It shows that when future rewards are not considered, the main targets of the attacker are substations 15 and 18. When future rewards are considered, the probability of attacking substation 13 is greatly increased, and the probability of defending substation 13 is also increased correspondingly. In both cases, the probabilities for attacking and defending other substations are very small which are thus not shown in Fig. 2.13.

The simulation for assessing the power grid adequacy is conducted and the final outcome is shown in Table 2.4 where the human dynamics parameters are chosen as L=10, M=2, b_1=0.7, b_2=0.7, m_c=0.7 and under these parameters, the power law exponent is the same as the real data. The simulation is conducted in Matlab using a laptop with 8 GB memory and four cores of 2.90 GHz. It takes 14 minutes to finish the Monto Carlo simulation to obtain the desired reliability indices. For the simulation outcomes shown in Table 2.4, assume that attacker and defenders can always make the right judgment about the attack type. These parameters and assumptions serve as the baseline of the following four types of sensitivity analysis.

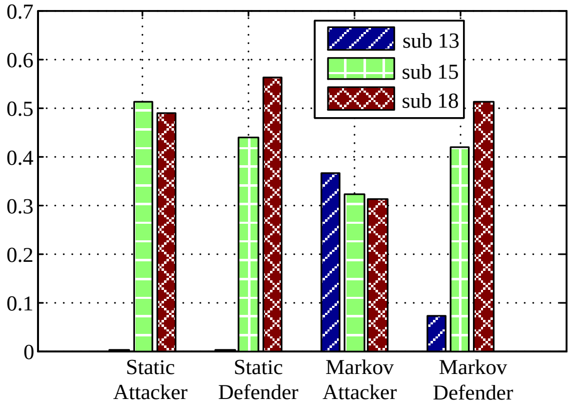


Figure 2. 13 Optimal mixed strategies for the players when all substations are up

Table 2. 4 System adequacy comparison with and without cyber attacks

Scenario	LOLP	EENS (MWh)
Without cyber attack	0.083	1.32E+05
With cyber attack	0.100	2.28E+05

The results in Table 2.4 show that the LOLP and EENS increase significantly considering cyber attacks and it demonstrates that cyber attacks may greatly compromise the overall adequacy of the power system.

2.6.1 Influence of the Judgment of the Attack Type

In the step 6 and step 8 of the adequacy assessment process in Fig. 2.12, the attacker and the defender need to make judgments about whether the attack type is consecutive or individual. Since the judgments influence the strategies and thus the attack/defense actions, its influence is studied and several scenarios are examined.

Scenario 1: Both the attacker and the defender can always make the right judgments.

Scenario 2: The attacker always makes the right judgment, but the defender always treats the attack type as individual one.

Scenario 3: Both the attacker and the defender always treat the attack as individual one.

Scenario 4: The attacker always makes the right judgment, and the defender randomly chooses one up-state substation to reinforce with equal probabilities.

Since most of the attacks are individual ones, this study do not consider the scenario when both the attacker and the defender always treat the attacks as consecutive ones. The system adequacy indices in these scenarios are shown in Fig. 2.14.

Comparing scenarios 1 and 4, it can be seen that the defender should adopt the game-theoretic approach to make the informed defense strategy, or else the consequence could be disastrous. Comparing scenarios 1 and 2, it is indicated that if the defender fails to make the right decision, the misjudgment and the deployment of non-optimal strategies would lead to decreased system adequacy. Comparing scenarios 1 and 3, it can be seen if the attacker always makes the right judgment, the adequacy of the power system will be degraded.

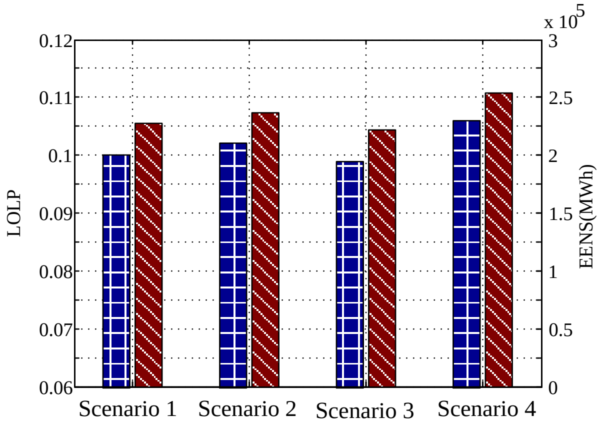


Figure 2. 14 Comparison of attack type judgment

2.6.2 **Influence of the Human Dynamics**

The cyber attack occurrence is checked in every time step as in step 5 of the adequacy assessment procedure in Fig. 2.12. The human dynamics analysis determines the cyber attack occurrence pattern, which is an essential factor influencing the long-term adequacy of the power system. To examine the influence of human dynamics, values of the social conformity psychology factor b_1 are varied while other factors and parameters remain unchanged. The obtained results are shown in Fig. 2.15.

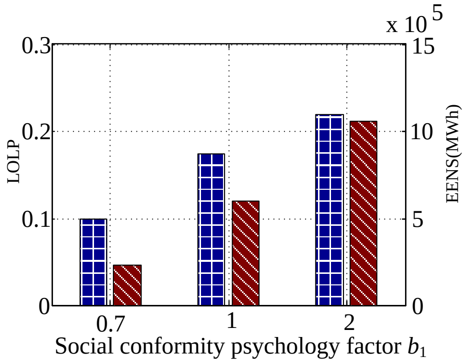


Figure 2. 15 Influence of social conformity psychology on system adequacy

It shows the LOLP and EENS indices both increase with the increase of the value of social conformity psychology factor b_1. It indicates that if some social means such as education could be implemented to decrease the occurrence number of cyber attacks initiated by the attackers, the power grid adequacy can be maintained.

2.6.3 Influence of the Cybersecurity Parameters

The failure probabilities of the substation p_{aud} and p_{ad} describe the cybersecurity level of the substations, which play a key role in power grid long-term adequacy evaluation as indicated in steps 7, 9 and 10 of the Fig. 2.12.

If the initial cybersecurity levels of all substations are the same, the influence of p_{aud} and p_{ad} on the power system adequacy is studied as shown in Fig. 2.16 and Fig. 2.17, respectively. It indicates that if the cyber security level of the power system is low, the power system adequacy will be greatly impacted as the success probability of cyber attacks is high.

Usually there are multiple substations in a bulk power grid. Although they are all important and should be safeguarded, it is crucial to identify the most critical substations to receive the budget which is usually limited. Thus, it is meaningful to study the influence of the cybersecurity level of individual substation on the overall power system adequacy for identifying the most critical substations. Simulations are conducted by specifying p_{aud}=0.1, p_{ad}=0.05 for a chosen substation while for all other substations it remains p_{aud}=0.15 and p_{ad}=0.1. The simulation results are displayed in Fig. 2.18. It can be seen that the cybersecurity levels of some substations are more critical to the overall power system adequacy than others. If the budget is limited, these security-critical substations should be given the priority for receiving the investment resources.

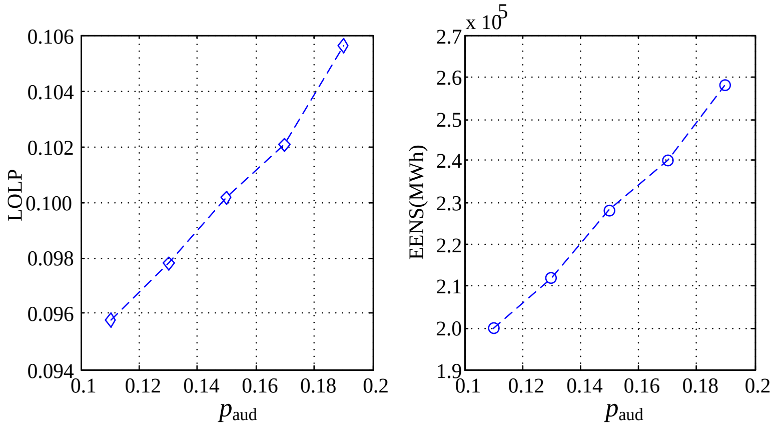


Figure 2. 16 Influence of p_{aud} on system adequacy

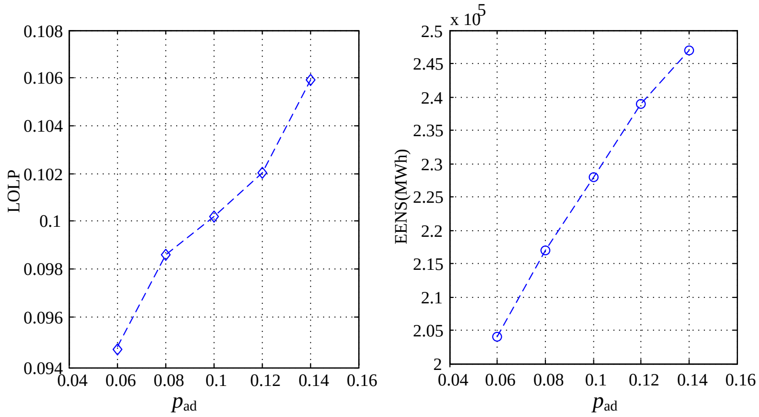


Figure 2. 17 Influence of p_{ad} on system adequacy

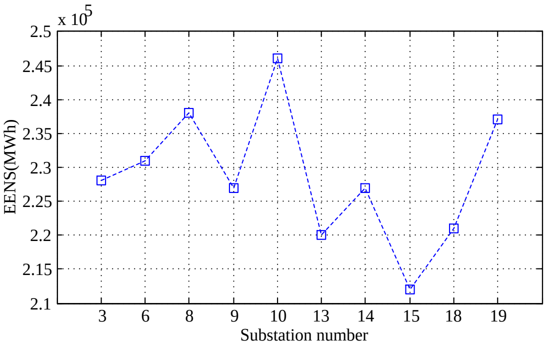


Figure 2. 18 Influence of individual substation cybersecurity on system adequacy

2.6.4 Influence of the Repair Time

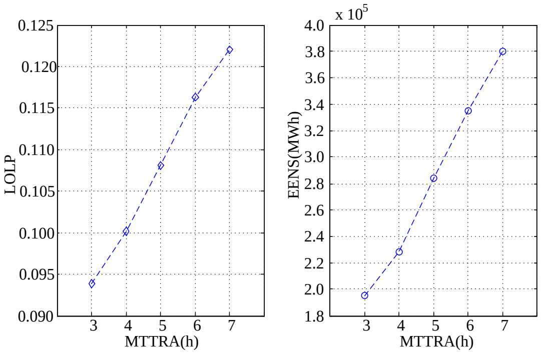


Figure 2. 19 Influence of MTTRA on system adequacy

The substation repair time have a great influence on power system adequacy as indicated in step 11 of Fig. 2.12. If an attacked substation is soon recovered, the failure time will be less and thus the power loss is decreased. The influence of MTTRA on the power grid adequacy is studied as shown in Fig. 2.19. It demonstrates that the increased repair time leads to the degraded power system adequacy. The simulation results suggest that the capability of restoring the power system after a successful cyber attack should be enhanced through developing appropriate investment plans.

2.7 Conclusions

The chapter was focused on proposing a holistic power system adequacy evaluation framework to incorporate the impact of substation cyber vulnerabilities into the conventional power system adequacy evaluation framework. To this end, two essential studies were conducted: the statistical occurrence patterns of the cyber attacks were analyzed based on historical cybersecurity data and human dynamics analysis; the consequence brought about by the cyber attacks was analyzed based on game-theoretic studies, i.e., Markov game for consecutive attacks and static game for individual attacks. In the proposed adequacy evaluation framework for cyber-physical power systems, the incidents caused by random physical failures and man-made cyber attacks were considered simultaneously. Simulation studies were conducted based on a representative IEEE reliability test system, and the influences of critical factors and parameters were analyzed. The results showed that substation cybersecurity risks should not be ignored in power system planning and operations.

3. Power System Reliability Evaluation Considering Load Redistribution Attacks

3.1 Introduction

The reliable operation of the power system relies on not only the working status of the current-carrying elements (such as generators, lines, transformers, buses), but also the state awareness of the power grid. The operator needs to be aware of the power system's status, so that they can dispatch the power, and response to contingencies. The state estimation plays a key role in ensuring the status awareness. When measurements are sent to the control center, the state estimator will estimate the state of the power grid based on those measurement.

In the past, if the cyber attacks on the measurements are not considered, the state estimation is usually reliable and can be trusted. However, the cyber vulnerability in the power grid is a big concern nowadays [49]. And it is found that by attacking multiple measurements in a coordinated manner, the attacker can manipulate the state estimation results. This attack is named false data injection attack [50]. Further, the load redistribution attack model [51] is proposed, which is more practical, as the generator measurements are not attacked.

If such attacks against the state estimation becomes frequent in the future, it is possible that the long-term power grid reliability is severely impaired, thus, it is critical to include the load redistribution attacks into the power grid reliability evaluation.

3.2 Intrusion Process Modeling for MITM Attack Against State Estimation

3.2.1 Attacks against Power System State Estimation

If the attacker aims to change the outcome of the state estimation, he/she needs to manipulate the measurement inputs of the state estimator. Practically speaking, the attacker can alter the measurements in the following ways by: compromising the voltage or current meters in substations; attacking the remote terminal units in the substations; tampering with the heterogeneous SCADA network; and intruding into the control center. The meters, RTUs, SCADA network and EMS are where the measurements are generated, collected, transmitted and received, respectively. Attacking the meters or RTUs can be achieved by both physical or cyber approaches, but it demands compromising numerous measurements located in various substations in a coordinated manner to successfully alter the outcome of state estimation. This is because the measurement inputs of the state estimator feature redundancy and inconsistency could be detected. The control center is usually well safeguarded, and it is very difficult to intrude into the control center. The SCADA network is widely distributed over a wide area, and there can be multiple vulnerabilities in the system configuration and in the protocols. Thus, it is relatively more practical for the attacker to tamper with the measurements in their transmission process despite it is still difficult and requires tremendous skill and effort.

An attack tree is illustrated in Fig. 3. 1, which consists of attacks against the substations, the hierarchical SCADA network and the control center. These combinations can result in a successful false data injection attack against state estimation. Specifically, in order to attack the SCADA network, three possible attack procedures should be performed by exploiting various vulnerabilities in devices and networks. The attacker needs to intrude into a node in the SCADA network, and gain the trust of the substations and the control center. In addition, if the communication is encrypted, cracking the encryption is needed.

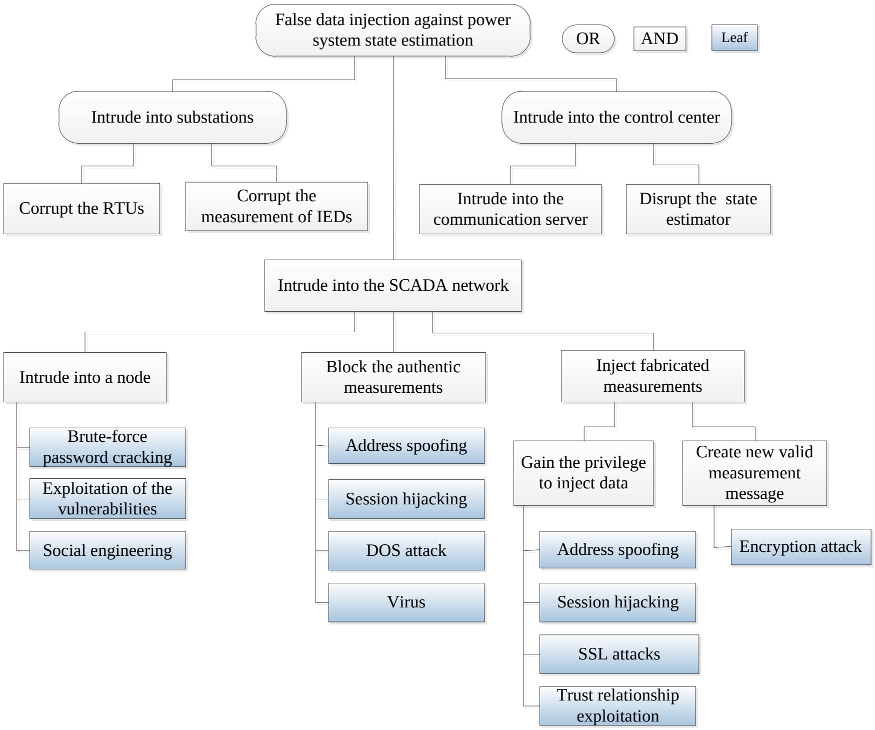

False data injection against power system state estimation
OR
AND
Leaf
Intrude into substations
Intrude into the control center
Corrupt the RTUs
Corrupt the measurement of IEDs
Intrude into the communication server
Disrupt the state estimator
Intrude into the SCADA network
Intrude into a node
Block the authentic measurements
Inject fabricated measurements
Brute-force password cracking
Exploitation of the vulnerabilities
Social engineering
Address spoofing
Session hijacking
DOS attack
Virus
Gain the privilege to inject data
Create new valid measurement message
Address spoofing
Session hijacking
SSL attacks
Trust relationship exploitation
Encryption attack

Figure 3. 1 Attack tree for the state estimation

3.2.2 Attack against Non-encrypted SCADA Network

The principle of altering the measurements in the transmission process can be described as shown in Fig. 3. 2.

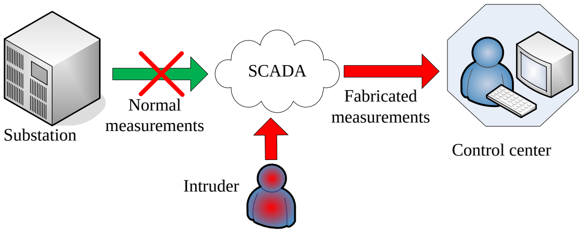


Figure 3. 2 Illustration of the attack

Generally, the attack against the measurements in the cyber-physical power grid involves three major steps/phases, which are described as follows:

(1) First, the attacker gains the privilege to get the access to a communication host in the SCADA network and installs malicious intrusion tools on it. The target host should be a critical

host that the transmitted measurements need to travel through, or the attacker needs to poison the route table to reroute the traffic. Multiple methods are available for the attacker to gain the privilege and control the target host, such as exploiting the vulnerabilities in the target host, cracking the password, or stealing the password via social engineering.

(2) Next, the attacker gains the trust of the substations. While the substations send communication request to the control center, the attacker in the SCADA network keeps monitoring the network traffic and waits for the information sent from the substations to the control center. The trust can be gained by spoofing the IP address of the control center and replying fake DNS response to the substations. After the victim host gains the trust of the substations, the connection between the substation and the victim host can be established.

(3) In order to gain the trust of the control center, the attacker establishes the connection between the victim host and the communication server in the control center. This can be accomplished by sending the fabricated certificate of the victim host to the control center. After completing these steps, the communication between the control center and substations can be monitored and maliciously modified by the attacker.

As described above, the intrusion process consists of a series of consequential fundamental attack phases. The attack will not be successful until all the fundamental attack phases are successful. At each attack phase, the attacker needs to exploit the vulnerabilities in the SCADA network to improve its privilege. After a successful attack phase the system will transit to a new state. The power system cyber layer is protected by the cyber security countermeasures such as firewalls and intrusion detection systems (IDSs). At each attack phase, if the vulnerabilities are detected and patched before the attacker can discover and exploit these vulnerabilities, the attack phase will not be successful and the system will return to the secure condition; or it will proceed to the next attack phase. This attack/defense process repeats until the system state reaches one of the two specific states: secure state or failure state. For gaining a better understanding, the interaction in the intrusion process is modeled by two competing agents, the attack agent and the detection agent with the opposite goals. The attack agent refers to the attacker and it aims to compromise the state estimation outcome. The detection agent includes the comprehensive behaviors of the firewall, IDS and security operator and it tries to detect the attack and protect the system.

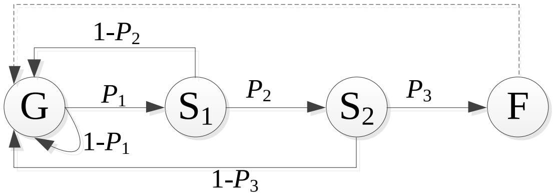


Figure 3. 3 Semi-Markov model for attack against non-encrypted SCADA

The semi-Markov process (SMP) model is widely used to model various stochastic intrusion processes [52]-[54]. An SMP is an extension of the conventional Markov process, and they share some similarities as they are both represented by a set of states and the associated transition probabilities between the states. The SMP significantly differs from the Markov process, as the sojourn time spent on each state, the occurrence of the state transition, and the transition probabilities do not need to be fixed, but can follow a probability density function [55]. Thus, the SMP is capable of generalizing various kinds of stochastic processes and modeling the stochastic process with non-exponential distributions for the state transition probabilities.

The state transition is described by an SMP in Fig. 3.3. As seen from Fig. 3.3, three major steps are required to accomplish a successful false data injection attack, which correspond to attacking the communication host, gaining trust for the substations and gaining trust of the control center, respectively.

By making the failure state the absorbing state [56], the time required to reach the absorbing state can be calculated, which is denoted as the mean time to attack (MTTA). Initially the system is in the secure state G in which no attack phase is successful. The attacker needs to succeed in three successive steps to finally execute a successful false data injection. Depending upon the success of each step, the system will transit to a new state. If the attacker succeeds in step 1, the system will transit to state S_1, and the success probability of step 1 is P_1. Similarly, after step 2 is successfully executed, the system will transit to state S_2, and the associated success probability of step 2 is P_2. After the successful step 3, the whole attack is accomplished, and the system will move to state *F*. Thus, state *F* is an absorbing state which indicates the end of all the attack steps. All the other steps are transient states as in case the attackers fail in the step, the attack steps will restart from state G. In summary, in the model shown in Fig. 3.3, the failure state *F* is the absorbing state while all other states {G, S_1, S_2} are transient states. The resultant transition probability *U* can be described as the following general form:

$$U = \begin{bmatrix} Q & B \\ 0 & I \end{bmatrix} \tag{3.1}$$

where submatrix *Q* is the transition probabilities within the transient states, and submatrix B is the transition probabilities from transient states to absorbing states [53]. Matrix *Q* is given by

$$Q = \begin{array}{c|ccc} & G & S_1 & S_2 \\ \hline G & 1 - P_1 & P_1 & 0 \\ S_1 & 1 - P_2 & 0 & P_2 \\ S_2 & 1 - P_3 & 0 & 0 \end{array} \tag{3.2}$$

3.2.3 Attack against Encrypted SCADA Network

If the communication between the substations and the control center adopts some more secure protocols such as secure DNP3 (Distributed Network Protocol) and IEC 61850 standards, the difficulty for the attacker will greatly increase. However, secured communication protocols may still be compromised. Absolute security cannot be ensured for the communication between the substations and the control center using cryptographic signatures and passwords in the communication protocols. This is because vulnerabilities exist in protocols, public and private keys management, as well as in the cryptographic software and algorithms [57].

Two specific examples are provided here. For example, a secure DNP3 protocol [58] termed DNPsec can be used to improve the security of DNP3. It adopts multiple authentication and encryption algorithms such as Triple Data Encryption Standard (3-DES), and keyed-Hash Message Authentication Code with Secure Hash Algorithm (SHA). However, 3-DES and SHA-1 are seen as outdated and insecure algorithms [59]-[60]. If the encryption is cracked, the communication would become vulnerable [61]. In [62], it is experimentally verified that the deployment of encrypted channels and authentication methods including secured DNP is vulnerable if the master device is infected by malwares. Further, for instance, a number of attack schemes have been designed targeting encryption algorithms of the Global System for Mobile Communications (GSM) network, such as cipher-text-only attack on GSM encryption algorithm A5/2. A few milliseconds are needed to interpret the encrypted information by the attack on A5/2, and the encryption key used for error correction can be recovered in one second. By using the encryption attacks, the attacker could eavesdrop the communication between the mobile station and the network as well as insert and modify data. The false base station is embedded into a GSM network, and the attacker intercepts and modifies the transmitted information among the channels. As the attacker is able to keep the fake station connected to destination networks by broadcasting the network number, the fake base station can be used to resend the identity information received from the mobile station. With the encryption attacks such as A5/2 attack, the attacker is able to disable the encryption between the fake station and the targeted network as well as the encryption between the mobile station and the fake station [63].

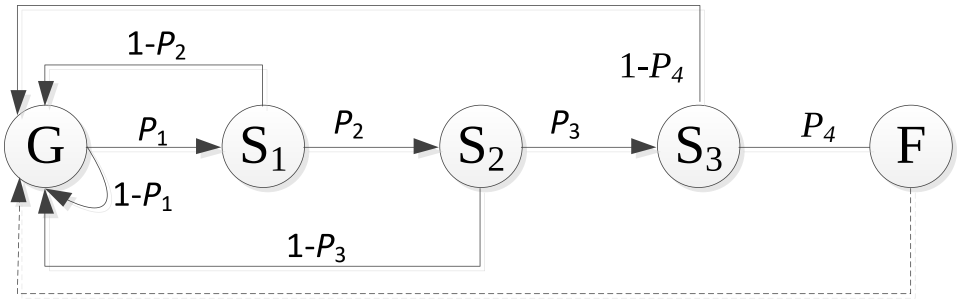


Figure 3. 4 Semi-Markov model for attack against encrypted SCADA

The vulnerabilities in the encryption have been widely studied. In [64], a practical encryption attack which targets the cryptographic protocol is presented. The cryptographic protocol can be cracked within about 150 minutes with the successful rate more than 95%. Even if more advanced cryptographic protocols are proposed and used in encrypted communications, various vulnerabilities are being identified and encrypted information could be interpreted and modified [65]. There can be several cryptographic vulnerabilities in the secure sockets layer (SSL) in the SCADA communication, such as weaknesses in the generation and seeding of the random number and cipher weaknesses. Theoretically, it is possible for the attacker to pass the MAC authentication adopted by the control center and RTUs in an SSL exchange. The attacker needs to successfully modify the handshake messages. The SSL can be compromised by intercepting the real key and substituting it with a false key during the key exchange sessions. Also, similar to other applications, SSL is vulnerable to viruses and worms. A typical example is the Slapper Worm [66].

In summary, as vulnerabilities exist in the encryption, the SCADA network using the secure protocols or encryption can still be compromised. The influence of the secure protocols is mainly represented by the increase of number of steps during attacks. Due to the encryption, the attacker needs to spend extra effort in cracking the encryption. The attack steps are shown in Fig. 3.4 and explained as follows:

(1) The attacker intrudes into the SCADA network and compromises a host of the network. After this step, the attacker will be able to intercept the measurements which are being sent from the measurements to the control center.

(2) The attacker needs to make effort to crack the encryption. For example, the attacker can use the deciphering tool to obtain the plaintext of the transmitted information.

(3) The attacker pretends to be the control center when communicating with the substations. After gaining the trust, the attacker drops the measurements which are sent from the substations.

(4) The attacker pretends to be the substations when communicating with the control center. After gaining the trust of the control center, the attacker could fabricate fake measurements and send them to the control center.

$$Q = \begin{array}{c} \\ G \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{cccc} G & S_1 & S_2 & S_3 \end{array} \\ \begin{bmatrix} 1-P_1 & P_1 & 0 & 0 \\ 1-P_2 & 0 & P_2 & 0 \\ 1-P_3 & 0 & 0 & P_3 \\ 1-P_4 & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{3.3}$$

Steps 1, 3 and 4 in the above procedure correspond to steps 1, 2 and 3 in the procedure discussed in Chapter 3.2, and step 2 is related to the effort made for cracking the encryption. While it is not trivial to accomplish this step, an advanced, intelligent attacker could crack the encryption. Similar to equation (3.2), the transition probabilities in this case are obtained based on Fig. 3.4, as represented by equation (3.3).

3.2.4 Calculation of MTTA

This chapter is focused on analyzing the power system reliability incorporating false data injection attacks. A key factor is to model the occurrence of the attacks, or the time interval between successful attacks. It is critical to model the overall time required to reach the final failure state, as in the transient states no fake measurements can be sent to the control center. To quantify the security of the SCADA system, the MTTA is applied to model the mean time required to go from the secure state to the failure state. The MTTA refers to the statistical value of the time and it statistically analyze the behavior of multiple attackers and defenders within a long range of time while the specific time of each attack may vary.

It is obvious that at each attack phase, the attack agent needs to spend a certain amount of time to obtain a new privilege. On the other side, the detection agent also needs to spend some time to detect the intrusion. In this study, the attack/defense time is modeled by nonnegative variables following a reasonable distribution. Let X_i denote the attack time needed for the attack agent to succeed in the *i*-th fundamental intrusion phase and it is assumed that X_i is a random variable uniformly distributed over the corresponding interval. It is described as $X_i \sim U[T_{a,i}^{min}, T_{a,i}^{max},]$ where $T_{\mathrm{a,i}}^{\mathrm{min}}$ and $T_{\mathrm{a,i}}^{\mathrm{max}}$ are the lower and upper bounds for the attack time of the *i*-th attack phase, respectively [53]. And the density function of the attack time for the *i*-th attack phase is represented by:

$$f(X_i) = \begin{cases} \frac{1}{T_{a,i}^{max} - T_{a,i}^{min}} & T_{a,i}^{min} < X_i < T_{a,i}^{max} \\ 0 & otherwise \end{cases} \tag{3.4}$$

Similarly, let Y_i denote the detection time needed for the detection agent to detect the attack action at the *i*-th attack phase. Y_i is also described by a uniform distribution time interval, and this defense time interval should be appropriately chosen to represent the interaction between the attack agent and the detection agent. It is obvious that there is a nonzero probability that the detection agent can detect the attack before the attack phase is finished. To represent this idea, the detection time is represented as $Y_{\mathrm{i}} \sim U[T_{\mathrm{d,i}}^{\mathrm{min}}, T_{\mathrm{a,i}}^{\mathrm{max}}]$. In this study, it is regarded that $0 \leq T_{\mathrm{d,i}}^{\mathrm{min}} < T_{\mathrm{a,i}}^{\mathrm{min}} < T_{\mathrm{a,i}}^{\mathrm{max}} < +\infty$. At each fundamental attack phase, if the attack action is detected before it is finished, the system state will return to the security state. The successful detection probability of the i-th attack phase could be represented as $P(Y_i < X_i)$, calculated as

$$P(Y_i < X_i) = \int_{T_{a,i}^{min}}^{T_{a,i}^{max}} P(\,Y_i < X_i | X_i = t) f(X_i | X_i = t) dt = \frac{T_{a,i}^{max} + T_{a,i}^{min} - 2\times T_{d,i}^{min}}{2\times(T_{a,i}^{max} - T_{d,i}^{min})} \tag{3.5}$$

For all the transient states, the sojourn time at each state is denoted as $Z_i = \min\{Y_i, X_i\}$. The mean sojourn time at each state is denoted as S_i and it is calculated as [53]:

$$S_i = \int_{T_{d,i}^{min}}^{T_{a,i}^{max}} (1 - P(\,Z_i \leq t))dt = \int_{T_{d,i}^{min}}^{T_{a,i}^{max}} P(\,\min\{Y_i, X_i\} \geq t)d =$$

$$\frac{-(T_{a,i}^{min})^2 + 2(T_{a,i}^{max})^2 + 3(T_{d,i}^{min})^2 + 2T_{a,i}^{min}T_{a,i}^{max} - 6T_{d,i}^{min}T_{a,i}^{max}}{6(T_{a,i}^{max} - T_{d,i}^{min})} \tag{3.6}$$

The *MTTA* from the initial secure state to the final failure state can be calculated as in [54]:

$$MTTA = \sum_i V_i \, S_i \tag{3.7}$$

where V_i is the expected number of times that the system is in transient state *i* before the system finally reaches the absorbing failure state and it could be calculated as [53], [54]:

$$V_i = q_i + \sum_j V_j \, Q_{ji}, \tag{3.8}$$

where q_i indicates the probability that the SMP begins from state *i*. In the study, the initial state is the secure state *G*.

The SMP model is applied to model the intrusion process, identify the transient and absorbing states, and finally calculate the MTTA. This study applies the uniform distribution to statistically model the dynamic transition probability over a time period. One might argue that the recovery from the failure state to the secure state as well as the development and adoption of the patches could be effective in preventing the next attack, which will thus affect the value of MTTA. It is true that a single action of recovery/patching could probably somehow increase the cybersecurity of the cyber network, but its influence on the final outcome of MTTA should be carefully examined. The MTTA is a statistical average value which models the security of the target SCADA network when facing multiple trials of attacks. Its value is mainly associated with the overall cybersecurity of the cyber network. The influence of a single vulnerability could be rather limited. Usually there are multiple vulnerabilities associated with the target, also the new vulnerabilities are continuously being discovered.

It should be noted that if some significant actions are taken to improve the cybersecurity (e.g., installing advanced intrusion detection systems, adopting the sophisticated encryption, or significantly upgrading the SCADA network), the semi-Markov process model or its parameters should be updated and thus the MTTA value could be updated accordingly. For example, when the encryption is enforced, the attack model should be extended from the three-step procedure to the four-step procedure, which will eventually influence the final outcome of MTTA.

Obviously, the system will be in the failure state for a certain period of cyber forensic time until the attack is detected by the detection agent and the system will return to the secure state. Currently there is no real data available to estimate the detection time in the failure state. In this study, without loss of generality, the mean time to detect is denoted as MTTD. Considering the intrusion process and the detection time in the failure state, over a long period of time the attack probability that the cyber system is in the failure state can be calculated as:

$$P_{attack} = \frac{MTTD}{MTTD+MTTA} \tag{3.9}$$

This probability can be used in the sampling of the occurrence probability of attacks when performing the power system reliability evaluation based on the Monte Carlo simulation method.

3.3 Regional Load Redistribution Attack Model

The conventional LR attack model requires attacking measurement from all substations [67]. In practice, the power system dispatch operators are usually well trained and have rich experiences.

And measurements modification caused by the false data injection attack could be unknowingly incorporated into the training simulator environment to train the operators [68]. And when the LR attack passes the bad data detection, the power system operators might suspect the outcome of state estimation based on their experience and take actions to verify and cross-check the measurements, such as by reconfirming the measurements with the cyber traffic rerouted, or contacting the field personnel [68]. The field personnel can check the measurements locally at the substation and compare them with those received by the control center. If the cross-checked substation is included in the attack strategy, the attack would be detected and the fabricated measurements would be ignored. Thus, this kind of cross-checking actions could effectively detect the measurement modification if the attacker alters the measurements in all the substations. Thus, it is reasonable and meaningful for an attacker to restrict the attack region to avoid detection which leads to a smaller amount of load curtailment. In addition, it is noted that cross-checking the measurements comes with the extra time and effort, and it is inefficient to heavily rely on it to detect the false date injection. Also, the number of the substations and their locations should be appropriately chosen and it is unrealistic to cross-check a large number of substations dispersed in a wide area.

The regional LR attack can be mathematically modeled as follows [69], [70], [71]:

$$\max \textstyle\sum_l S_l^* \tag{3.10}$$

s.t.

$$\textstyle\sum_l \Delta L_{l,a} = 0 \tag{3.11}$$

$$\Delta PF_a + SF_a \cdot KL_a \cdot \Delta L_a = 0 \tag{3.12}$$

$$\left|\Delta L_{l,a}\right| \le \tau L_{l,a} \tag{3.13}$$

$$B_a \Delta\theta_a + KL_a \cdot \Delta L_{a=0} \tag{3.14}$$

$$\Delta\theta_i - \Delta\theta_j = 0 \quad \forall i,j \in bound\ of\ attack\ region \tag{3.15}$$

$$\{S^*\} = \min \textstyle\sum_l S_l \tag{3.16}$$

s.t.

$$\textstyle\sum_g P_g - \sum_l (L_l - S_l) = 0 \tag{3.17}$$

$$PF - SF \cdot KP \cdot P + SF \cdot KL \cdot (\Delta L + L - S) = 0 \tag{3.18}$$

$$|PF_b| \le PF_b^{max} \tag{3.19}$$

$$P_g^{min} \le P_g \le P_g^{max} \tag{3.20}$$

$$-\Delta L_l \le S_l - \Delta L_l \le L_l \tag{3.21}$$

where S_l is the load loss at bus l; L is the load demand; ΔL is the attack on the load demand measurements; PF is the power flow; ΔPF_a is the power flow change in the attack region a; $\Delta\theta_i$ and $\Delta\theta_j$ are voltage angles on the attack region boundary; τ is a ratio; SF_a, KL_a, B_a and KP are coefficient matrixes; P_g is the generation; P_g^{min} and P_g^{max} are generation limits.

The optimization problem (3.10)-(3.21) is a bilevel problem, where (3.10)-(3.15) is for the upper-level attacker and (3.16)-(3.21) are for the lower-level operator.

Regional LR attacks have a decreased probability of being detected, and this risk can be quantified as follows. Denote n_A as the number of substations in the attack region, and n_T as the total number of substations in the whole power system. If the power system operator chooses one substation to cross-check the measurements, the probability of detecting the LR attack can be calculated by

$$P_{dect} = \frac{n_A}{n_T} \tag{3.22}$$

3.4 Power System Reliability Modeling

The main steps of the non-sequential MCS method for assessing the power system reliability considering LR attack proposed in this study are depicted in Fig. 3.5 [47]. The basic procedures can be illustrated as follows.

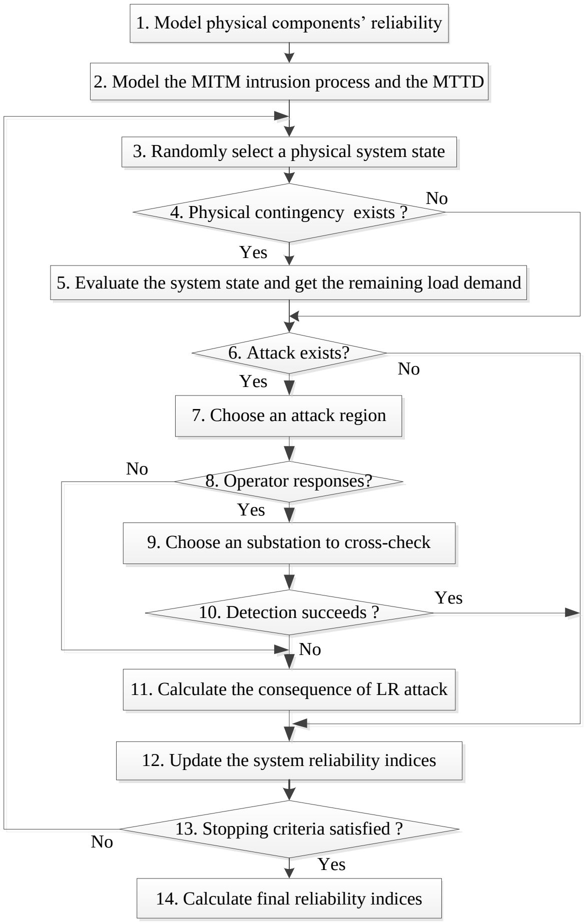

1. Model physical components' reliability
2. Model the MITM intrusion process and the MTTD
3. Randomly select a physical system state
4. Physical contingency exists ?
No
Yes
5. Evaluate the system state and get the remaining load demand
6. Attack exists?
No
Yes
7. Choose an attack region
No
8. Operator responses?
Yes
9. Choose an substation to cross-check
10. Detection succeeds ?
Yes
No
11. Calculate the consequence of LR attack
12. Update the system reliability indices
13. Stopping criteria satisfied ?
No
Yes
14. Calculate final reliability indices

Figure 3. 5 Flowchart for power grid reliability assessment considering LR attacks

Step 1) Model the reliability of the main physical components, including each generator, line and load demand by the reliability parameters such as mean time to repair (MTTR) and mean time to failure (MTTF). This step is well established in the conventional reliability evaluation.

Step 2) Model the intrusion process based on the SMP, and get the MTTA and the MTTD.

Step 3) Randomly choose a physical system state based on non-sequential MCS.

Step 4) Check whether there is any physical failure. If not, go to step 6; or go to the next step.

Step 5) Evaluate the system state based on OPF. There may be some load curtailments due to the physical failures. After this step, the system state load curtailment caused by physical failures could be obtained and the remaining load demand is used as the input parameters for the possible LR attack.

Step 6) Check whether there is an LR attack sampled using MCS as illustrated in (3.23).

$$f_a = \begin{cases} 0 & r_a \le P_{attack} \\ 1 & r_a > P_{attack} \end{cases} \tag{3.23}$$

where r_a is a random number derived from [0, 1]. If the value of f_a is zero, it indicates that an LR attack exists and the program proceeds to the next step; otherwise it entails that there is no LR attack and the program goes to step 12.

Step 7) Choose an attack region. In this study, the attack region should be of appropriate size and the size is measured by the number of branches in the attack region. The size of the attack region should not be too small so that it is possible to cause load curtailment.

Step 8) Check whether the operator responds. If the operator suspects the measurements received in the control center, the measurements in a certain substation will be cross-checked; otherwise the program goes to step 11. Since it depends on the operator's experience on whether cross-checking should be performed, the operator's experience is modeled by a response probability p_c and the higher value of p_c indicates that the operator is more experienced. A random number r_c is generated from [0, 1] and if $r_c \le p_c$, the operator will respond; otherwise he/she will not respond.

Step 9) Choose the substation to cross-check. It is assumed that only one substation will be cross-checked due to the limited number of staff and time available. The substation should be chosen based on some reasonable strategies to increase the detection probability.

Step 10) Check whether the attack is detected. If the cross-checked substation is included in the attack region, the measurement manipulation in this time step will be found and thus the power system dispatch in this time step is not affected.

Step 11) Determine the consequence of the LR attack.

Step 12) Update the reliability index based on the load curtailment obtained both in steps 5 and 11.

Step 13) If the stopping criterion is not satisfied, go to step 3. In this study, the 3% coefficient of variation of the EENS is chosen as the stopping criterion.

Step 14) Calculate the desired system reliability indices.

3.5 Case Studies and Simulation Results

In this chapter, the case study is conducted based on IEEE RTS79 system [48]. The transmission capacity of each line is adjusted to 60% of its original value to more clearly illustrate the idea proposed in this study. The simulation is based on MATLAB programming.

3.5.1 MTTA of the Attack

As discussed, the intrusion process is modeled by the SMP and it could be specified by the distribution of the sojourn time in each state transition. While the appropriate values of the sojourn times should be obtained from real statistical data, currently there is little data available. The accurate assessment of MTTA is particularly challenging because of the limited historical data available. Generally, experts require less time than novices to accomplish an attack step. In this case study, the range of time values varies from several hours to a few days, and the lower and upper bounds correspond to the time quantities needed by the experts and the novices, respectively. These values match the estimation in [72]. In real practices, for each SCADA system, the operations, events, incidents and intrusion traces are recorded by log files, which are accessible to the security managers. Also, the honeypot can aid in collecting the intrusion data. The log files and the honeypot data can be the evidence for cyber forensics. With these data, the specific time associated with the attack and detection can be statistically analyzed. The realistic values can be obtained based on the statistical methods like those discussed in [31], [73].

Some example values associated with the sojourn times are given in Table 3.1 for illustrating the idea proposed in this study.

Table 3. 1 Example time intervals for non-encrypted SCADA

State Transitions	T_d^{min}(h)	T_a^{min}(h)	T_a^{max}(h)
G to S_1	2	20	50
S_1 to S_2	2	12	30
S_2 to F	2	15	40

Based on the values in Table 3.1, the MTTA can be calculated as 795 hours. To demonstrate how the attack times might influence the MTTA, the value of $T_a^{\min}$ in Table 3.1 is changed by multiplying a factor β and the results are shown in Fig. 3.6. It shows that the increase of the attack time in the attack phases leads to an increased MTTA.

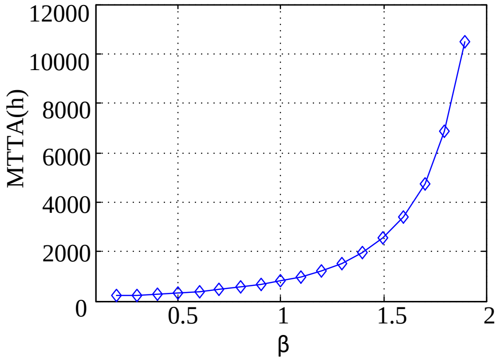


Figure 3. 6 The influence of attack time in the attack phases

Table 3. 2 Example time intervals for encrypted SCADA

State Transitions	T_d^{min}(h)	T_a^{min}(h)	T_a^{max}(h)
G to S_1	2	20	50
S_1 to S_2	2	15	50
S_2 to S_3	2	12	30
S_3 to F	2	15	40

If the communication is encrypted, the required number of steps will increase from three to four. If the parameters associated with each step are given as in Table 3.2, the calculated MTTA is 2,409 h. In this case, the MTTA is significantly larger than that when the encryption is not enforced. This outcome clearly demonstrates that the encryption can greatly increase the expected time to accomplish a successful false data injection attack.

3.5.2 Regional Load Redistribution Attack

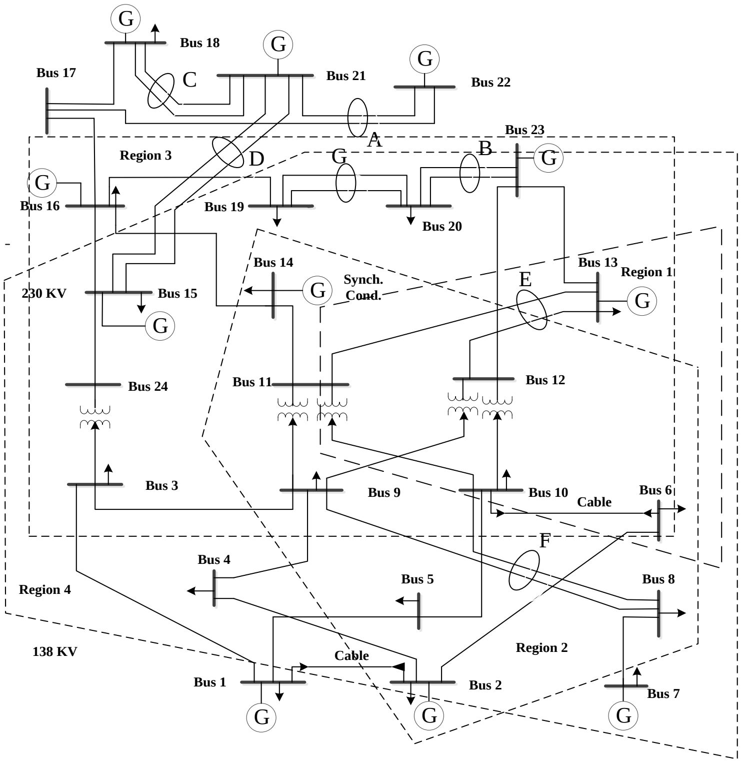


Figure 3. 7 Regional load redistribution attack schemes with IEEE RTS79 system

Fig. 3.7 depicts examples about how a regional LR attack can be constructed. The attacker can choose one region as the local attack region, such as the region 1. For example, the region 1 consists of buses 6, 10, 11, 12, and 13. However, buses 6, 10, 11, 12, and 13 are all connected with the non-attack region. So the buses 6, 10, 11, 12 and 13 are all boundary buses in attack region 1. The detailed consequence of these attack regions is shown in Table 3.3. From this table, it can be seen when the attacker chooses different attack regions there can be different amounts of load curtailment at different bus locations, and they have different probabilities of being detected.

Table 3. 3 Examples of regional LR attacks

Attack region	Probability of being detected	Curtailment (MW)	Curtailment Location
Region 1	0.208	30.61	Bus 6
Region 2	0.375	61.98	Bus 14
Region 3	0.583	73.12	Bus 6 and 14
Region 4	0.750	122.67	Bus 3, 6 and 14

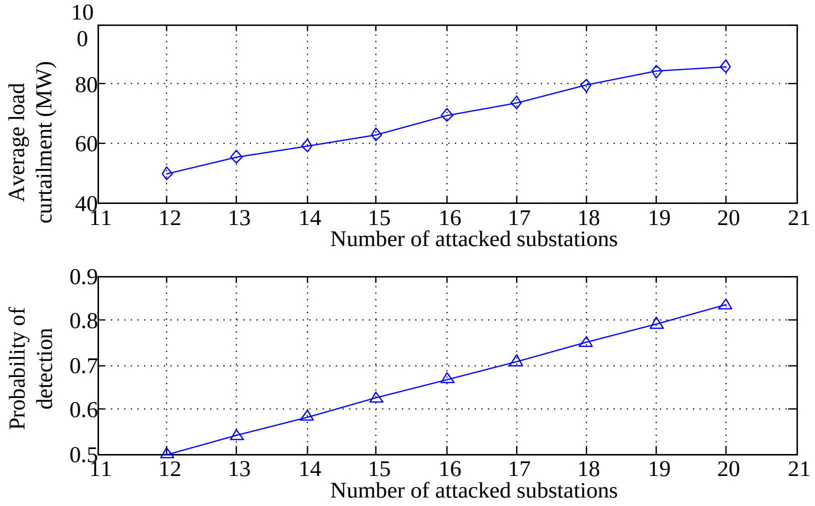


Figure 3. 8 Regional attack results

Further, the load curtailment and the risk associated with the attack region is statistically analyzed as shown in Fig. 3.7. About 2,000 attack regions are randomly sampled. For each of the sampled attack region, the load curtailment is calculated based on (3.22)-(3.33), the probability of detection is obtained based on (3.34). These attack regions are grouped according to the number of substations in the attack region, and the average load curtailment for each group is calculated as shown in the top subgraph of Fig. 3.7. Also, the probability of detection of each group is obtained as shown in the bottom subgraph of Fig. 3.7.

From the results shown in Fig. 3.7, it is found that the average load curtailment increases when the number of substations in the attack region increases. This is because the increased number of attacked substations provides a larger room for the attacker to compromise the state estimation outcome. However, the increased number of the attacked substations comes with a higher probability of being detected. Hence, there is a compromise between the load curtailment and the risk of being detected when the attacker chooses the attack region. As a result, it is reasonable for the attacker to randomly choose an attack region without the knowledge about the cross-check strategy.

3.5.3 Reliability Modeling of Power System

Based on the intrusion modeling and the analysis of the LR attack, the power system reliability evaluation considering the LR attacks is calculated. The basic parameters of the intrusion are shown in Tables 3.1 and Table 3.2, and the MTTD is chosen as 9 hours.

If no cross-checking is performed, the attacker will launch the complete LR attack and the attack region will be the whole network. By comparing scenarios 1 and 2, it is shown that the influence of LR attack on the overall power system reliability is not negligible. By comparing scenarios 2 and 3, the influence of β is demonstrated. As the decrease of β entails less time spent on the attack phases, the result shows the attacker’s capability can have great influence on the overall power system reliability. The EENS value in scenario 4 is less than that in scenario 2, indicating that the encryption can greatly contribute to maintaining the power system reliability.

Table 3. 4 Reliability evaluation with complete LR attack

Scenario number	Encryption	β	P_{MITM}	EENS(MWh)
1	No	No attack	0	1.970e5
2	No	1	0.011	2.241e5
3	No	0.5	0.026	2.640e5
4	Yes	1	0.004	2.069e5

If the cross-checking is performed, it is reasonable for the attacker to launch regional LR attack. In this study, the attack region is randomly selected. The cross-checking probability is described by p_c and two cross-check strategies are considered. In the random strategy, one substation is randomly selected for cross-check. In the selective strategy, a substation is randomly selected among the top 5 substations with the highest load demands. The results are shown in Table 3.5.

Table 3. 5 Reliability evaluation with regional LR attack

Scenario number	β	P_{MITM}	p_c	Cross-check strategy	EENS (MWh)
5	1	0.011	0.3	Random	2.081e5
6	0.5	0.026	0.3	Random	2.111e5
7	1	0.011	0.5	Random	2.036e5
8	1	0.011	0.7	Random	1.975e5
9	1	0.011	0.3	Selective	1.974e5

By comparing scenarios 5 and 6 in Table 3.5 and scenarios 2 and 3 in Table 3.4, it is concluded that the cross-check can improve the power system reliability as less non-optimal power dispatches are performed. Be comparing the scenarios 5, 7 and 8, it is shown that the increased cross-check can help maintain the power system reliability, which indicates the more experienced and better trained operators are essential to maintain the power system reliability. By comparing scenarios 5 and 9, it can be found that the power system reliability can be improved if a more effective cross-check strategy is adopted.

In the above analysis, the influence of various factors is examined, including β, cross-check probability p_c, and cross-check strategy. Based on the obtained results, the defense strategy against LR attacks can be derived accordingly. Generally, the defense methods against LR attacks can be divided into two categories. The first category of methods attempts to reduce the probability of the successful injection of false data, based on techniques for increasing the number of steps required to compromise the final objective (e.g. encryption), decreasing the detection time required for each step, increasing the time of attack for each step, among many others. The second category of methods aims to detect the false data injection if the false data injection is successful, based on techniques for increasing the cross-check success probability, optimizing the selection of substations for cross-check, and so forth. It should be noted that defense methods come with extra costs, such as capital investment to encrypt the communication, installing advanced intrusion detection software, or human resources needed for performing the cross-check task. The quantitative methods proposed in this chapter and the associated outcomes could provide some useful insights for aiding in the judicious allocation of limited budget.

3.6 Conclusions

In this study, the malicious attack against the state estimation was modeled by SMP considering the major intrusion phases and the associated attack/detection time in each attack phase. A practical regional LR attack model was proposed to avoid the cross-check detection. Based on the attack model and the LR attack model, a holistic power system reliability evaluation framework for incorporating the LR attack was proposed based on Monte Carlo simulation. The simulation was conducted based on the IEEE RTS79 system and the influences of various factors were investigated, including the attack time in the attack phases, the cross-check probability and cross-check strategy.

4. Coordinated Attacks on Electric Power Systems in a Cyber-Physical Environment

4.1 Introduction

Most previous research work was focused on standalone attacks, which studied how to choose multiple components of same kind in a certain attack scenario in order to maximize the loss. It is possible that the intelligent attacker may coordinate different attacking mechanisms and different targets of attacks in order to launch a successful cyberattack or to maximize the resultant damage. Indeed, the coordination between different attacking mechanisms and different targets was well demonstrated in the 2015 Ukrainian power grid attack. Spear-phishing emails with malware were used to gain the initial access; the breakers were tripped to isolate several substations; malware was used to destroy files in the workstation to delay the restoration; and DoS attack was launched against phone calls to deny customers' blackout information. In this cyberattack, the attacker coordinated malware, tripping of switches, DoS attack at different stages of the attack, and it alerts the researchers and industrial practitioners to pay more attentions to the coordination between different attack scenarios.

While the majority of existing work studied the optimal selection of possible targets of attack in a coordinated manner, this chapter focuses on the coordination between different attack scenarios. To facilitate the readers to better understanding this chapter, the schematic overview of the whole chapter is shown in Fig. 4.1.

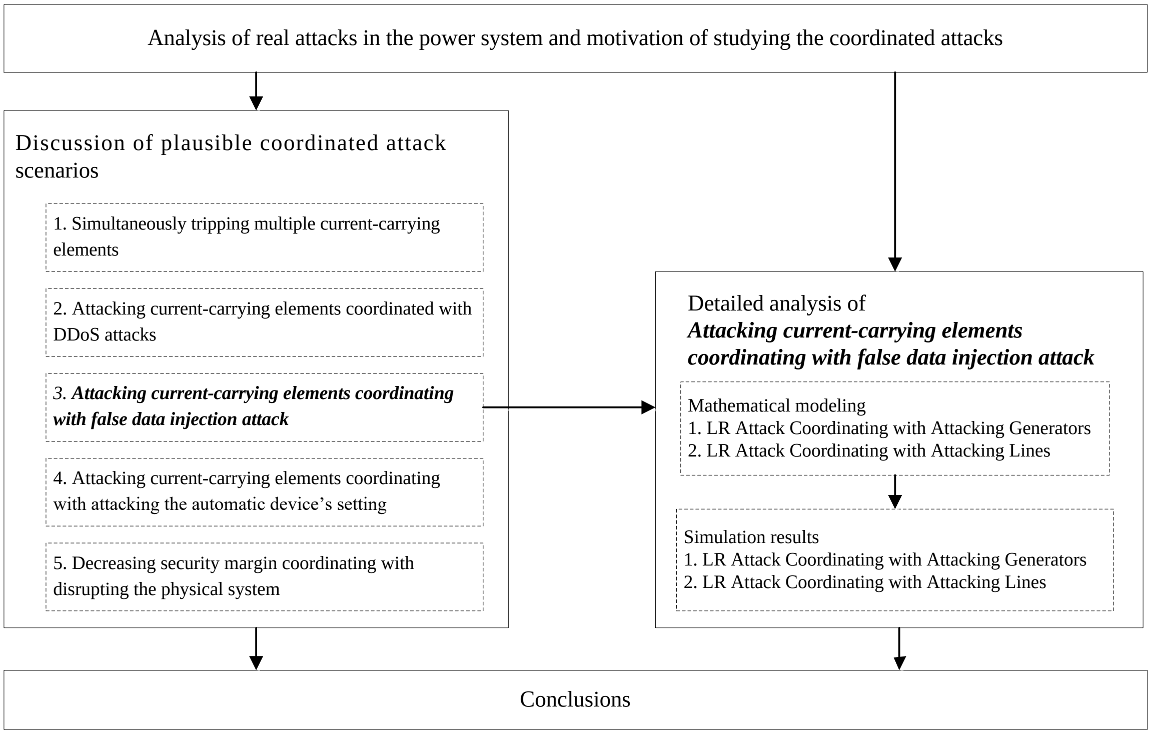

Analysis of real attacks in the power system and motivation of studying the coordinated attacks
Discussion of plausible coordinated attack scenarios
1. Simultaneously tripping multiple current-carrying elements
2. Attacking current-carrying elements coordinated with DDoS attacks
3. Attacking current-carrying elements coordinating with false data injection attack
4. Attacking current-carrying elements coordinating with attacking the automatic device's setting
5. Decreasing security margin coordinating with disrupting the physical system
Detailed analysis of
Attacking current-carrying elements coordinating with false data injection attack
Mathematical modeling
1. LR Attack Coordinating with Attacking Generators
2. LR Attack Coordinating with Attacking Lines
Simulation results
1. LR Attack Coordinating with Attacking Generators
2. LR Attack Coordinating with Attacking Lines
Conclusions

Figure 4. 1 Schematic overview of the chapter

4.2 Power System Vulnerabilities and Coordinated Attacks

4.2.1 Analysis of Attacks against Power Systems

The modern smart grid can be viewed as a cyber-physical human-in-the-loop system. The physical part, cyber part and human part are responsible for energy transmission, monitoring and control, and decision-making, respectively. And they are interconnected and the secure operation of the power grid requires the normal working of each indispensable part. The failure or malfunction in any part can negatively affect the power grid, or even possibly cause a catastrophic consequence.

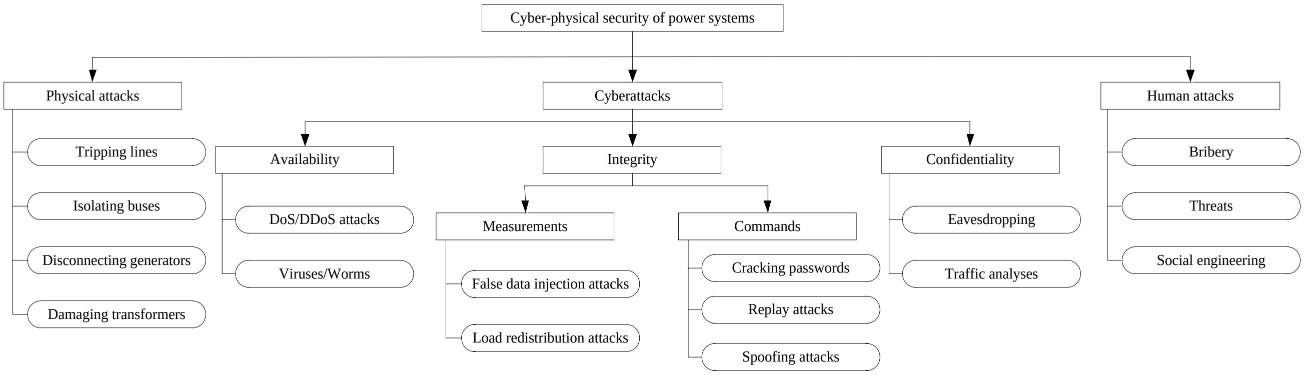


Figure 4. 2 Attacks against electric power systems

The power system as a critical infrastructure can be a valuable target for the attackers in war, terrorism and sabotage activities. While the power system could be directly attacked by physical means, it has been reported that the power system communication network is under constant cyberattacks. The power system associated personnel, especially those who are depressed or dissatisfied, can also intentionally or unintentionally leak critical information, or even be forced to take some detrimental actions. In Fig. 4.2, the attacks related to the security of power systems are depicted. The attacks are classified into three types: physical attack, cyberattack and human attack as the smart grid is a cyber-physical interconnected complex network controlled by the operators. The attack through or against the power system personnel was termed the “human attack”. Cyberattacks are classified into the attacks against the availability, integrity and confidentiality which are the basic requirements of a general cyber network. An attack against the availability can cause the loss of control of the local devices or a delayed response. An attack against the integrity can compromise the data and information communication in the cyber network, which can severely affect the normal operation of the power grid. An attack against the confidentiality can cause the leakage of critical information. While all the cyberattacks have negative impacts on the power grid, the attack against integrity would be relatively more severe. Thus, it is further divided into the attack against the measurements and the attack against the commands. For each attack type, several specific examples are provided. It is worth noting that with the development of the smart grid it is quite possible that new attack methods will be endlessly developed in the coming future.

The attacks can affect the security of the power grid in different ways. Some attacks can proactively affect the working status of the current-carrying devices in the field, such as tripping a line by a bomb or sending fabricated control commands to the generator. Some attacks can mislead the power dispatch decision-making; for example, the cyberattacker can manipulate a set of the measurements to change the state estimation outcome and mislead the operator to make non-optimal or even wrong dispatch decisions. Some attacks can cause the loss of control of the local device or control systems; for example, the attacker can infect an IED with a virus and make the related device unresponsive to commands; distributed denial of service (DDoS) attack can also be used to block the communication and cause the delay of operation commands sent to local devices or the measurements sent to the control center. The goal of some attacks may not be to directly influence the operation of the power grid, but to acquire critical information. This is also highly harmful as the information can be used for aiding future attacks, such as bypassing the intrusion detection, cracking the password, gaining the desired control privilege or designing optimal attack plan, etc.

4.2.2 Power System Operation and Coordinated Attacks

The secure operation of the power grid needs to abide by several requirements, mainly including the normal operation of the current-carrying devices; the accurate and timely transmission of the measurements and alarms; sufficient situation awareness, wise decision-making and quick response of the operator; the prompt implementation of genuine control actions; the correct setting and operation of the automatic control and protection devices; etc. These requirements are especially demanding in case of disturbances, failures or attacks.

The operation of the power system and how it could be affected by various kinds of attacks are shown in Fig. 4.3. The failures of the current-carrying devices; the absence, delay or manipulation of the measurements and commands transmitted in the supervisory control and data acquisition (SCADA) network; the wrong decision-making or late response of the operator; or the alteration of the setting of the automatic control and protection devices can all potentially result in power system economic loss, load curtailment or equipment damage. Because N-1 or even N-2 security standards are implemented, the cyber-physical power grid has a certain inherent amount of resiliency in withstanding attacks or failures, therefore the possibility of suffering great losses is not guaranteed in cases of standalone attacks. However, if multiple parts or functions are attacked in coordination, the possibility of great losses would be massively increased. Thus, it is quite possible that a well-informed attacker can launch coordinated attacks to efficiently maximize damage. Several possible coordinated attack scenarios are introduced and discussed below.

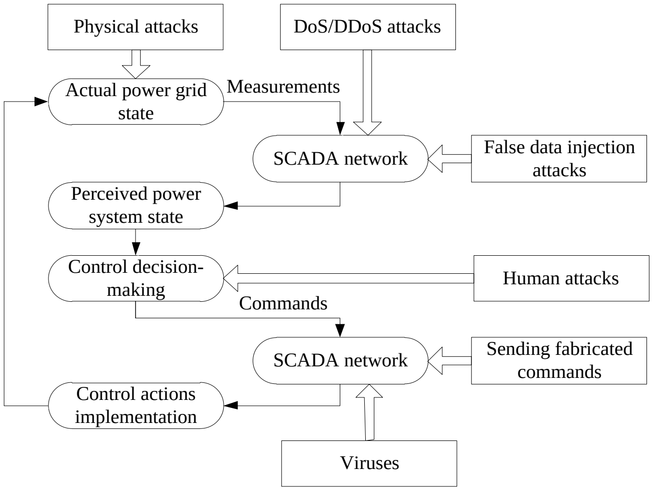


Figure 4. 3 Power system operation and attacks

(1) *Simultaneously tripping multiple current-carrying elements*

A power system usually has sufficient transmission and generation capacities and the tripping of one line/generator will probably not result in great power failure. However, if multiple elements are tripped simultaneously either by a physical, cyber or human attack, great failures can easily occur. This is a common plan of coordinated attacks, two examples of which are provided in Figs. 4 and 5.

As shown in Fig. 4.4, if an intelligent attacker chooses multiple critical lines and attacks them simultaneously, the sudden loss of multiple lines can cause massive power loss.

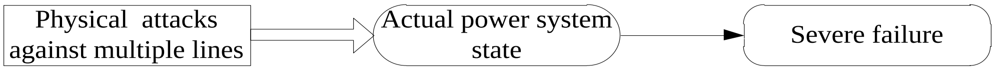

Physical attacks against multiple lines
Actual power system state
Severe failure

Figure 4. 4 Coordinated physical attacks against lines

If a cyberattacker intrudes into multiple substations and gains the desired control privilege, the attacker is able to trip the components directly connected to these attacked substations. This intrusion can cause a serious disturbance on the power system and lead to great failures as shown in Fig. 4.5.

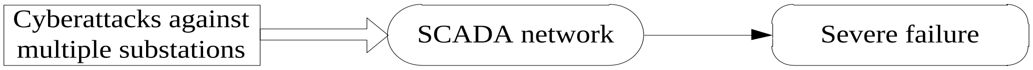


Figure 4. 5 Coordinated cyberattacks against substations

(2) *Attacking current-carrying elements coordinated with DDoS attacks*

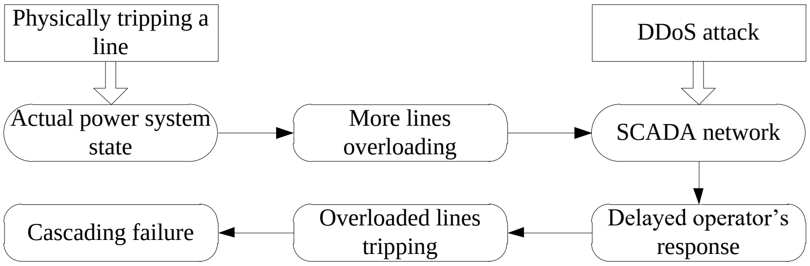

Physically tripping a line
DDoS attack
Actual power system state
More lines overloading
SCADA network
Cascading failure
Overloaded lines tripping
Delayed operator's response

Figure 4. 6 Physically tripping a line coordinating with DDoS attack

When the physical system is disrupted, the operators' prompt and thoughtful response is critical for preventing further failures. If the operators fail to take remedial actions in a timely manner, great failures can happen, such as the 2003 northeast blackout [74]. So an attacker can launch coordinated attacks to disrupt the physical system while simultaneously delaying the response of the operators. A representative example of this kind of coordination is physically tripping a line together with a DDoS attack as shown in Fig. 4.6. When the physical operation is disrupted after the line is tripped, the attacker can launch a DDoS attack to delay or disrupt the measurements sent to the control center. This can lead to a delay in the remedial action decision and its implementation. Such delays may result in cascading failures.

(3) *Attacking current-carrying elements coordinating with false data injection attack*

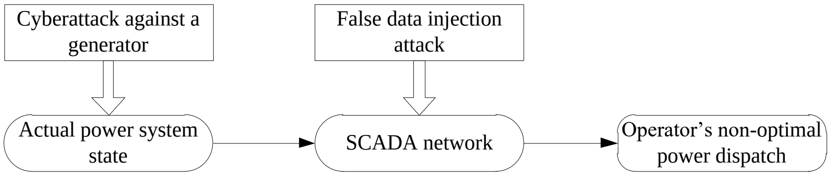

Cyberattack against a generator
False data injection attack
Actual power system state
SCADA network
Operator's non-optimal power dispatch

Figure 4. 7 Cyberattack against a generator coordinating with false data injection attack

A failure in the physical system requires the system operator to take reasonable remedial actions to decrease the loss. If a failure or attack happens, and the operator takes non-optimal or even wrong actions, unnecessary loss can happen. Thus, the attacker can coordinate attacks to disrupt the physical system and mislead the power dispatch of the operator. An example of this kind of coordinated attacks is shown in Fig. 4.7. The attacker can disconnect a generator to disrupt the power grid operation and launch false data injection attack to mislead the power dispatch in coordination. By this way, unnecessary loss or even great failure can occur.

(4) *Attacking current-carrying elements coordinating with attacking the automatic device's setting*

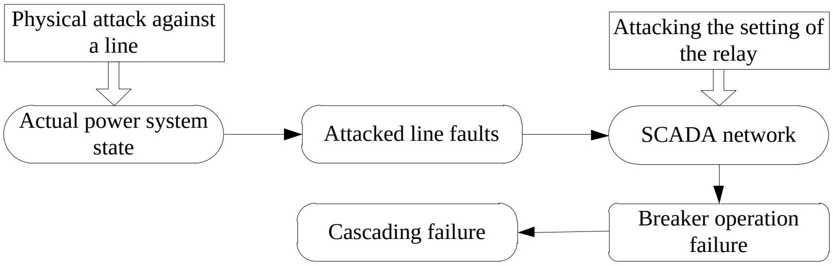

Physical attack against a line
Attacking the setting of the relay
Actual power system state
Attacked line faults
SCADA network
Cascading failure
Breaker operation failure

Figure 4. 8 Faulting a line coordinating with changing the relay's setting

When a major physical element fails because of either physical attack or cyberattack, it can cause disturbance to other parts of the system. To limit the disturbance, the automatic devices need to react promptly; otherwise, more affected elements may fail. For example, if a line is grounded, the breaker at each end of the line needs to operate to trip the faulted line. If they fail to operate, more related parts may fail and this can easily cause greater failures. Thus, an attacker can coordinate the attacks to fault the physical element and disable its related automatic devices. An example of this kind of coordinated attacks is described in Fig. 4.8. The attacker can intrude into the SCADA network and change the setting of a relay and later launch a physical attack against its related line (e.g. connecting it to ground) and thus the breaker will not operate when the fault happens. In this case, the lines, generators and loads connected to the faulted line will be tripped and this could cause cascading failures.

(5) *Decreasing security margin coordinating with disrupting the physical system*

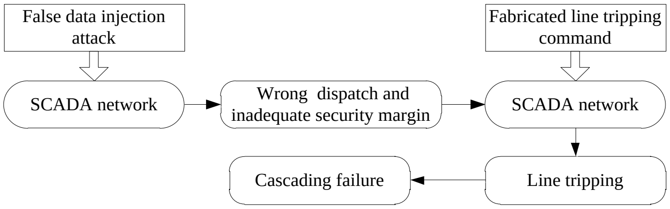

False data injection attack
Fabricated line tripping command
SCADA network
Wrong dispatch and inadequate security margin
SCADA network
Line tripping
Cascading failure

Figure 4. 9 False data injection attack coordinating with tripping a line

In power system operations, the operator needs to make wise operation decisions aided by various decision-making tools. Usually the power dispatch strategy should allow adequate security margin and stability margin [75]. If the power dispatch strategy is deliberately misled by false data injection attack or the operator is threatened, the power system state after the dispatch can be very vulnerable. The attacker can launch other attacks to directly disrupt the physical system, due to the limited security margin, and system instability can happen and cause a great blackout. A possible scenario of this kind of coordinated attacks is shown in Fig. 4.9.

4.3 Principle of Coordinated Attacks

In Chapter 4.2, multiple coordinated attack scenarios are proposed and discussed. Since it is difficult to mathematically model all these coordinated attack scenarios in detail in a single study, this chapter is focused on analyzing the coordination scenario 3 to demonstrate the potential damaging effects and limitations of the coordinated attacks.

The false data injection attack modeling indicated that by manipulating well-selected measurements the attacker could purposely alter the final outcome of the state estimation without being detected [50]. While there are multiple different specific models [16] for the false data injection attack, the LR attack is chosen as a representative example in this study.

The basic principles of an LR attack are described as follows [51]:

$$\sum_{i=1}^{N_D} \Delta P_{D,i} = 0 \tag{4.1}$$

$$\Delta P_F = -SF \times KD \times \Delta P_D \tag{4.2}$$

$$-\tau P_{D,i} \leq \Delta P_{D,i} \leq \tau P_{D,i} \tag{4.3}$$

where $\Delta P_{D,i}$ is the attack on the i_{th} load demand measurement; N_D is the number of load demands; ΔP_F is the attack on the line power flow measurements; SF is the shifting factor matrix determined by the topology and parameters of the transmission network; KD is the bus-load incidence matrix determined by the positions of the load demands; $P_{D,i}$ is the i_{th} actual load demand; τ is a factor indicating the limit on attack magnitude of the load demand measurements.

The mathematical modeling of an LR attack can be described by a bilevel model as shown in Fig. 4.10 [67].

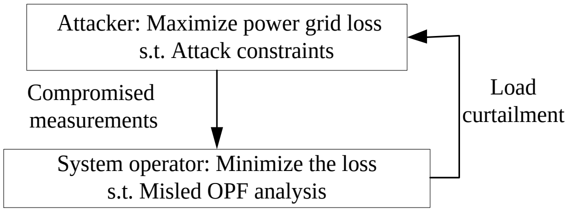


Figure 4. 10 Bilevel modeling for the LR attack

As a type of practical cyberattacks, an LR attack could possibly cause power loss by misleading the power system operators. Besides the LR attack, the power system is vulnerable to various attacks in both cyber and physical domains, such as shooting a generator or transmission line which can result in the tripping of the element. If the power grid is disrupted and the power dispatch is misled in coordination, the consequence might be more severe. To effectively protect the cyber-physical grid, it is meaningful to study how an LR attack could coordinate with other disruptive attacks against the current-carrying elements. This can be generally described by a bilevel model shown in Fig. 4.11, and it is explained as follows.

The attacker aims to maximize the load curtailment though coordinated attacks while the defender aims to minimize it. Thus, the attacker needs to take the defender’s remedial actions into consideration when making the optimal attack plans. At the upper level the attacker tries to determine the measurement attack vector and current-carrying elements to be attacked. The attack strategy aims at achieving the maximum load curtailment under the attack constraints. At the lower level, the defender takes corrective actions to minimize the loss after the attacks. And the defender could be modeled by the optimal power flow (OPF) analysis.

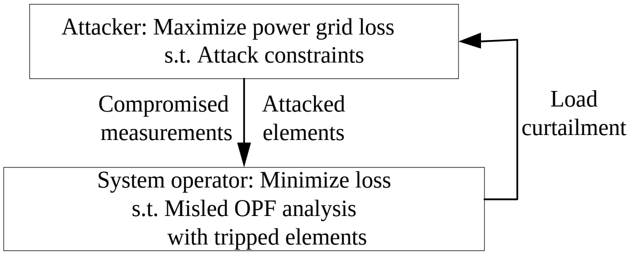


Figure 4. 11 A bilevel model for the coordination of LR attack and other attacks

This framework can be applied to various kinds of specific cyber and physical attacks coordinating with an LR attack. For the attacks to trip physical current-carrying elements, different attack cyber or physical mechanisms can be adopted. For instance, the cyberattack methods for tripping a generator include infecting the generator control computer with a virus; gaining control privileges and sending a tripping command to the generator; and attacking the database to alter configurations and settings of the related protective devices. Similar methods can also be applied to trip transmission lines. The physical attack methods for disrupting a line/generator include various vandalism and terrorism activities such as shooting and explosion, etc.

While both cyber and physical attack methods can be applied to trip generators and lines, generally it is relatively easier to trip a line than a generator by a physical attack, so this study considers cyberattacks against generators and physical attacks against lines.

4.4 LR Attack Coordinating with Attacking Generators

The attacker could first launch an LR attack. If the LR attack is successful, the power system operator will develop a wrong understanding of the load demands at the load points. Then the attacker could trip certain generators. If the LR attack and the attack against generators are well coordinated, the operator's remedial action after the attacks will be based on the false load demand measurements. The mathematical model for an LR attack coordinating with cyberattacks against generators is illustrated in the bilevel model below.

$$\max \{\textstyle\sum_{i=1}^{N_D} P_{C,i}^{*}\} \tag{4.4}$$

subject to:

$$\textstyle\sum_{i=1}^{N_D} \Delta P_{D,i} = 0 \tag{4.5}$$

$$\Delta P_F = -SF \times KD \times \Delta P_D \tag{4.6}$$

$$-\tau P_{D,i} \leq \Delta P_{D,i} \leq \tau P_{D,i} \quad \forall i \tag{4.7}$$

$$\Delta P_{D,i} = 0 \leftrightarrow \eta_{D,i} = 0 \quad \eta_{D,i} \in \{0,1\} \ \forall i \tag{4.8}$$

$$\Delta P_{F,j} = 0 \leftrightarrow \eta_{F,j} = 0 \quad \eta_{F,j} \in \{0,1\} \ \forall j \tag{4.9}$$

$$\sum_{i=1}^{N_D} C_{D,i}\,\eta_{D,i} + 2 \times \sum_{j=1}^{N_F} C_{F,i}\eta_{F,j} + \sum_{k=1}^{N_G} C_{G,k}\left(1 - \nu_{G,k}\right) \leq R_c \quad \forall \nu_{G,k} \in \{0,1\} \tag{4.10}$$

$$P_C^* = \arg\{\min \sum_{i=1}^{N_D} P_{C,i}\} \tag{4.11}$$

subject to:

$$\sum_{k=1}^{N_G} P_{G,k} = \sum_{i=1}^{N_D}(P_{D,i} - P_{C,i}) \tag{4.12}$$

$$P_F = SF \times KP \times P_G - SF \times KD \times (P_D + \Delta P_D - P_C) \tag{4.13}$$

$$-P_{F,j}^{max} \leq P_{F,j} \leq P_{F,j}^{max} \quad \forall j \tag{4.14}$$

$$\nu_{G,k} \times P_{G,k}^{min} \leq P_{G,k} \leq \nu_{G,k} \times P_{G,k}^{max} \quad \forall k \tag{4.15}$$

$$0 \leq P_{C,i} \leq P_{D,i} + \Delta P_{D,i} \quad \forall i \tag{4.16}$$

where the binary parameter $\eta_{D,i}$ indicates the i_{th} load demand measurement is attacked if it equals 1; the binary parameter $\eta_{F,j}$ indicates the j_{th} line power flow measurement is attacked if it equals 1; the binary parameter $\nu_{G,k}$ indicates the k_{th} generator is attacked if it equals 0; N_F and N_G are the number of transmission lines and the number of generators, respectively; C_D, C_F and C_G denote the cost required to attack the load demand measurements, the power flow measurements and the generators, respectively; R_c is the cyberattack resource that the attacker has. P_D, P_C, P_F and P_G are the actual load demands, load curtailments, line power flows and generator active power outputs, respectively; and KP is the bus-generator incidence matrix.

The attacker's goal is to maximize the total load curtailment as described in (4.4) under the constraints (4.5)-(4.10). Constraints (4.5)-(4.7) are the basic constraints of an LR attack. Constraints (4.8)-(4.10) ensure that the attacks are within the attack resource limitation of the attacker. Similar to the work in [76], constraint (4.10) uses dimensionless attack resource and attack cost to model the attacker's capacity and the difficulty to attack a target, respectively. If the attack resource owned by the attacker is greater than the total attack cost needed to compromise the selected targets, these targets will be successfully attacked.

The defender aims to minimize the load curtailment as shown in (4.11) under the constraints (4.12)-(4.16). And the corrective action of the defender is described by DC OPF analysis. Constraint (4.12) ensures the power balance in the whole power system. Constraints (4.13) and (4.14) describe the line power flow limitation under the LR attack. Constraint (4.15) restricts the generation outputs. Constraint (4.16) indicates the load curtailment limitations.

The actions of the attacker and the defender in this coordinated attack scenario are illustrated in Fig. 4.12. The attacker needs to develop the optimal attack strategy by solving the optimization problem represented by (4.4)-(4.16), which considers the optimal response of the defender. Then based on the obtained optimal attack strategy, the attacker first manipulates the measurements in a coordinated manner to pass the bad data detection mechanism of the state estimation, and thus the power system operator is misled to trust the manipulated load demand measurements. Then the attacker trips the generators and causes disturbance in the power system. The power system operator takes remedial actions trying to minimize the load demand. As the power re-dispatch strategy is developed based on the manipulated load demand measurements, some load demands may have to be curtailed.

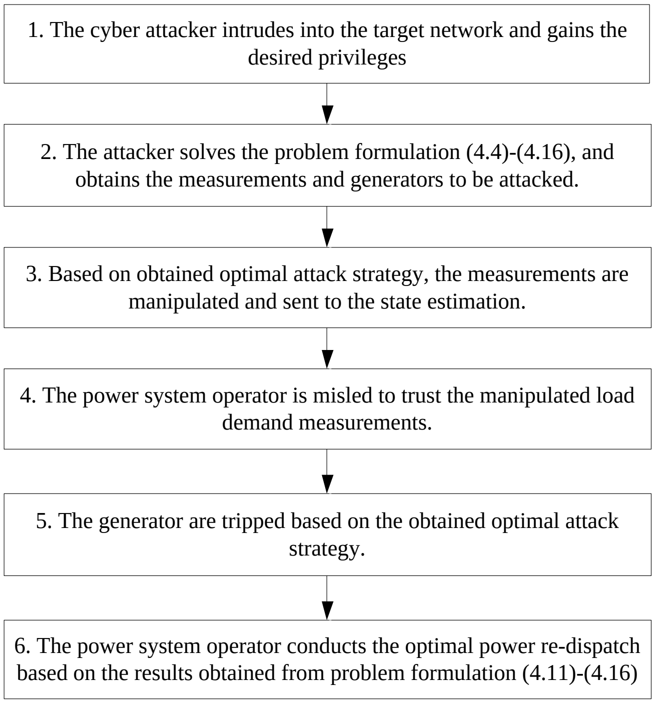

1. The cyber attacker intrudes into the target network and gains the desired privileges
2. The attacker solves the problem formulation (4.4)-(4.16), and obtains the measurements and generators to be attacked.
3. Based on obtained optimal attack strategy, the measurements are manipulated and sent to the state estimation.
4. The power system operator is misled to trust the manipulated load demand measurements.
5. The generator are tripped based on the obtained optimal attack strategy.
6. The power system operator conducts the optimal power re-dispatch based on the results obtained from problem formulation (4.11)-(4.16)

Figure 4. 12 Illustration of the LR attack coordinating with attacking generators

4.5 LR Attack Coordinating with Attacking Lines

Besides the generation capacity, the transmission capacity is also a critical factor in maintaining the power system reliability. Similar to the coordination in Chapter 4.4, the attacker could first launch an LR attack to mislead the operator about the load demands and then physically trip one or more lines. The attacker needs to carefully choose the measurement attack vector and target lines to maximize the damage. The mathematical model for an LR attack coordinating with attack against lines is shown as follows.

$$\max \{\textstyle\sum_{i=1}^{N_D} P_{C,i}^{*}\} \tag{4.17}$$

subject to:

$$\textstyle\sum_{i=1}^{N_D} \Delta P_{D,i} = 0 \tag{4.18}$$

$$\Delta P_F = -SF \times KD \times \Delta P_D \tag{4.19}$$

$$-\tau P_{D,i} \leq \Delta P_{D,i} \leq \tau P_{D,i}\ \forall i \tag{4.20}$$

$$\Delta P_{D,i} = 0 \leftrightarrow \eta_{D,i} = 0 \quad \eta_{D,i} \in \{0,1\}\ \forall i \tag{4.21}$$

$$\Delta P_{F,j} = 0 \leftrightarrow \eta_{F,j} = 0 \quad \eta_{F,j} \in \{0,1\}\ \forall j \tag{4.22}$$

$$\sum_{i=1}^{N_D} C_{D,i} \times \eta_{D,i} + 2 \times \sum_{j=1}^{N_F} C_{F,j} \times \eta_{F,j} \leq R_c \tag{4.23}$$

$$\sum_{j=1}^{N_F} C_{FP,j}(1 - \nu_{F,j}) \leq R_p\ \ \forall \nu_{F,j} \in \{0,1\} \tag{4.24}$$

$$P_C^* = \arg\{\min \sum_{i=1}^{N_D} P_{C,i}\} \tag{4.25}$$

subject to:

$$P_{F,j} = \nu_{F,j} \times \frac{1}{x_{F,j}} \sum_{n=1}^{N_B} A_{nj}\delta_n\ \ \forall j \tag{4.26}$$

$$\sum_{k \in J_n} P_{G,k} - \sum_{j=1}^{N_F} A_{nj}\, P_{F,j} + P_{C,n} = P_{D,n} + \Delta P_{D,n} \forall n \tag{4.27}$$

$$-P_{F,j}^{max} \leq P_{F,j} \leq P_{F,j}^{max}\ \forall j \tag{4.28}$$

$$P_{G,k}^{min} \leq P_{G,k} \leq P_{G,k}^{max}\ \forall k \tag{4.29}$$

$$0 \leq P_{C,i} \leq P_{D,i} + \Delta P_{D,i}\ \forall i \tag{4.30}$$

where the binary $\nu_{F,j}$ indicates the j_{th} line is attacked if it is equal to 0; $C_{FP,j}$ indicates the physical attack cost required to attack line *j*; R_p is the attacker's physical attack resource while R_c is the cyberattack resource; $x_{F,j}$ is the reactance of the line *j*; δ_n is the voltage phase angle (rad) of bus *n*; J_n is the set of generators in bus *n*; N_B is the number of buses; A_{nj} equals 1 if the power flow of line *j* is defined from bus *n* to another bus, and it equals 0 if it is from another bus to bus *n*.

The attacker's strategy is described in (4.17)-(4.24), and constraints (4.21)-(4.23) ensure that the cyberattack resource limitation is satisfied and constraint (4.24) ensures that the physical attack resource limitation is met. The defender's strategy to minimize the load curtailment is described in (4.25)-(4.30). The line power flow is shown in (4.26) and the attack on lines is incorporated [77]. Constraint (4.27) represents the power input-output balance relationship at each bus. And the limitations on the power flows, generator outputs and load curtailments are shown in (4.28), (4.29) and (4.30), respectively.

The actions of the attacker and the defender in this coordinated attack scenario are illustrated in Fig. 4.13.

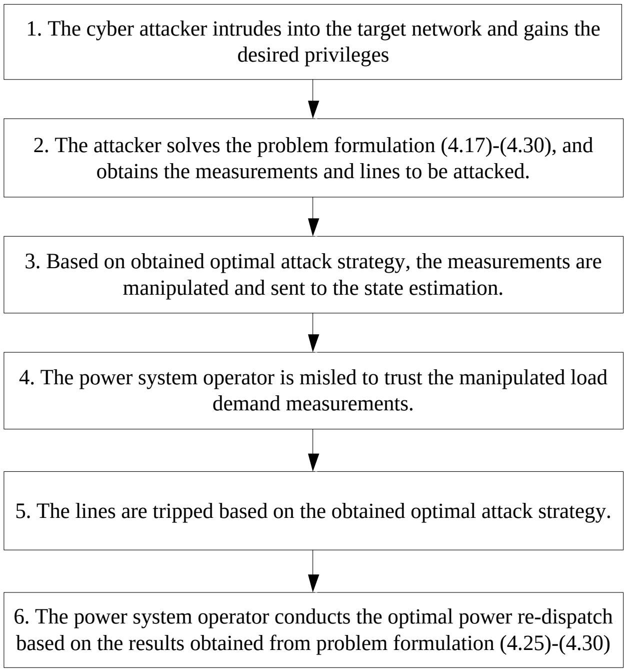

1. The cyber attacker intrudes into the target network and gains the desired privileges
2. The attacker solves the problem formulation (4.17)-(4.30), and obtains the measurements and lines to be attacked.
3. Based on obtained optimal attack strategy, the measurements are manipulated and sent to the state estimation.
4. The power system operator is misled to trust the manipulated load demand measurements.
5. The lines are tripped based on the obtained optimal attack strategy.
6. The power system operator conducts the optimal power re-dispatch based on the results obtained from problem formulation (4.25)-(4.30)

Figure 4. 13 Illustration of the LR attack coordinating with attacking lines

Currently there are very few commercial solvers which can directly solve a bilevel optimization problem. To solve the bilevel optimization problems for obtaining the attacker's optimal strategy, some transformation is needed, and the Karush-Kuhn-Tucker (KKT)-based method is applied in this study. The lower level problem represents the defender's response to the attack, it is linear and convex, thus its duality problem and the Lagrange multipliers can be obtained. So for an LR attack coordinating with attacks against lines/generators, the original bilevel problem can be transformed to an equivalent mixed-integer linear programming (MILP) problem. In this study, the obtained MILP problem is finally solved by the CPLEX solver [78].

4.6 Case Studies

In this study, the case studies are performed based on a modified IEEE 14-bus system. There are 20 lines in the test system. The capacity of the line from bus 1 to bus 2 is 160 MVA, the capacity of the line from bus 2 to bus 3 is 100 MVA, and the capacities of all other lines are 60 MVA. Other parameters associated with the test system can be found in [79]. It is assumed that the power grid is fully measured and there is a power flow measurement at each end of every transmission line, and there is a load demand measurement at each load point. So there are a total of 51 attackable measurements.

4.6.1 LR Attack Coordinating with Attacking Generators

Generally, the more important a generator is, the stronger the corresponding protection is and thus the higher the required attack cost will be. Considering this, the attack costs for the generators are assigned in proportion to their generation capacities as shown in Table 4.1. And the attack cost required to compromise each measurement is 1.

If the attack magnitude limit on the load measurement is 50%, and the total cyberattack resource is 35, after solving the bilevel optimization problem described by (4.4)-(4.16), the attacker would launch an LR attack to shift the load from bus 2, 3, 5, 6 and 9 to bus 4 which is already heavily loaded, and generator 4 would be attacked as shown in Fig. 4.14. And the system's total load curtailment is 7.52 MW which is on bus 4. Although the attacker could spend all the attack resource to trip both generators 5 and 6, the total load curtailment in this case would be 5.15 MW, which is less than that caused by coordinating LR attack and tripping generators. This validates the speculation that coordinated attacks could be more effective than a standalone attack.

Table 4. 1 Parameters of Generations

Generator	1	2	3	4	5	6
Bus	1	1	2	3	6	8
P_G^{min}(MW)	0	0	0	0	0	0
P_G^{max}(MW)	100	100	50	30	50	20

C_G	50	50	25	15	25	10

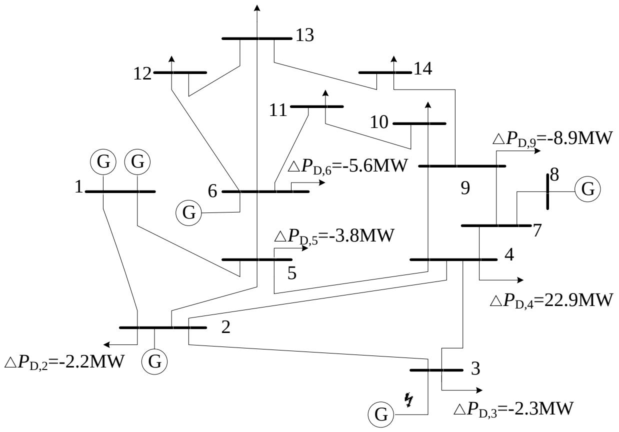


Figure 4. 14 Example of LR attack coordinating with attacking generators

When the attack resource is 50, the attacker's optimal strategy is to attack generators 4, 5 and 6. And no attack resource is spent on launching an LR attack. After tripping these two generators, the load curtailments are 7.2 MW, 4.6 MW and 14.9 MW on buses 5, 9 and 14, respectively.

Table 4. 2 Comparisons of different attack strategies

Cyberattack resource	Attack strategy	Load curtailment (MW)
35	Coordinated attack	7.52
	LR attack	0
	Generator attack	5.15
45	Coordinated attack	22.1
	LR attack	2.4
	Generator attack	7.1
55	Coordinated attack	28.6
	LR attack	3.1
	Generator attack	26.4

In order to demonstrate the advantages of the proposed coordinated attack strategy, it is compared with two pure attack strategies, i.e., LR attack and generator attack. The comparison results are provided in Table 4.2. For cases where the cyberattack resource is 35, 45 and 55, the load curtailment for each attack strategy is calculated. It is shown that in these conditions the load curtailment for the coordinated attack strategy is always the maximal, which proves that coordinated attack strategy is more effective than the LR attack and generator attack.

The sensitivity analysis for the cyberattack resource is performed to investigate the contribution of the LR attack as shown in Fig. 4.15. Besides the load curtailment, it also indicates whether the attacker's optimal strategy is based on only attacking generators or the combination of attacking both generators and measurements. It is shown that when the attack resource is too small, no load curtailment will be caused as the power grid has certain redundancies to resist the weak attacks. With the increase of attack resource, the attacker could maximize the load curtailment, possibly by attacking only generators, or by attacking both generators and measurements. When the attack resource is high enough, attacking the measurements would not be considered in developing the optimal attack strategy. This is because although attacking generators is more costly, generally it is more effective than the LR attack - thus the attack against generators receives a higher priority. With enough attack resource, the generation capacity will be significantly reduced, which can cause a large amount of load curtailment. With great generation removing and load curtailment, the power flow on the lines will drop to the level which is far below the line transmission capacity. This makes it ineffective to launch an LR attack.

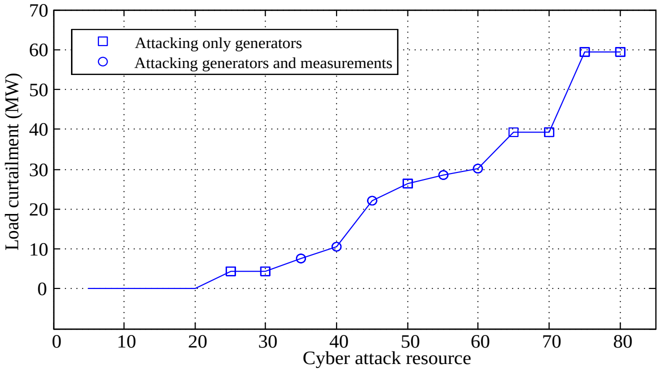


Figure 4. 15 Sensitivity analysis for the cyberattack resource

It is obvious that the load measurement attack magnitude limit τ has a significant influence on the LR attack's performance. The increase of τ will allow the attacker to have more space to manipulate the load measurements, which may result in more severe damage. Thus it can be regarded as a parameter indicating the defense level of power system. The influence of τ on the power system reliability is illustrated in Fig. 4.16. It can be seen that in general the increase of τ will facilitate the attacker to bring more load curtailment to the power grid. If the power system operator makes efforts to detect the abnormal load changes, the reliability of power system will be somehow increased in the event of coordinated attacks. Detection of load measurement attacks could be accomplished by comparing the loads with historical data and deploying secured load measurement units, etc.

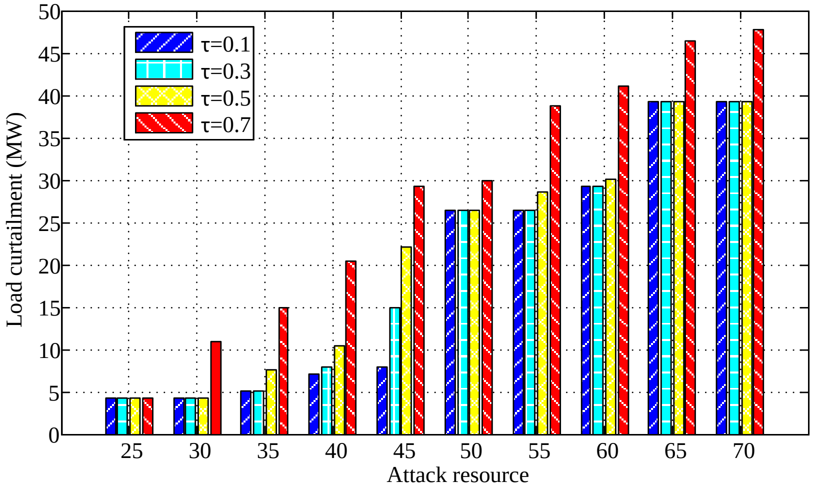


Figure 4. 16 Influence of load measurement attack magnitude limit τ

Table 4. 3 Influence of the security factor

Security factor	Load curtailment (MW)
1.0	22.1
1.1	10.5
1.2	7.5
1.3	5.2
1.4	4.3

As shown in Equation (4.10), a target of attack is associated with certain cost. The cost represents the difficulty of attacking that target, and more specifically it is related to the security level of the target. The security of the target can be improved by several approaches, such as conducting intrusion testing to reduce the vulnerabilities, i.e., the attack cost is improved. The security factor φ is introduced for analyzing the influence of the intrusion testing, and the original attack costs are updated by multiplying φ, which indicates that more cost is needed to attack a target with the intrusion testing conducted. And a more thorough intrusion test can lead to increased attack cost. In order to test the influence of intrusion testing, a sensitivity study is conducted regarding the security factor when the cyberattack resource is 45. For different values of the security factor, the load curtailments are calculated, and the results are shown in Table 4.3. It clearly shows that the load curtailment decreases rapidly with the increase of the security factor. It indicates the intrusion test can contribute to mitigating the consequence of attack.

4.6.2 **LR Attack Coordinating with Attacking Lines**

In this part, case study is performed to illustrate the optimal strategy to coordinate LR attack and the attack against lines. By solving the bilevel optimization problem described by (4.17)-(4.30), the optimal attack strategy is shown in Fig. 4.17. The associated parameters are as follows: the cyber and physical attack resource of the attacker is 25 and 1, respectively; the attack cost required to compromise each line is 1; τ is set as 50%.

Fig. 4.17 shows that the attacker could launch an LR attack to shift the loads from buses 2, 6 and 9 to buses 3 and 4. And in this case the line from bus 5 to bus 4 would be easily overloaded in the perceived state estimation. Besides the LR attack, the line from bus 1 to bus 2 will be physically tripped as it is the major transmission line to transfer the generation from the high-capacity generators located in bus 1. By tripping that line the transmission capacity is greatly reduced. The detailed load curtailments for the coordinated attacks are presented in Table 4.4. In order to demonstrate the effect of coordinated attacks, the load curtailment results are also shown in Table 4.4 if only the line is attacked. By comparison, it is concluded that if the attacker sabotages certain critical lines to reduce the transmission capacity as well as manipulates the measurements to mislead the operator to make uninformed power dispatch, the combined results could be more severe.

Table 4. 4 Load curtailment comparison for different attack strategies

	Bus number	Coordinated attacks	Only attacking the line
Load loss on bus (MW)	2	0	4.5
	3	5.4	13.5
	4	0	10.1
	5	0	0.2
	6	0	2.2
	9	20.7	6.2
	10	9.0	3.0
	11	3.5	1.5
	12	0	1.6
	13	0	2.8
	14	14.9	3.7
Total load curtailment (MW)		53.5	49.3

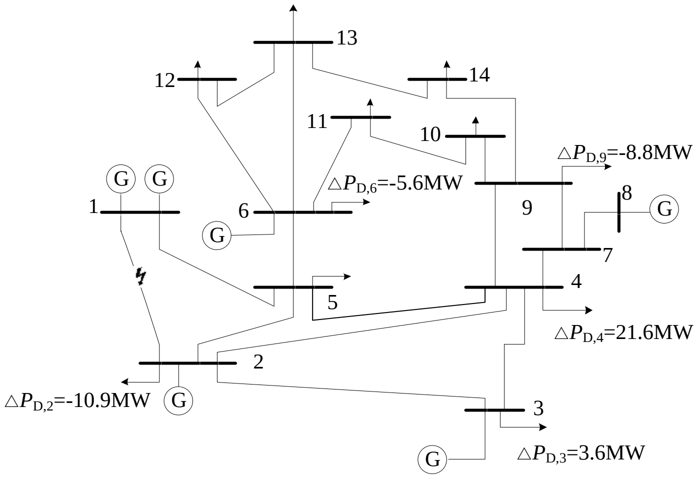

13
12
14
11
10
$\triangle P_{D,9}$=-8.8MW
G
G
$\triangle P_{D,6}$=-5.6MW
1
6
9
8
G
G
7
4
5
$\triangle P_{D,4}$=21.6MW
2
$\triangle P_{D,2}$=-10.9MW
G
3
G
$\triangle P_{D,3}$=3.6MW

Figure 4. 17 Example of LR attack coordinating with tripping a line with cyberattack resource of 25

Another case study is conducted when the attacker has cyberattack resource of 45 and physical attack resource of 1; it means the attacker can attack 45 measurements and trip 1 transmission line at maximum. The coordinated attack strategy is calculated and shown in Fig. 4.18, and it can result in 59.6 MW load curtailment. In order to demonstrate the advantages of the proposed coordinated attack strategy, it is compared with alternative attack strategies as shown in Table 4.5. From Table 4.5, it can be seen that if the attacks are not coordinated, the attacker with the cyber resource of 45 and physical resource of 1 can maximally cause 51.7 MW load loss, which combines the loss caused by LR attack and the loss caused by line attack. That is obviously lower than in the coordinated attack strategy, and this proves that the coordinated attack strategy can result in more severe consequence.

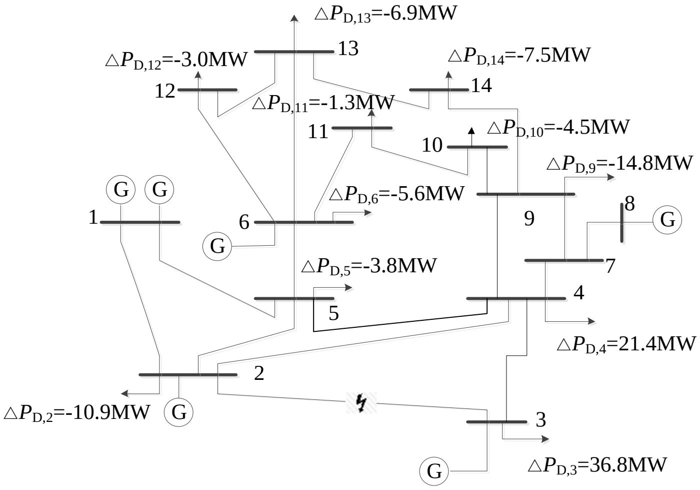


Figure 4. 18 Example of LR attack coordinating with tripping a line with cyberattack resource of 45

Table 4. 5 Comparison with different attack strategies

Resource	Attack strategy	Load curtailment (MW)
Cyber resource 45 and physical resource 1	Coordinated attack	59.6
Cyber resource 45	LR attack	2.4
Physical resource 1	Line attack	49.3

For the computation time and scalability of the proposed method, it is found that it takes about 1 minute to solve the problem in the IEEE 14-bus system using a PC with four 2.9 GHz cores and 8 GB memory. As can be seen in (4.4)-(4.16), and (4.17)-(4.30), the proposed coordinated attack strategy consisting LR attack and generator/line attack is first formulated as a bilevel problem. The bilevel problem can be transformed into a mixed integer linear programming (MILP) problem. The computation time is mainly spent on solving this MILP problem. With the increase of the size of the system, the size of this MILP program increases correspondingly, thus the computation time will also increase. If the system size is very large, the computation speed may need to be improved for quickly identifying the attacker's optimal attack strategy. The following efforts can be made:

(1) Improving the solution method for the bilevel problem. There are various ways to solve the bilevel problem, if the method for solving the bilevel problem is improved, the computation time can be reduced. Some papers have devoted to increase the computation speed, such as [80]

(2) Deploying advanced computation platform. If the problem is solved using some high-performance computation platforms, such as cloud computing, less computation time is needed.

4.7 Conclusions

In this study, the cyber-physical security of the modern power grid was analyzed from the cyber, physical and human aspects. Based on the working principle of the power system, the representative coordinated attack scenarios were analyzed. A general bilevel framework was proposed to study the coordination between LR attack and other disruptive attacks. Two specific attack scenarios were investigated in detail: the coordination between LR attack and cyberattack against generators; the coordination between LR attack and physical attack against lines. The case studies were conducted on a representative IEEE 14-bus system and they showed that by attacking the critical generation or transmission elements and manipulating deliberately selected measurements in coordination, the operation of the power grid might be disrupted and the power system operator could be misled to develop an uninformed power dispatch strategy, thus the load curtailment could be maximized. It is suggested that effective methods should be deployed to prevent possible coordinated attacks.

.

5. A Robustness-Oriented Power Grid Operation Strategy Considering Attacks

5.1 Introduction

Considering the increased cyber-physical vulnerabilities of contemporary power grids, it is important to improve the system resiliency and robustness in the face of possible attacks. This is of great importance, as it is not guaranteed that the attacks can always be detected and thwarted. For the resiliency and robustness of electric power grids, currently there are no clear and universally accepted definitions for them [81], [82], and sometimes these two terms are used interchangeably [81], [83]. In [81], it is mentioned that the robustness focuses on the ability to resist disturbances while resiliency focuses on the survivability and rapid recovery. In [82], a systematic resiliency construct is proposed and robustness is a critical part of resiliency, as shown in Fig. 5.1. In this construct, the system resiliency can be divided into long-term resiliency and short-term resiliency, which correspond to the planning stage and the operating stage, respectively. Long-term resiliency is most often related to purchasing and installing new devices coupled with improving management strategies. Short-term resiliency includes robustness prior to an event, resourcefulness during an event, and rapid recovery after an event.

Various methods can be implemented for detecting possible attacks (including cyberattacks, physical attacks, or coordinated cyber-physical attacks), such as firewalls and intrusion detections systems in the cyber network, video cameras in the substations and control centers, and the patrolling of the police. Unfortunately, there is no guarantee that the attacks could be efficiently detected. Considering this, it is of critical importance to make the power system operate in a robust state so as to resist the disturbances caused by malicious attacks. In this case, even if the disturbances are successfully caused by the attacks, the undesirable consequence could be minimized. For example, the attacker may exploit the vulnerabilities in a substation network and gain the needed privilege to send fabricated commands to open all the breakers simultaneously in the substation and isolate this substation. This can possibly cause a great cascading failure or even a complete load loss if the system is not in a robust state. Rather, the load loss can be minimized if the power system operates in a robust state and is capable of resisting the disturbance.

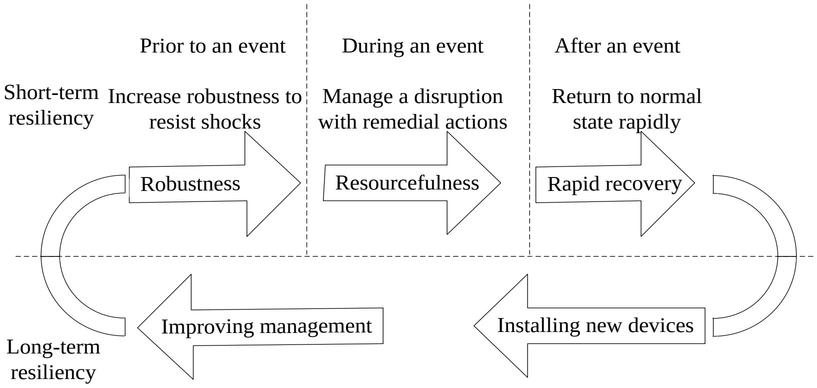


Figure 5. 1 Resiliency construct of power systems

In sum, generally there are two ways to defend a power system if it is under an attack or an attack is anticipated. One is to enhance security countermeasures, such as intensified cyber scanning and physical patrolling, to detect and thwart the attack [84]. The other is to adjust the power system operating state so as to increase the robustness of the power grid. While a number of research has been conducted regarding the first measure, little work has been done on how power system operation strategies should be adjusted so as to enable the power grid to be more resistant to significant attacks.

A typical way to improve the power system’s robustness is to incorporate the security constraints into the operation strategy. Conventionally, to ensure the power grid’s economic and secure operation under both normal conditions and possible random contingencies, SCOPF analysis is adopted as an effective method to optimize the system’s operating state in order to enable the power grid to withstand potential credible contingencies without damaging equipment and shedding loads. While there can be some variations in the specific formulations of SCOPF, however, the existing work on SCOPF with N-1 security criteria generally only considers the outages of a generator or a transmission line as a credible outage scenario. Obviously, this limits the power system's capability of dealing with more serious contingencies, such as the loss of a substation and the simultaneous tripping of multiple transmission lines. These are probable contingencies in a cyber-physical environment that could be caused by intelligent, coordinated attacks. They could pose a great threat to the power system operation and should be considered.

5.2 Attacks and Resultant Impacts

5.2.1 Attack Cases

The power system primarily consists of two parts: the physical current-carrying system and the cyber monitoring and control network. The power system's cyber supervisory control and data acquisition (SCADA) system transmits measurements, alarms and operation commands between the widely distributed substations and the control centers. Both the cyber and physical layers could be targeted and attacked. Depending on the specific targets of attacks and methods, there can be numerous possible attack strategies.

For example, a capable attacker could intrude into the substation local computer by exploiting the vulnerabilities in the protocols or operating systems to gain the desired control privilege. Then, in the worst-case scenario, the attacker could send fabricated commands to trip all the breakers controlled by the local substation computer. This may cause a sudden isolation of the attacked substation and possibly trigger cascading failures. Highly capable attackers may be able to attack more than one substation, which might lead to even worse consequences. Another attack scenario is related to the simultaneous tripping of multiple meticulously selected transmission lines. The unexpected tripping of these lines could bring a significant disturbance to the power system operation, and possibly result in second-order failures. It is also possible that the attacker could simultaneously attack different types of power grid components including buses and branches.

There are usually a number of substations and transmission lines in a bulk power system, so it is challenging for the attacker to identify the most critical substations and lines that may lead to the most severe consequence if being compromised. However, it is wise for the defender to consider the worse-case scenario when deciding the power dispatch strategy. Thus, no matter whether the attacker is able to successfully identify the most valuable targets or not, it is reasonable for the defender to minimize the worst consequence that can be caused by the attacker, which is the focus of this study.

The possible attack scenarios can be conceived by experienced operators, and they may vary with time, terrorism activity patterns, and geographical locations. It is expected that in the future imminent attacks against power grids and the corresponding risk levels would be advised ahead of time, similar to the existing National Terrorism Advisory System developed for enforcing homeland security by issuing alerts and warning notifications and elevating security levels according to intelligence agencies [85].

5.2.2 Impact Analysis of Attacks

For the possible attack scenarios, the impact should be estimated for deciding the optimal operating strategy. The risk of attacks against power systems is determined by three factors: the power system operating state, the target of attack and the system configuration, as shown in Fig. 5.2. The targets of attack can be lines, generators, and substations. The power system operating state is characterized by the output of each generator, the voltage at each bus, and the power flow of each branch and the load demand at each load bus, etc. The system configuration contains information on the power system topology, the number of generators, and the number of transmission lines.

The analysis of cascading failures in electric power systems is a challenging task, and multiple methods have been developed based on different mechanisms. In some studies, such as [86], the cascading failure is simulated based on pure topological analysis. The computation is fast but it should be applied with caution, as the flow pattern is different from that based on strict power flow analysis. Some work performs cascading failure simulations based on DC power flow analysis, such as the OPA model [87]. However, DC power flow analysis has known disadvantages as it cannot truly reflect bus voltage behaviors and has a poor capability to model the dynamic instability. The AC power flow based models such as those in [75] are computationally intensive and have to make assumptions when power flow analysis does not converge. Despite these efforts to model cascading failures, there are no cascading failure models without an obvious limitation. An ideal cascading failure model needs to consider all the associated cyber, physical, and human factors, such as power flow analysis, instability analysis, load demand uncertainties, operators' response, protection failures, and cyber-physical interactions. However, such a comprehensive and computationally-efficient model has not been developed in the existing research thus far.

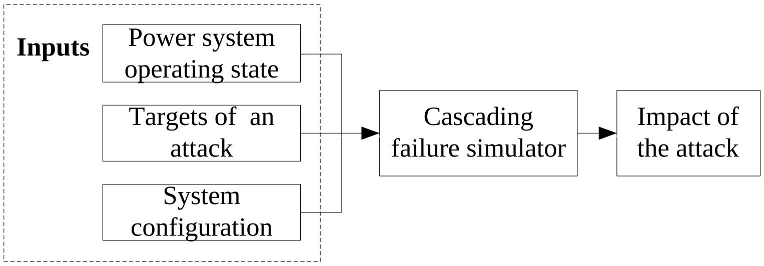


Figure 5. 2 Risk of attack against power system

As this chapter is focused on investigating the influence of operating state on the cascading failure risk considering different attack scenarios, the detailed modeling of cascading failures is outside the scope of this study. The cascading failure simulator in [43] is adopted in this study, whose working principle is illustrated in Fig. 5.3.

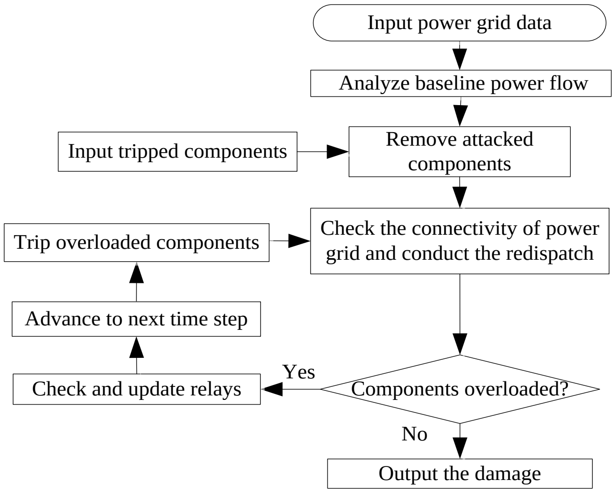

Input power grid data
Analyze baseline power flow
Input tripped components
Remove attacked components
Trip overloaded components
Check the connectivity of power grid and conduct the redispatch
Advance to next time step
Yes
Check and update relays
Components overloaded?
No
Output the damage

Figure 5. 3 Cascading failure simulation flowchart

5.3 Problem Formulation

5.3.1 General *SCOPF* Formulation

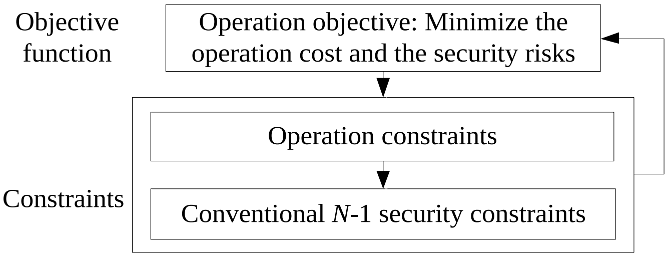

Objective function
Operation objective: Minimize the operation cost and the security risks
Operation constraints
Constraints
Conventional N-1 security constraints

Figure 5. 4 Conventional SCOPF framework

As shown in Fig. 5.4, in the conventional *N*-1 contingency constrained OPF analysis, usually the random failure of one system element is considered such as the tripping of one transmission line/generator caused by aging, storms, or vegetation contact. If the SCOPF only considers random failures, the power system has limited resistance against well-planned attacks that could result in simultaneous tripping of multiple devices - the consequence could be disastrous.

A representative formulation of the SCOPF with N-1 security consideration can be described as follows [88]- [89]:

$$\text{Minimize } \ f_0\left(x_0, u_{f0}, u_{s0}\right) \tag{5.1}$$

$$\text{s.t.} \quad g_0\left(x_0, u_{f0}, u_{s0}\right) = 0 \tag{5.2}$$

$$h_0\left(x_0, u_{f0}, u_{s0}\right) \leq h_s^{max} \tag{5.3}$$

$$g_c^0\left(x_c^0, u_{fc}, u_{s0}\right) = 0 \qquad c \in C \tag{5.4}$$

$$h_c^0\left(x_c^0, u_{fc}, u_{s0}\right) \leq h_f^{max} \quad c \in C \tag{5.5}$$

$$\left|u_{fc} - u_{f0}\right| \leq \varepsilon_{fc}^{max} \quad c \in C \tag{5.6}$$

$$g_c\left(x_c, u_{f0}, u_{sc}\right) = 0 \qquad c \in C \tag{5.7}$$

$$h_c\left(x_c, u_{f0}, u_{sc}\right) \leq h_s^{max} \quad c \in C \tag{5.8}$$

$$\left|u_{sc} - u_{s0}\right| \leq \varepsilon_{sc}^{max} \quad c \in C \tag{5.9}$$

where the objective function f_0 represents the total generation cost in the normal state; x is the state variables of the power grid; u is the control variables; g and h are the equality and inequality constraints of the SCOPF model, respectively; and ε is the control variable adjustment limits. The subscripts 0 and c refer to the normal state and contingency state, respectively. The subscripts f and s indicate the fast corrective control and slow corrective control, respectively. C represents the predefined contingency set.

Equations (5.2), (5.4) and (5.7) are the set of equality constraints for ensuring the active and reactive power balances at every bus. Expressions (5.3), (5.5) and (5.8) are the sets of inequality constraints indicating the active and reactive power generation limits, bus voltage limits, transmission line power flow limits, etc. Expressions (5.6) and (5.9) are the coupling control variable adjustment limits, which mainly represent the active power generation ramping limits and other possible short-term control variable limits such as spinning reserves.

5.3.2 Extended SCOPF Formulation Considering Attacks

In recent years, possibilities of different forms of attacks are increasing rapidly due to more active terrorism activities and the wider deployment of cutting-edge emerging smart grid technologies, especially those deployed in the cyber layer. Consequently, it is natural and pressing to extend the conventional SCOPF to incorporate probable attack scenarios. In this way, the power system should not only withstand the outage of a traditional credible contingency, but also have a certain degree of robustness to intelligent malicious attacks.

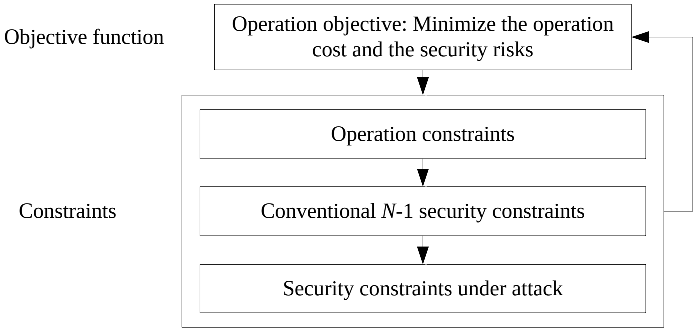

Objective function
Operation objective: Minimize the operation cost and the security risks
Constraints
Operation constraints
Conventional N-1 security constraints
Security constraints under attack

Figure 5. 5 An extended SCOPF framework considering probable attack scenarios

The framework for incorporating the attack scenarios into the SCOPF is proposed as shown in Fig. 5.5. The objective function is to minimize the operation cost and the security risks. The constraints consist of three aspects: operational limitations in the normal state; conventional *N*-1 security constraints; and security constraints under well-organized attacks. The operational constraints can be represented by (5.2)-(5.3); the *N*-1 security constraints can be represented by (5.4)-(5.9); and the security constraints associated with the attacks can be defined by the operator.

The major difference between the proposed extended SCOPF and the conventional SCOPF is that a security constraint set related to probable attacks is added. The conventional SCOPF only considers random failures, such as the failure of a transmission line or a generator. Since simultaneous failures of multiple components could rarely happen, generally they are not considered in traditional power system planning and operations. However, intelligent attackers could make meticulous plans to trip multiple components simultaneously, which do not fall into the traditional category of credible contingencies. Generally, the conventional SCOPF can be applied under normal conditions, and the proposed SCOPF should be enforced when a potential imminent attack is advised by national or regional security agencies. Several issues should be dealt with when applying the proposed SCOPF. First, the targets of attacks should be estimated. The targets could be to simultaneously trip lines, generators, substations, or a combination of different components, etc. Second, the probability of a successful attack should be estimated.

5.3.3 Short-Term Post-Contingency Feasibility Check

After the failure of a single element in the N-1 analysis, the power grid should be capable of withstanding the short-term disturbance and preventing system collapse before the corrective actions are taken. This is represented by (5.4)-(5.6). In this study, it is assumed that the short-term post-contingency feasibility is satisfied if each branch power flow does not exceed its short-term rating. If the power flow of a branch exceeds the short-term rating, this branch would be tripped shortly before the operator takes remedial actions to reduce the power flow in that branch, thus more second-order failures could happen. The short-term feasibility modeling could be very complicated when considering the fast-response operating reserves, energy storages, and automatic generation controls.

In principle, if this short-term post-contingency feasibility check is not considered, the operational margin of the power system can become larger, which would lead to improved results, i.e., reduced operation cost and/or reduced risks due to attacks.

5.3.4 Long-Term Post-Contingency Feasibility Check

For every possible failure scenario in the *N*-1 analysis, if there is at least one violation (e.g. a line overloading), it is checked whether there exists a feasible corrective action strategy to remedy the situation. This is represented by (5.7)-(5.9). Specifically, this feasibility check is conducted based on the following long-term post-contingency optimal power flow analysis [88].

$$\text{Minimize} \quad zs_c = sum(z_c) \tag{5.10}$$

$$\text{s.t.} \quad g_c\left(x_c, u_{f0}, u_{sc}\right) = 0 \tag{5.11}$$

$$h_c\left(x_c, u_{f0}, u_{sc}\right) \le h_s^{max} \tag{5.12}$$

$$|u_{sc} - u_{s0}| \le \varepsilon_{sc}^{max} + z_c \tag{5.13}$$

$$z_c \ge 0 \tag{5.14}$$

where z_c is the relaxation vector, and zs_c is the sum of all the elements in z_c. For each contingency scenario *c*, if the above OPF analysis does not converge or if the outcome zs_c is greater than zero, it indicates that the current solution point is infeasible for contingency *c*.

5.3.5 Post-Attack Impact Analysis

Within the limited capability, the attacker usually have multiple target(s) to attack. For example, for a bulk power system with n_b buses and n_l transmission lines, the attackers can have $\binom{n_b}{2}$ alternative targets if they have the capability to isolate two buses. Denote *a_max* as the total number of possible targets of attacks, and in this case, *a_max* =$\binom{n_b}{2}$. If attackers' capability allows them to attack two transmission lines, the number of targets a_max in this case is $\binom{n_l}{2}$. The number of alternative targets could be tremendous for a bulk power system, which increases rapidly with the increase of the attacker's capability.

Although the attacker could have multiple potential targets, it is reasonable for the defender to strive to minimize the most detrimental impact that could be caused by the attacker. Let $Loss_a$ represent the load curtailment caused by attack scenario a. The maximum loss is denoted by

$$Loss_a^{max} = \max(Loss_a) \quad a = 1, \dots, a\_max \tag{5.15}$$

In a more realistic sense, the defender may not know exactly the attacker's capability and the related targets of attack when performing the power dispatch, but has to consider multiple possible situations, e.g., attacking one substation with a probability of 0.5 and two transmission lines with a probability of 0.5. Generally, assume there are M possible attack situations, and the probability of the attack situation m is $p(m)$, the expected loss E_{loss} is calculated as follows:

$$E_{loss} = \sum_{m=1}^{M} p(m) Loss_a^{max}(m) \tag{5.16}$$

$$\sum_{m=1}^{M} p(m) = 1 \tag{5.17}$$

According to the meaning of robustness discussed in the Introduction chapter, a power system operating in a robust state should have less load loss after being attacked; on the other side, a power system state of less robustness can result in a more serious load loss in the face of attacks. Thus, the load loss after attacks can indicate the power system's robustness, which is used to quantitatively measure the robustness in the following analyses and case studies.

5.4 Parallel Hybrid Solution Methodology

A hybrid strategy is proposed in this study to solve the problem defined in Chapter 5.4 [90].

5.4.1 **Computation Strategy**

1) *Objective Function*

The extended SCOPF incorporating attacks considers generation cost in the normal state, the N-1 contingency risk and the risk of attacks. All these three aspects are considered in the objective function as shown below:

$$f = f_0(x_0, u_{f0}, u_{s0}) + \alpha(\sum_{c=1}^{c\_max} p_c \times OF_k(c) + pe) + p_A \times \pi \times E_{loss} \tag{5.18}$$

where α is the coefficient to penalize the conventional N-1 violations; *c_max* is the total number of N-1 contingencies; p_c is the probability of contingency *c;* $OF_k(c)$ is the sum of the line violations; k is the selected critical contingency in the iteration; pe is the penalty; p_A is the probability that an attack could happen and it can be estimated by the security agency and may vary with time; and π is a factor to measure the impact of load loss in terms of monetary value in the unit of $/MW.

2) *Illustration of the Solution Method*

Table 5. 1 Illustration of the solution method

	PSO	SCOPF
Objective function	f in Eq. (5.18)	f_0 in Eq. (5.1)
Control variables	P_G^{max}	u_f, u_s
Outcome	Global solution	Candidate solution P_k^*
Decomposition strategy	Globally shrink the feasible solution region	Locally solve the SCOPF in the shrunk region
Parallelization strategy	Parallel	Sequential

The decomposition of the hybrid method is shown in Table 5.1. PSO (Particle Swarm Optimization) is a widely used artificial intelligence based method with the advantages of simplicity, global search capability, and robustness [91]. The PSO is applied to globally search the feasible region for the SCOPF by confining the upper bounds of control variables. In this study, control variables refer to the maximum generation active power outputs, and a set of them forms a feasibility region. For every feasibility region found by a PSO particle, the SCOPF is solved by the PDIP procedure in the Matpower package [79] to derive a candidate solution P_k^* .

3) Steady-State Security Assessment (SSSA)

In this study, the SCOPF in each iteration includes not only the normal state but also a critical contingency k. After the SCOPF obtains a solution point P_k^* for the power grid operation, it is checked for every contingency $c \in C$ based on AC power flow analysis. The SSSA is performed to update the critical contingency k and check the feasibility of the obtained solution.

For each contingency, the overloading level $OF_k(c)$ is calculated as follows:

$$OF_k(c) = \sum_{b=1}^{b\_max} (PF_b^{max} - abs(PF_b(c)))\ c \in\ C \quad (5.19)$$

where PF_b is the power flow on the transmission line b; PF_b^{max} is the transmission line capacity for line b; and b_max is the total number of transmission lines.

4) Contingency Filtering

For every checked contingency, if there is a violation, the long-term post-contingency feasibility check should be conducted, which is however time-consuming. So it is desirable to check as few post-contingencies as possible. Here $n_v(c)$ is defined as the number of violations, and the contingency c with the least number of violations is chosen to update the critical contingency k.

5.4.2 Computational Procedure

The procedure of the solution method is depicted in Fig. 5.6 and the major steps are illustrated as follows.

Step 1: Initialize the PSO parameters, especially the range of the upper bounds of active power generations. Each particle is defined as the set of upper bounds for the active generations and thus the dimension of a particle is the number of generators.

Step 2: Randomly choose an initial critical contingency k. This is different from the algorithm in [90] where the initial critical contingency k is empty.

Step 3: Solve the optimal power flow defined by each particle. The optimal power flow consists of expressions (5.1)-(5.3) and (5.7)-(5.9) where the contingency set C includes only k. If the optimal power flow calculation does not converge, the objective function in (5.18) is set to infinity and go to step 12; otherwise, a candidate solution point P_k^* is obtained and go to the next step.

Step 4: Calculate the system state under each contingency in the contingency set C by using AC power flow analysis. The contingency set is predefined and it includes the failures of every generator and every transmission line in this study. The overloading level $OF_k(c)$ is calculated for each contingency c.

Step 5: Based on the power flow analysis results obtained in step 4, a candidate contingency *k_c* is proposed for each particle. And the candidate contingency with the largest occurrence time for all the particles is chosen as the contingency k.

Step 6: Check the short-term and long-term feasibilities of each contingency as described in Chapter 5.4. If they are infeasible, a penalty pe is added to the objective function in (5.18).

Step 7: Estimate the possible attack conditions, the probability of each condition and the possible targets for each attack condition.

Step 8: For each possible target of attack under each attack condition, its consequence is calculated based on the cascading failure simulator depicted in Fig. 5.3.

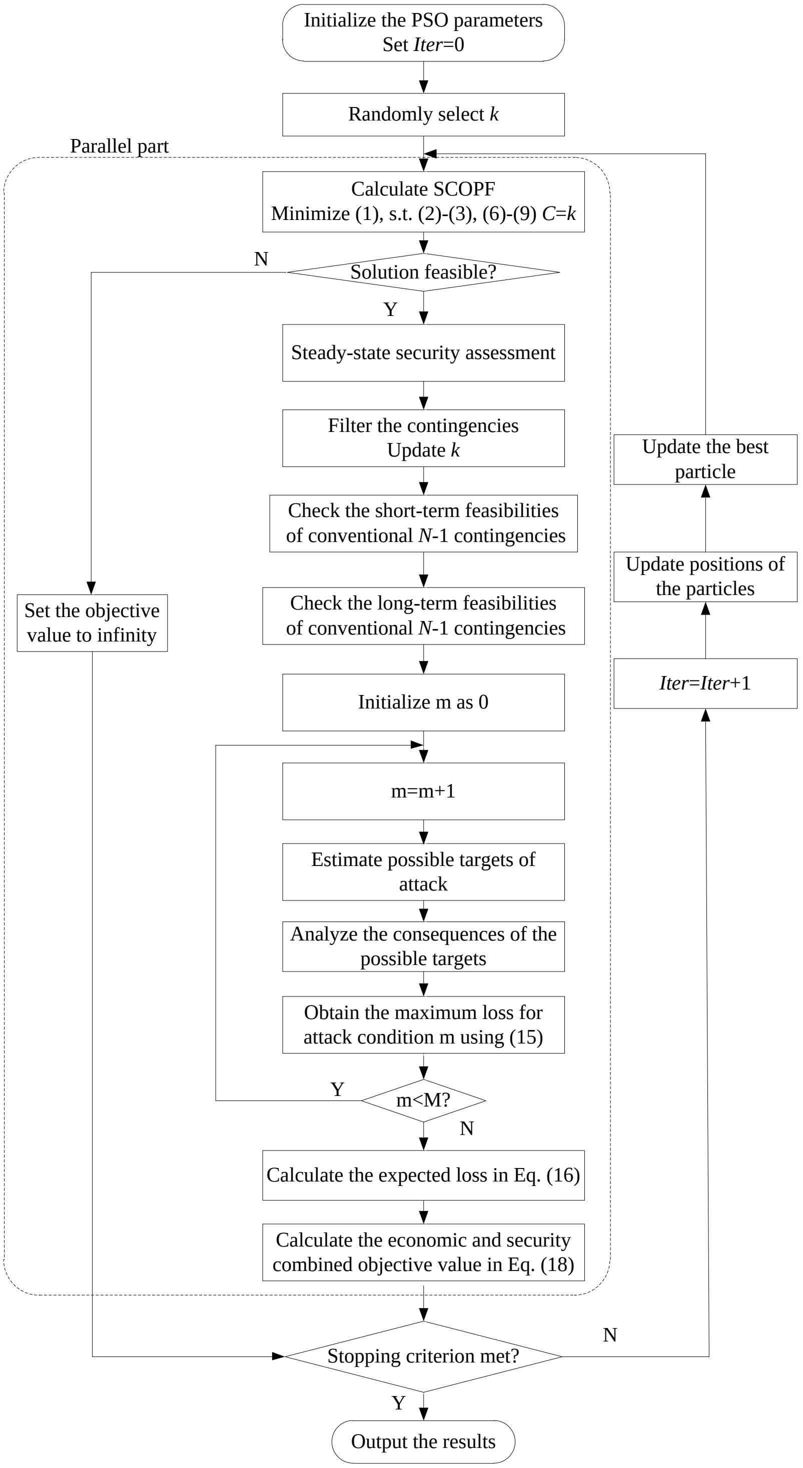

Initialize the PSO parameters
Set Iter=0
Randomly select k
Parallel part
Calculate SCOPF
Minimize (1), s.t. (2)-(3), (6)-(9) C=k
N
Solution feasible?
Y
Steady-state security assessment
Filter the contingencies
Update k
Check the short-term feasibilities of conventional N-1 contingencies
Check the long-term feasibilities of conventional N-1 contingencies
Set the objective value to infinity
Initialize m as 0
m=m+1
Estimate possible targets of attack
Analyze the consequences of the possible targets
Obtain the maximum loss for attack condition m using (15)
Y
m<M?
N
Calculate the expected loss in Eq. (16)
Calculate the economic and security combined objective value in Eq. (18)
Update the best particle
Update positions of the particles
Iter=Iter+1
N
Stopping criterion met?
Y
Output the results

Figure 5. 6 Procedure of the hybrid solution methodology

Step 9: Calculate the maximum loss under each attack scenario using (5.15).

Step 10: Check if all the attack scenarios are considered, if not go to step 8; otherwise, calculate the expected loss using (5.16).

Step 11: Update the overall objective function in (5.18) considering the operation cost, N-1 contingencies and the expected loss caused by attacks.

Step 12: Check whether the stopping criterion is satisfied. The stopping criterion can be the convergence of the PSO or the maximum number of iterations. If the stopping criterion is not met, go to step 13; otherwise stop the program.

Step 13: Update the positions of particles based on the rules of the PSO algorithm, then return to step 3.

5.5 Case Studies

The proposed SCOPF analysis incorporating attacks is verified on the IEEE 14-bus, IEEE 39-bus and IEEE 118-bus systems. The systems' data and parameters are derived from the Matpower package. The transformer off-nominal turn ratios and phase shift angles are neglected. Also, the bus shunt conductance and susceptance are not considered.

In the following case studies, the short-term rating of each transmission line is assumed to be 120% of its long-term rating. The coefficient α is set to be 1.2, and the probability for each contingency p_c is chosen as 0.01. The penalty value pe is selected as 200. It is assumed that the security agent estimates the attack occurrence probability p_A to be 0.05, and the factor π is set as 2,000 \$/MW which includes not only the revenue loss but also the inconvenience brought to the customers. These values are chosen by referring to the existing literature [90]-[91] for performing case studies in this chapter. Actually, these values can be changed for different conditions. For example, if the operator focuses more on the N-1 contingency risk, the value of α should be increased. If the power system components are aging, the probability of N-1 contingencies p_c should be increased; on the contrary, it should be decreased after a maintenance is carried out. If security agent alerts a highly possible attack, the attack occurrence probability p_A needs to be increased. Also, p_A can be set to zero if the power system operator does not consider the risk of attacks, and the proposed SCOPF problem in this case shrinks to a conventional *N*-1 SCOPF.

For comparison, analyses based on multiple OPF algorithms are conducted for each test system including the conventional *N*-1 SCOPF; the SCOPF considering attacking two lines; the SCOPF considering attacks against two buses; the SCOPF considering attacks against one bus and one line; the SCOPF considering the two possible attack conditions (attacking one substation; attacking two branches) with corresponding probabilities. In this chapter, the abbreviation BAC-OPF refers to the SCOPF considering attacks against one bus; and the abbreviation LAC-OPF refers to the SCOPF considering attacks against two lines.

The conventional *N*-1 SCOPF is the baseline, which is compared with the proposed SCOPF to demonstrate the advantage of the proposed method.

5.5.1 IEEE 14-bus System

The IEEE 14-bus system consists of 20 branches, 5 generation units and 14 buses. The transmission capacity of each branch is set to 140 MVA. So there are 25 *N*-1 contingencies. This study does not consider the contingencies that could cause an islanding. The maximum active power generation adjustment ε_{sc}^{max} for each generator in the long-term post-contingency analysis is set to be 30 MW.

1) *N*-1 *SCOPF*

If the power system operators do not consider the malicious man-made threats, the SCOPF considering the *N*-1 contingencies is applied to determine the operating state of the power system. Based on this strategy, the active power output of each generator is shown in Table 5.2. And the generation cost in this case is $8,302.

Table 5. 2 Active power outputs based on N-1 SCOPF in IEEE 14-bus system

Generator number	Power output (MW)
1	135
2	37
3	58
4	8
5	27

Under this operating condition, the risk of the power system under attacks can be calculated. If the attacker has the capability to isolate a bus, the impact is shown in Table 5.3. The maximum load loss is resulted in when bus 1 is isolated, and 46% of the load will be curtailed. It indicates that the power system under this operating strategy is vulnerable to a bus-isolating attack.

Table 5. 3 Loss for bus-isolating attack in 14-bus system under N-1 SCOPF

Attacked bus	Load loss ratio	Attacked bus	Load loss ratio
1	0.46	8	0.06
2	0.10	9	0.11
3	0.36	10	0.03
4	0.18	11	0.01
5	0.03	12	0.02
6	0.04	13	0.05
7	0.06	14	0.06

Table 5. 4 Loss for line-tripping attack in 14-bus system under N-1 SCOPF

Attacked lines	Load loss ratio
{1,2}	0.35
{3,6}	0.21
{11,16}	0.05
{12,19}	0.02
{16,18}	0.03
{17,20}	0.06

If the attackers have the capability to simultaneously trip two lines, there are 190 attack scenarios, and part of the high-impact results is shown in Table 5.4. The maximum load loss among all the 190 scenarios is caused when lines 1 and 2 are tripped, and the load loss ratio is 35%.

When an attack is anticipated, the informed operators can adjust the operating strategy to increase the robustness of the power system.

2) *SCOPF Considering Attacking One Bus (BAC-OPF)*

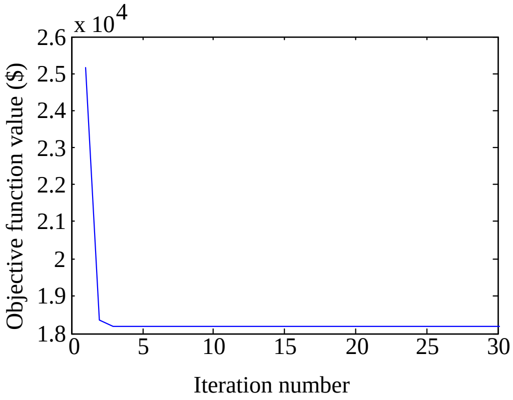


Figure 5. 7 Convergence of PSO for BAC-OPF in IEEE 14-bus system

If a bus-isolating attack is anticipated, the convergence curve of the PSO for the BAC-OPF is shown in Fig. 5.7. The convergence is reached after 11 iterations. And the power outputs of the generators are shown in Table 5.5. The total generation cost in the normal state is $8,748.

Table 5. 5 Active power outputs based on BAC-OPF in IEEE 14-bus system

Generator number	Power output (MW)
1	92
2	46
3	100
4	0
5	25

Table 5. 6 Loss for bus-tripping attack in IEEE 14-bus system under BAC-OPF

Attacked bus	Load loss ratio	Attacked bus	Load loss ratio
1	0.30	8	0.02
2	0.11	9	0.11
3	0.36	10	0.03
4	0.22	11	0.01
5	0.03	12	0.02
6	0.04	13	0.05
7	0.02	14	0.06

By comparing Table 5.2 and Table 5.5, it can be seen that the generation is shifted from generator 1 to generator 3. In this case, the generation on bus 1 is reduced, and thus when bus 1 is attacked, the resultant impact is reduced. Under the BAC-OPF, the maximum load loss is caused when bus 3 is isolated as shown in Table 5.6, which is however still smaller than that under the *N*-1 SCOPF.

To study the impact of short-term post-contingency feasibility check, when the short-term post-contingency feasibility is not considered, the power system operating state based on BAC-OPF is shown in Table 5.7. The generation cost is $8,401, and the maximum load loss ratio is reduced to 35% when bus 1 is attacked. Compared with the BAC-OPF considering the short-term feasibility as shown in Table 5.6, the load loss is a bit smaller and the cost is much reduced.

Table 5. 7 Active power outputs based on BAC-OPF without considering short-term feasibility in IEEE 14-bus system

Generator number	Power output (MW)
1	117
2	40
3	53
4	22
5	31

3) *SCOPF Considering Attacks against Two Lines (LAC-OPF)*

Table 5. 8 Active power outputs based on LAC-OPF in IEEE 14-bus system

Generator number	Power output (MW)
1	77
2	53
3	40
4	31
5	61

Table 5. 9 Loss for line-tripping attack in IEEE 14-bus system under LAC-OPF

Attacked lines	Load loss ratio
{1,2}	0.12
{1,5}	0.12
{1,15}	0.12
{2,4}	0.24
{3,6}	0.12
{7,8}	0.21

Similarly, if a line-tripping attack is anticipated, the corresponding LAC-OPF could be enforced. The outputs of generators in this case are shown in Table 5.8 and the corresponding generation cost is $8,905. Some examples are provided in Table 5.9 to illustrate the impact of line-tripping attacks, and the maximum load loss among all the 190 scenarios is resulted in when lines 2 and 4 are tripped. The amount of load loss is 24% which is lower than that in the *N*-1 SCOPF.

4) *SCOPF Considering Attacks against Two Buses*

Table 5. 10 Active power outputs in IEEE 14-bus system based on the proposed SCOPF considering attacks against two buses

Generator number	Power output (MW)
1	83
2	41
3	44
4	37
5	57

For the operating state obtained based on the *N*-1 SCOPF shown in Table 5.2, when the attacker is capable of attacking two buses at the same time, some most serious attack scenarios and the resultant consequences are shown in Fig. 5.8. The worst consequence is 95% load loss when buses 5 and 9 are attacked.

For the proposed SCOPF incorporating attacks against two buses, the system state operating state is shown in Table 5.10, which indicates the generation cost is $8,771. Based on this operating state, some most severe attack scenarios and the resultant consequence are shown in Fig. 5.9. The worst consequence among all the possible attack scenarios is resulted in when buses 1 and 2 are tripped, and the load loss ratio is 55%. This value is significantly less than that in the *N*-1 SCOPF.

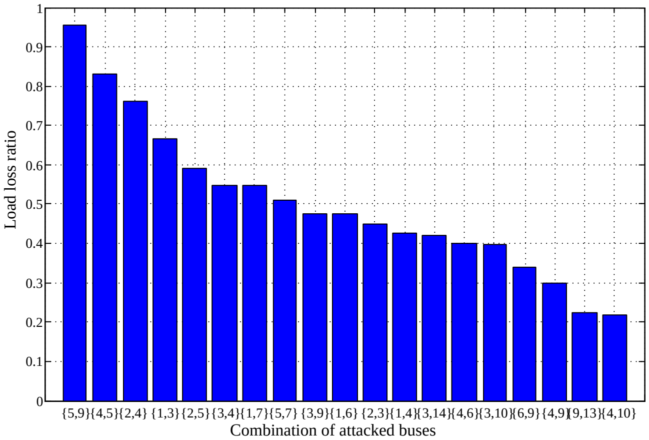


Figure 5. 8 Load loss ratio in IEEE 14-bus system based on the N-1 SCOPF when two buses are attacked

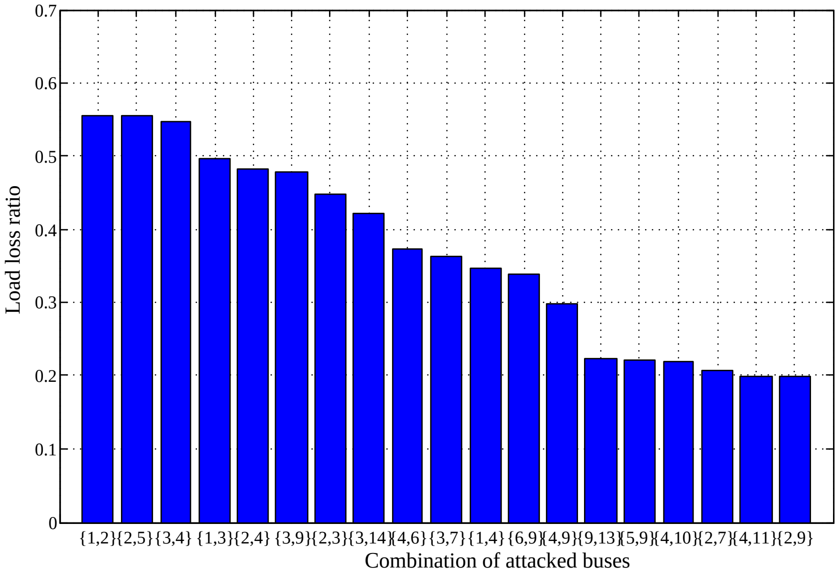


Figure 5. 9 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF when two buses are attacked

5) *SCOPF Considering Two Possible Attack Conditions*

Table 5. 11 Active power outputs in IEEE 14-bus system based on proposed SCOPF considering two possible attack conditions

Generator number	Power output (MW)
1	105
2	40
3	26
4	35
5	56

For the operating state obtained based on the *N*-1 SCOPF, when facing two possible attack conditions, attacking a bus and attacking two lines, with probabilities 0.5 and 0.5, respectively, the expected loss is 40.5% based on the consequences in Tables 5.3 and 5.4.

For the proposed SCOPF considering these two attack conditions (a bus, two lines) and the probabilities (0.5, 0.5), the obtained system operating state is shown in Table 5.6 and the generation cost is $8,541. Under this operating state, the consequences of attacks when a bus is tripped are shown in Fig. 5.10. The maximum load loss ratio when attacking a bus is 37% when bus 3 is isolated. The consequences of attacks when two lines are tripped are shown in Table 5.7. The maximum load loss ratio when attacking two lines is 31% when lines 1 and 2 are isolated. Thus, the expected loss is 34%, which is lower than 40.5% in the *N*-1 SCOPF.

Table 5. 12 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF incorporating two attack conditions when two lines are tripped

Attacked lines	Load loss ratio
{1,2}	0.31
{3,6}	0.24
{1,14}	0.09
{17,20}	0.06
{11,16}	0.05
{16,18}	0.03

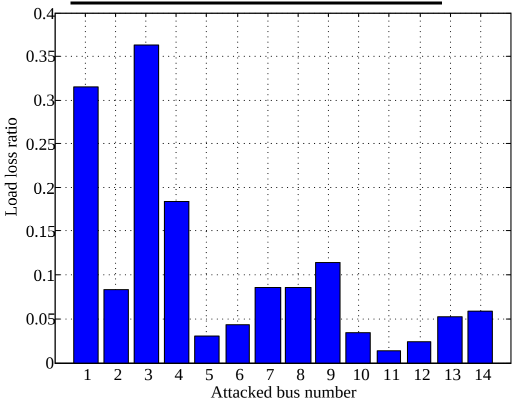


Figure 5. 10 Load loss ratio in IEEE 14-bus system based on the proposed SCOPF incorporating two attack cases when a bus is tripped

By comparing the above *N*-1 SCOPF and the four SCOPF analyses considering attacks, the operational costs in the normal state for the SCOPF analyses considering attacks go higher than that in the *N*-1 SCOPF, but the load loss ratios are always lower than those in the *N*-1 SCOPF. It shows the robustness of the power system under the proposed SCOPF incorporating attacks is clearly improved as the load losses in the optimized cases are less. By comparing the operation cost and the load loss, it is concluded that the increase of robustness comes at the cost of decreased economy.

5.5.2 IEEE 39-bus System

1) *Comparison of N-1 SCOPF, BAC-OPF and LAC-OPF*

The IEEE 39-bus system consists of 46 branches, 10 generators and 39 buses. The branch capacities are set to 125% of the values in Matpower. The maximum active power generation adjustment ε_{sc}^{max} for each generator in the long-term post-contingency analysis is set to be 30% of the maximum generation. Similar to the IEEE 14-bus system, three kinds of OPFs are analyzed and the active power output of the power system under these three conditions are shown in Table 5.8. It clearly shows that the generations are different when different attack scenarios are considered. For the *N*-1 SCOPF, the generation cost in the normal state is $41,886, and the generation cost in the normal state is increased to $43,618 for the BAC-OPF assuming the attacker has the capacity to attack one bus, and $44,997 for the LAC-OPF assuming the attacker has the capacity to simultaneously attack two lines.

Table 5. 13 Active power generation comparison for IEEE 39-bus system (MW)

Generator number	*N*-1 SCOPF	BAC-OPF	LAC-OPF
1	673	848	695
2	646	575	646
3	672	725	632
4	652	614	652
5	508	508	356
6	663	687	481
7	580	466	406
8	555	395	564
9	657	606	865
10	692	867	998

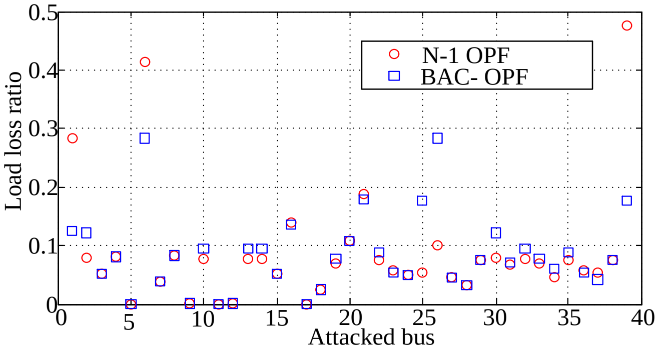


Figure 5. 11 Comparison of the impact of bus-isolating attack in IEEE 39-bus system

The system risks in the face of bus-isolating attacks using different operating strategies are compared in Fig. 5.11. When operating based on *N*-1 SCOPF, the impact of the attack can be rather serious, and the worst impact is caused when bus 39 is tripped and 47.6% of the load will be lost. Besides this worst-case scenario, there are multiple very serious scenarios. For example, 41.4% of the load will be lost if bus 6 is isolated, and 28.3% of the load will be lost if bus 1 is isolated. The risk due to attacks is greatly reduced if the power system operates based on the BAC-OPF and the maximum load loss is 28.3% when bus 26 is isolated.

Table 5. 14 Loss in line-tripping attack based on N-1 SCOPF in IEEE 39-bus

Attacked lines	Load loss ratio	Attacked lines	Load loss ratio
{35, 23}	1	{1, 19}	0.38
{38, 23}	1	{23, 2}	0.38
{35, 3}	0.47	{10, 15}	0.36
{35, 1}	0.47	{13, 1}	0.33
{38, 2}	0.47	{10, 2}	0.28
{1, 28}	0.47	{3, 1}	0.28

Table 5. 15 Loss in line-tripping attack based on LAC-OPF in IEEE 39-bus

Attacked lines	Load loss ratio	Attacked lines	Load loss ratio
{42, 23}	0.52	{19, 44}	0.38
{10, 12}	0.52	{12, 11}	0.31
{3, 23}	0.52	{10, 42}	0.19
{35, 38}	0.46	{11, 1}	0.19
{19, 18}	0.42	{45, 44}	0.12
{23, 11}	0.42	{12, 15}	0.04

In Fig. 5.11, comparing the results based on *N*-1 SCOPF and BAC-OPF, it can be seen that the load loss ratio for an individual bus may increase or decrease. However, the average loss among all the 39 attack scenarios for the *N*-1 SCOPF is 8.74%, and the average loss for the BAC-OPF is 8.49%. It can be seen not only the maximum load loss in the BAC-OPF is less than in the *N*-1 SCOPF, but also the average load loss in the BAC-OPF is less than that in the *N*-1 SCOPF, which validates the effectiveness of the proposed method.

For the line-tripping attack, it is assumed that the attacker is able to simultaneously disconnect two transmission lines. If the power system operates based on the *N*-1 SCOPF, the impact of the attack could be rather serious, and the most significant impact can be 100% load loss if transmission branches {35, 23} or {38, 23} are tripped, as shown in Table 5.14. But for the LAC-OPF, the maximum load loss ratio is 52%, which is significantly reduced as compared with the previous case, as shown in Table 5.15. This proves that the LAC-OPF can contribute to reducing the risk of line-tripping attacks.

2) *SCOPF Considering Attacks Against One Bus and One Line Simultaneously*

In a more general sense, the attacker may attack different kinds of components to initiate a cascading failure, and in this chapter a case study is considered when attacking one bus and one line simultaneously. For the operating state obtained based on the *N*-1 SCOPF, the consequences of attacks are depicted in Fig. 5.12. In several scenarios, such as attacking bus 13 and line 28, bus 14 and line 35, as well as bus 21 and line 23, the load loss ratio is 1, which means all the load demands in the system are lost.

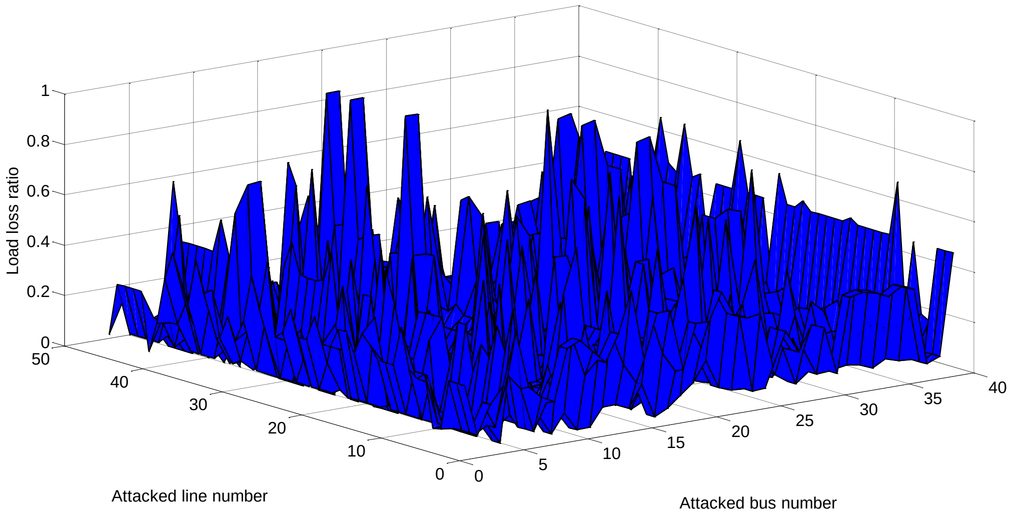


Figure 5. 12 Load loss ratio in IEEE 39-bus system based on N-1 SCOPF

For the proposed SCOPF incorporating attacking one bus and one branch, the system state operating state is shown in Table 5.16, and the generation cost is $42,097. The consequences of attack for all the 1794 possible scenarios are shown in Fig. 5.13. Among all these possible scenarios, the worst consequence is 82% load loss when bus 5 and line 35 are attacked. By comparing with the N-1 SCOPF, the maximum load loss ratio is reduced by 18%, which demonstrates that the proposed method can also be applied to cases when different kinds of components are attacked simultaneously.

Table 5. 16 Active power outputs in IEEE 39-bus system considering attacks against one bus and one line simultaneously

Generator number	Output	Generator number	Output
1	709	6	687
2	646	7	570
3	580	8	528
4	652	9	690
5	508	10	728

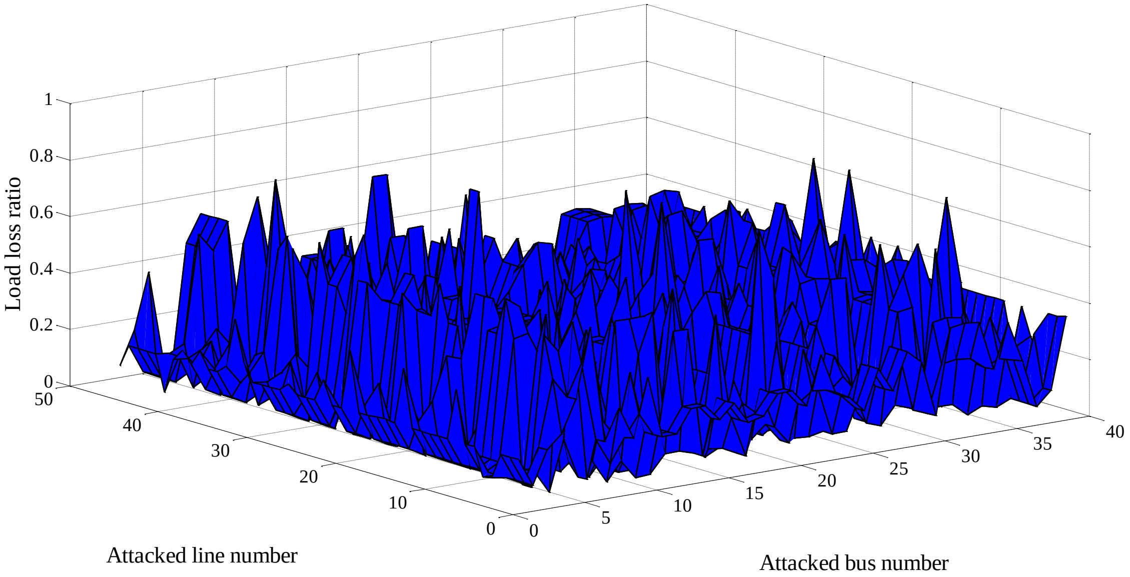


Figure 5. 13 Load loss ratio in IEEE 39-bus system based on the proposed SCOPF considering attacks against one bus and one line simultaneously

5.5.3 **IEEE 118-bus System**

The IEEE 118-bus system has 186 transmission lines, 54 generations and 118 buses. The transmission capacity of each branch is set to 200 MVA and ε_{sc}^{max} for each generator is set to be 30% of the maximum generation. If the power system is faced with bus-isolating attacks and the attacker has the capability to trip one substation, there are 118 possible targets of attack. Also, if the power system is faced with line-tripping attacks and the attacker has the ability to simultaneously trip two branches, there can be 17,205 possible targets.

Table 5. 17 Active power generation in IEEE 118-bus system

Generator number	Output (MW)			Generator number	Output (MW)		
	N-1 SCOPF	BAC-OPF	LAC-OPF		*N*-1 SCOPF	BAC-OPF	LAC-OPF
1	52	50	53	28	355	246	369
2	16	21	17	29	346	247	246
3	36	39	36	30	448	403	403
4	10	17	11	31	1	15	9
5	201	201	201	32	4	6	6
6	89	89	89	33	3	11	8
7	42	46	43	34	25	41	34
8	32	35	33	35	29	49	39
9	39	42	40	36	0	6	0
10	0	0	0	37	436	460	448
11	160	160	204	38	0	1	0
12	207	283	207	39	4	4	4
13	34	24	30	40	504	369	506
14	7	7	7	41	0	23	0
15	37	30	34	42	0	8	0
16	19	33	25	43	0	0	0
17	23	36	28	44	0	0	0
18	57	69	62	45	233	244	176
19	46	68	56	46	38	40	39
20	19	20	20	47	0	16	12
21	196	152	201	48	7	23	20
22	50	51	51	49	30	39	37
23	37	65	50	50	8	18	16
24	38	68	53	51	35	36	36
25	151	158	155	52	37	42	41
26	149	158	130	53	14	16	14
27	0	2	0	54	0	0	0

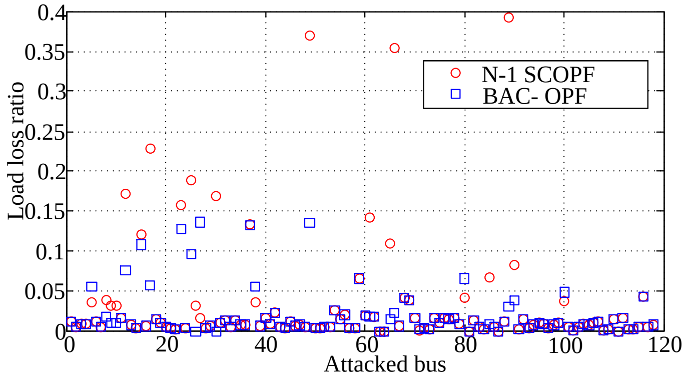


Figure 5. 14 Comparison of the impact of bus-isolating attack in IEEE 118-bus system

Table 5. 18 Loss in line-tripping attack based on N-1 SCOPF

Attacked lines	Load loss ratio	Attacked lines	Load loss ratio
{94, 33}	0.33	{38, 141}	0.24
{93, 33}	0.33	{38, 94}	0.24
{38, 69}	0.29	{38, 93}	0.24
{31, 69}	0.29	{96, 33}	0.24
{38, 116}	0.27	{141, 31}	0.24
{31, 116}	0.27	{94, 31}	0.24

For the bus-isolating attack, the performances of BAC-OPF and N-1 SCOPF are compared in Fig. 5.14. For the N-1 SCOPF, the worst-case scenario for the bus-isolating attack is 39.2% load loss if bus 89 is isolated; while for the BAC-OPF, the worst-case scenario is 13.6% load loss when bus 27 is attacked. The average loss among all the 118 attack scenarios for the N-1 SCOPF is 3.31%, and the average loss for the BAC-OPF is 1.85%. By comparison, it is concluded that the average load loss in the BAC-OPF is less than that in the N-1 SCOPF. The maximum load loss and the average load loss both demonstrate the effectiveness of the proposed in minimizing the consequence of attack.

Table 5. 19 Loss in line-tripping attack based on LAC-OPF in 118-bus system

Attacked lines	Load loss ratio	Attacked lines	Load loss ratio
{38, 98}	0.22	{31, 66}	0.21
{38, 105}	0.22	{96,66}	0.21
{31, 99}	0.22	{33, 67}	0.21
{33, 98}	0.22	{8, 31}	0.19
{33, 105}	0.22	{38, 36}	0.19
{38, 66}	0.21	{51, 33}	0.19

For the line-tripping attack, the performance of the N-1 SCOPF is shown in Table 5.18. The most severe impact is 33% load loss when lines {94, 33} are attacked. For the LAC-OPF, the maximum load loss is 22% as shown in Table 5.19, which is significantly reduced.

It should be noted that the number of combinations of attacked components can increase rapidly if the attacker is capable of attacking a number of components. For example, if the attacker is able to attack five buses in the IEEE 118-bus system, the number of combinations exceeds 1.7×10^5. If the attacker is able to attack five lines, the number of combinations is more than

1.7×10^9. This tremendous amount of combinations leads to high computational burden. Thus, in these cases, efficient methods for quickly identifying the most valuable targets should be deployed.

5.6 Conclusions

In this study, the conventional SCOPF considering *N*-1 contingencies was extended to incorporate probable attack scenarios. The proposed SCOPF model considered the generation operation cost in the normal state, conventional *N*-1 contingencies as well as the risk of malicious attacks. The possible attack scenarios and their probabilities were incorporated into the objective function of the proposed SCOPF model. An improved solution method was investigated based on PSO for conducting the global search as well as on PDIP for finding the local SCOPF solution. And parallel computing for speeding up the calculation was used in this study. The mathematical model and the computational strategy were verified based on three representative test systems. The simulation results demonstrated that the proposed SCOPF model is able to provide increased robustness to the power grid in the face of predictable cyberattacks.

6. An Improved Defender-Attacker-Defender Model for Transmission Lines Defense Considering Offensive Resource Uncertainties

6.1 Introduction

Conventionally, to ensure the power grid's reliable and secure operation the *N*-1 or even *N*-2 criteria are implemented in power grids for maintaining the desired power supply capability in the face of random equipment failures and different forms of disturbances [92]. But they are insufficient to protect the power systems against malicious attacks, which usually target multiple critical components simultaneously. In this regard, some research was devoted to studying the vulnerabilities of the power systems and identifying the critical components for protection. For example, in [43] the random chemistry algorithm was adopted to identify the combination of critical components whose failures can incur a disastrous cascading failure. The critical scenarios were detected by a proposed principal component analysis and the maximum power flow analysis in [93]. In [76] and [94], bilevel attacker-defender models were developed. In these models, it is assumed that the attacker tries to maximize the damage considering the corrective action taken by the defender against the disturbance. These attacker-defender models can be solved by a bilevel max-min optimization technique.

Based on the vulnerability analysis which can identify the critical components or weakness of the network, it is meaningful to develop strategies to wisely allocate the limited defensive resources (including budgets, security-related human resources, etc.) to efficiently safeguard the power grid. In [94] and [95], a trilevel defender-attacker-defender model was studied, and the defenders include the security personnel who harden some well-selected components before the attack occurs and the power system operator who re-dispatches the power after the attack takes place in order to minimize the damage. For this trilevel model, the implicit enumeration algorithm [94] and the C&CG algorithm were adopted [96]. Besides the trilevel modeling, game-theoretical approaches were also widely adopted. For example, in [97], when assuming both the attacker and the defender take actions without knowing the action of the other, a two-player game theoretic approach was developed for selecting the critical components for protection. When the interaction between the attacker and the defender involves multiple rounds, Markov game could be adopted [98].

The trilevel model is being more widely adopted in recent power system defense studies. In the trilevel model [99], the defender at the top-level determines the elements to be protected under the constraint of the budget; the attacker at the middle-level disrupts the selected elements subject to the limitation of the offensive resources. The defender at the bottom-level typically refers to the power system operator, who takes corrective power re-dispatch actions to alleviate the overloading and minimize the impact. The offensive resources can have different meanings for different types of attacks. For example, in physical attacks they may mean the number of attackers and the weapons/tools used. In cyber-attacks, they can refer to the skill sets, capabilities, privileges of the cyber attacker. The offensive resources possessed by the attacker determine the number of the components that attacker can disrupt. This chapter focuses on the development of defensive strategies which can be applied to both physical attacks and cyber-attacks. For simplicity, the number of lines that the attacker can disrupt is used to denote the offensive resources; similarly, the number of lines that the defender can protect denotes the defensive resource; the offensive resource uncertainty is denoted by a probabilistic distribution of the number of lines that the attacker can disrupt. In real practices, professional security agents and experts can help estimate the numbers of elements that the attacker is capable of disrupting based on the information on the potential attacks. For example, the homeland security agency could estimate how many power grid elements that the terrorists can attack given the number of terrorists and the tools they use. The cyber network security experts are able to estimate the capability of the cyber intruders by performing cyber forensics and checking the logs.

However, in real-world scenarios, the decision-making for the allocation of the defensive resource often involves a number of uncertainties, as it is extremely difficult for the defender to obtain accurate and complete information about the attacker. For example, the security agency often could not accurately know the offensive resources that the attacker has when making the decision on the defensive strategy; in other words, the defender is confronted with the problem of developing defense strategies without a clear understanding of the number of components which might be affected by the attack. In this study, the defensive strategy specifically refers to identifying the critical lines for defense; also, the attack strategy means determining the lines that should be attacked.

This study aims to solve this defensive strategy development problem considering the offensive resource uncertainties. Specifically, an MAS defender-attacker-defender model is proposed, where the uncertainties in the offensive resource are modeled as a set of attack scenarios with corresponding probabilities, and the max-min defender-attacker interaction in each attack scenario is considered. The proposed MAS defender-attacker-defender model is solved by a method combining both robust optimization and stochastic programming.

6.2 Problem Formulation

6.2.1 Conventional DAD Model

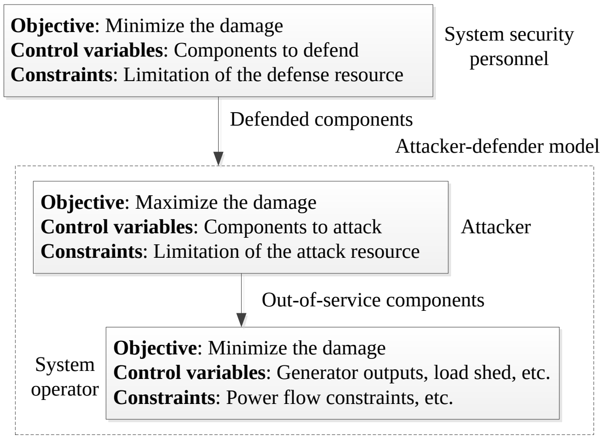

Objective: Minimize the damage
Control variables: Components to defend
Constraints: Limitation of the defense resource
System security personnel
Defended components
Attacker-defender model
Objective: Maximize the damage
Control variables: Components to attack
Constraints: Limitation of the attack resource
Attacker
Out-of-service components
System operator
Objective: Minimize the damage
Control variables: Generator outputs, load shed, etc.
Constraints: Power flow constraints, etc.

Figure 6. 1 Conventional defender-attacker-defender model

As shown in [94] and [95], a trilevel defender-attacker-defender model was found to be suitable for developing defensive strategies against malicious attacks. This trilevel model is shown in Fig. 6.1, which involves three agents acting in sequence: (a) at the top-level, the power system security personnel identify the critical components, aiming to minimize the consequence caused by the attacker; (b) at the middle-level, the attacker seeks to maximize the consequence by attacking the judiciously-selected targets; (c) at the bottom-level, the power system operator takes remedial actions to minimize the consequence after the attacker disrupts the targeted components. The middle-level and the bottom-level form a typical attacker-defender model, which describes the attacker’s decision-making to identify the components to attack. This attacker-defender model is a bilevel optimization problem, in which the offensive resource is often involved and has a great impact on the consequence of the attack. In this study, similar to [100] the offensive resource is quantitatively represented by the maximum number of components that the attacker is able to successfully trip. Once the offensive resource is known, the bilevel attacker-defender optimization problem can be solved. This is the basis for solving the trilevel problem depicted in Fig. 6.1, as this trilevel model assumes that the security personnel at the top-level have the complete and accurate information about the offensive resource.

The mathematical representation of the defender-attacker-defender model is briefly introduced as follows.

$$\min_{w \in \boldsymbol{W}} \max_{v \in \boldsymbol{V}} \min_{\substack{\{\delta,\, P^g, \\ P^f, \Delta P^d\}}} \sum\nolimits_{n \in \boldsymbol{N}} \Delta P_n^d \tag{6.1}$$

$$\text{s.t. } \sum\nolimits_{l \in \boldsymbol{L}} w_l \leq r^d \qquad \forall w_l \in \{0,1\} \tag{6.2}$$

$$\sum\nolimits_{l \in \boldsymbol{L}} (1 - v_l) \leq r^a \quad \forall v_l \in \{0,1\} \tag{6.3}$$

$$P_l^f = (w_l + v_l - w_l v_l) \frac{\delta_{o(l)} - \delta_{d(l)}}{x_l} \quad \forall l \in \boldsymbol{L} \tag{6.4}$$

$$\sum\nolimits_{j \in \boldsymbol{J}_n} P_j^g - \sum\nolimits_{l | o(l) = n} P_l^f + \sum\nolimits_{l | d(l) = n} P_l^f \quad + \Delta P_n^d = P_n^d \quad \forall n \in \boldsymbol{N} \tag{6.5}$$

$$0 \leq P_j^g \leq \overline{P}_j^g \qquad \forall j \in \boldsymbol{J} \tag{6.6}$$

$$-\overline{P}_l^f \leq P_l^f \leq \overline{P}_l^f \qquad \forall l \in \boldsymbol{L} \tag{6.7}$$

$$0 \leq \Delta P_n^d \leq P_n^d \qquad \forall n \in \boldsymbol{N} \tag{6.8}$$

The variables and constants are explained as follows: r^d and r^a are the defensive resource and the offensive resource, respectively, i.e., the number of components the defender can protect and the number of components the attacker can disrupt; w and v indicate the defensive resource allocation vector and offensive resource allocation vector, respectively; $\boldsymbol{W}$ and $\boldsymbol{V}$ are the feasible sets for w and v, respectively; δ, P^g, P^f, ΔP^d mean the bus voltage angle vector, generator power output vector, transmission line power flow vector, and load demand curtailment vector, respectively; $\boldsymbol{N}$, $\boldsymbol{J}$ and $\boldsymbol{L}$ are the set of buses, the set of generators, and the set of transmission lines, respectively; Subscripts *n*, *j*, *l* denote indices of the buses, generators and transmission lines, respectively; x_l, $\overline{P}_j^g$, $\overline{P}_l^f$ and P_n^d are the reactance of line *l*, maximum generation of generator *j*, power flow limit of transmission line l, and load demand at bus n, respectively; $o(l)$ and $d(l)$ are the origin bus and the destination bus of line l, respectively.

As shown in the objective function (6.1), the security personnel allocate the limited defensive resource to defense certain lines, aiming to minimize the load curtailment considering the optimal attack strategy made by the intelligent attackers, in which the power re-dispatch carried out by the operator is incorporated. Constraint (6.2) captures the limitation of the offensive resource. w_l is a binary decision variable, if its value is 1, it means line l is protected. Similarly, constraint (6.3) shows the limitation of the defensive resource. v_l is a binary decision variable; when its value is 0, it means line l is attacked. Constraints (6.4)-(6.8) are related to the optimal power flow analysis. Constraint (6.4) calculates the power flow on the transmission lines, and the status of line l is obtained by $w_l + v_l - w_l v_l$. A line will be out of service only when it is attacked and it is not being protected. Constraint (6.5) ensures the power inflow and outflow balance at each bus. Constraint (6.6) ensures that the generation output of each generation does not exceed its maximum capacity. It is indicated in (6.7) that the line power flow is restricted within the allowed range $[-\overline{P}_l^f, \overline{P}_l^f]$. The non-negativity constraint (6.8) guarantees that the load loss is less than the nominal demand.

Note that in the conventional model the offensive resource r^a in (6.3) is a given value, which indicates that the defender knows the capability of the attacker before the attack is launched. This can be a strong assumption in real applications.

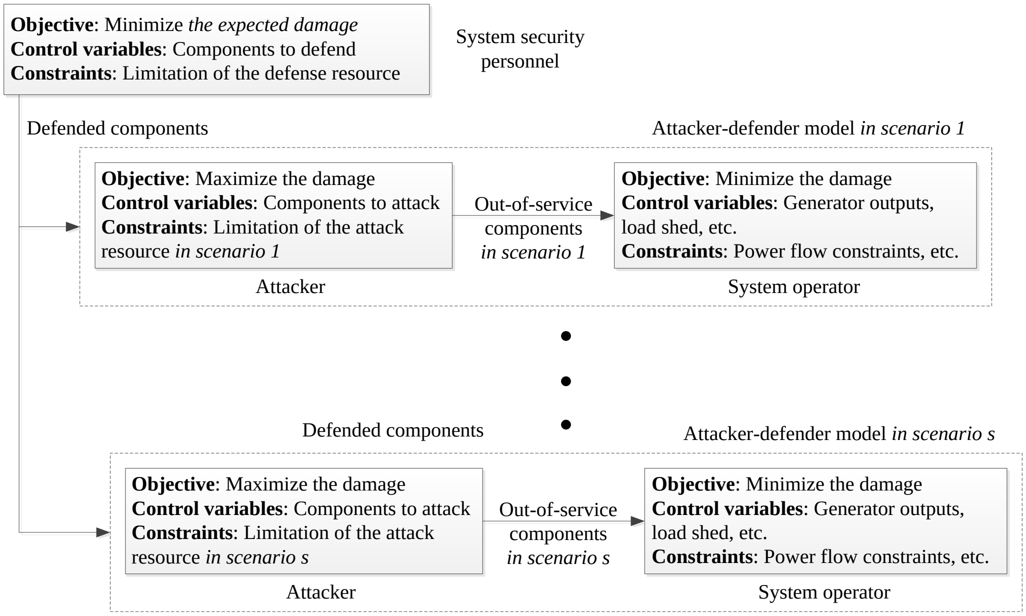

Objective: Minimize *the expected damage*
Control variables: Components to defend
Constraints: Limitation of the defense resource
System security personnel
Defended components
Attacker-defender model *in scenario 1*
Objective: Maximize the damage
Control variables: Components to attack
Constraints: Limitation of the attack resource *in scenario 1*
Attacker
Out-of-service components *in scenario 1*
Objective: Minimize the damage
Control variables: Generator outputs, load shed, etc.
Constraints: Power flow constraints, etc.
System operator
Defended components
Attacker-defender model *in scenario s*
Objective: Maximize the damage
Control variables: Components to attack
Constraints: Limitation of the attack resource *in scenario s*
Attacker
Out-of-service components *in scenario s*
Objective: Minimize the damage
Control variables: Generator outputs, load shed, etc.
Constraints: Power flow constraints, etc.
System operator

Figure 6. 2 Proposed Multiple-Attack-Scenario defender-attacker-defender model

6.2.2 Modeling of Uncertainties

In a more realistic sense, the security personnel are often not able to obtain the exact information about the offensive resource. In other words, the security personnel has to develop the defensive strategy with uncertain information about the offensive resource, although the offensive resource is well known to the attacker. In this study, the uncertainty of the offensive resource is modeled by a probability distribution over a set of offensive resources. For each offensive resource, an attacker-defender model should be built, which corresponds to the middle and bottom levels in Fig. 6.1. Thus, each offensive resource is studied with an associated attack scenario, and an attack scenario is characterized by its offensive resource. A specific example of the offensive resource set and the probability distribution is given here. For example, if the security personnel estimate the attacker may have the capability to disconnect two lines, three lines, four lines or five lines with probabilities 0.2, 0.3, 0.4 and 0.1, respectively, the attack scenario set is {two lines, three lines, four lines, five lines}, and the probability distribution is {0.2, 0.3, 0.4, 0.1}. The security personnel’s objective is to allocate the defensive resource optimally to defend the power grid considering all these four attack scenarios and the corresponding probabilities, neither the attack scenario {two lines} with probability 1, nor the attack scenario {four lines} with probability 1.

The possible attack scenarios and the related probabilities can vary with time, the activity pattern of the adversaries, and weather, etc. It is beyond the scope of this study to accurately estimate the uncertainty when an attack is imminent. It is believed in the future that the power system defenders and operators will be warned of the possible attacks ahead of time with the aid of intrusion detection systems, experienced security administrators, and even intelligence services like the National Terrorism Advisory System.

The focus of this chapter is on the decision-making support to determine which lines should be defended, which can be applied to both cyber-attacks and physical attacks. The detailed methods to defend the lines can be different in different types of attacks, such as enhanced communication traffic scanning for defending against cyber-attacks, and intensified patrolling or installing surveillance video equipment for deterring physical attacks, among many others.

6.2.3 Proposed DAD Model Considering Uncertainties

The MAS defender-attacker-defender model is proposed in Fig. 6.2. At the top-level, the security personnel make decisions to identify the components to defend in order to minimize the expected damage considering all the possible attack scenarios and their corresponding probabilities. In each scenario with a certain amount of offensive resources given, the attacker determines the components to attack whereas the corrective power re-dispatch performed by the power grid operator is considered. In this proposed MAS defender-attacker-defender model, from top to bottom three kinds of agents are involved: the security personnel, the attacker, and the operator. The top-level agent is interacting with multiple middle-level agents. This is different from the conventional defender-attacker-defender model, in which the top-level agent interacts with only one middle-level agent. It should be noted that this MAS defender-attacker-defender model can easily shrink to the conventional defender-attacker-defender model, which only considers one single attack scenario.

For the sake of clarity and brevity, the transmission lines are assumed to be the only assets that can be defended by the security personnel and disrupted by the attacker. Also, the damage is characterized by the load curtailment caused by the attacker.

The mathematical problem for the proposed MAS defender-attacker-defender model is represented by an equivalent optimization problem as follows.

$$\min_{w\in\boldsymbol{W}} E_{\Omega(\boldsymbol{S})}[\max_{v(s)\in\boldsymbol{V}(s)} \min_{\substack{\{\delta(s),P^g(s),\\ P^f(s),\Delta P^d(s)\}}} \sum\nolimits_{n\in\boldsymbol{N}} \Delta P_n^d\,(s)] \tag{6.9}$$

$$\text{s.t.} \sum\nolimits_{l\in\boldsymbol{L}} w_l \le r^d \qquad \forall w_l \in \{0,1\} \tag{6.10}$$

$$\sum\nolimits_{l\in\boldsymbol{L}} (1 - v_l(s)) \le r^a(s) \;\; \forall v_l \in \{0,1\} \;\; \forall s \in \boldsymbol{S} \tag{6.11}$$

$$P_l^f(s) = \big(w_l + v_l(s) - w_l v_l(s)\big)\frac{\delta_{o(l)}(s) - \delta_{d(l)}(s)}{x_l} \quad \forall l \in \boldsymbol{L} \;\; \forall s \in \boldsymbol{S} \tag{6.12}$$

$$\sum\nolimits_{j\in\boldsymbol{J}_n} P_j^g(s) - \sum\nolimits_{l|o(l)=n} P_l^f(s) + \sum\nolimits_{l|d(l)=n} P_l^f(s) + \Delta P_n^d(s) = P_n^d \quad \forall n \in \boldsymbol{N} \;\; \forall s \in \boldsymbol{S} \tag{6.13}$$

$$0 \le P_j^g(s) \le \overline{P}_j^g \qquad \forall j \in \boldsymbol{J} \;\; \forall s \in \boldsymbol{S} \tag{6.14}$$

$$-\overline{P}_l^f \le P_l^f(s) \le \overline{P}_l^f \qquad \forall l \in \boldsymbol{L} \;\; \forall s \in \boldsymbol{S} \tag{6.15}$$

$$0 \le \Delta P_n^d(s) \le P_n^d \qquad \forall n \in \boldsymbol{N} \;\; \forall s \in \boldsymbol{S} \tag{6.16}$$

where s is an attack scenario, and $\boldsymbol{S}$ is the set of attack scenarios, Ω is the probability distribution of $\boldsymbol{S}$. $E_{\Omega(s)}$ is the expected value of load curtailment considering the probability distribution Ω of the attack scenario set $\boldsymbol{S}$.

There are great differences between the proposed MAS defender-attack-defender model and the conventional defender-attack-defender model, and the proposed model is more practical and complicated as explained in the following. (a) The objective function of the proposed MAS defender-attack-defender model in (9) is to minimize the expected loss considering all the possible attack scenarios, while the conventional defender-attack-defender model only considers a single known attack scenario. (b) In the proposed model, for each possible attack scenario the decision-making of the attacker and the related optimal power flow analysis based remedial re-dispatch should be incorporated in the defender's defensive strategy development, as shown in constraints (6.11)-(6.16). Compared with the conventional model, the proposed model offers a more flexible approach for the defender to allocate the limited resource to safeguard the power grid considering multiple possible attack scenarios.

In the proposed MAS defender-attacker-defender model, there are three agents at different levels, i.e., the security personnel at the top level, the attacker at the middle level, and the operator at the bottom level. The action sequence of them is explained as follows. The security personnel first takes actions to protect a few deliberately selected critical lines. The decision of selecting critical lines is made considering the offensive resource uncertainties as well as the subsequent optimal decision-making of the attacker and the operator. After the security personnel makes efforts to protect the selected lines, the attacker takes actions to attack certain deliberately-chosen lines. The decision-making of the attacker takes into account the following response of the operator. After the attack is launched and the attacked lines are tripped, the power system operator takes corrective actions to minimize the load curtailment. It should be noted that in the decision-making process of the security personnel, there are uncertainties about the number of lines that the attacker can disrupt. But in the decision-making process of the attacker, the attacker has a clear understating of the number of lines she/he can disrupt.

In the decision-making process of the middle-level attacker, the attacker needs to take the response of the bottom-level operator into consideration. This means that the attacker needs to consider the variable physical and functional features of the power system, as shown in (6.12)-(6.16). For example, the voltage angles of the buses and the impedances of the lines are considered for calculating the transmission line power flows in (6.12). The power balance at each bus is modeled in (6.13). The capacity of each generator/line is considered in (6.14)-(6.15). The maximum load loss at each bus is accounted for in (6.16). In sum, the middle-level offensive resource allocation is modeled at the system level considering the characteristics and functions of the major elements, aiming to maximize the load loss. And the load loss in the objective function (6.9) indicates the technical and economic impacts.

6.3 Solution Method

This chapter presents the solution method for the MAS defender-attacker-defender problem formulated in (6.9)-(6.16) in Chapter 6.2.

The solution method is based on the C&CG algorithm. The trilevel MAS defender-attacker-defender problem is transformed to an upper-level problem (ULP) and a lower-level problem (LLP) in order to implement the C&CG algorithm. In the ULP, the security personnel determine the defensive resource allocation considering a set of offensive strategy combinations while each offensive strategy combination consists of attack strategies for all possible attack scenarios. The ULP generates the lower bound for the MAS defender-attacker-defender problem. In the LLP, for each attack scenario, the attack strategy is modeled by a bilevel optimization problem and the optimal offensive plan for each attack scenario is obtained. These obtained offensive strategies for all attack scenarios form an offensive strategy combination, which will be added to the set of offensive strategy combinations if the convergence is not met. The expected value of load loss for all the attack scenarios forms the upper bound for the MAS defender-attacker-defender problem. The ULP and the LLP will be calculated iteratively until the lower bound and upper bound merge, which means that the convergence is achieved and the obtained value is an optimal solution.

The ULP and the LLP are explained in detail as follows.

6.3.1 Upper-Level Problem

In the ULP, the security personnel determine the optimal allocation of the defensive resource to minimize the expected damage caused by a given set of offensive strategy combinations $\widehat{\boldsymbol{V}}$.

$$\widehat{\boldsymbol{V}} = [\widehat{\boldsymbol{V}}^1, \cdots \widehat{\boldsymbol{V}}^i, \cdots \widehat{\boldsymbol{V}}^k] \tag{6.17}$$

where k is the number of offensive strategy combinations, and the sign $\widehat{\ }$ means the value of a variable is given or known. Denote the dimension of $\boldsymbol{S}$ as n_S, thus n_S is the number of attack scenarios. For the example given in Chapter 6.2 n_S is 4. Each offensive strategy combination consists of n_S offensive strategies, and each offensive strategy corresponds to certain known offensive resource. Thus,

$$\widehat{\boldsymbol{V}}^i = \{\hat{v}^i(\boldsymbol{S}_1), \cdots, \hat{v}^i(\boldsymbol{S}_{n_S})\} \qquad \forall i = 1, \cdots, k \tag{6.18}$$

The ULP is constructed as follows:

$$\min \xi \tag{6.19}$$

$$\xi \geq \sum_{s\in S}\{\Omega(s)[\sum_{n\in \boldsymbol{N}} \Delta P_n^{d,i}(s)]\} \qquad \forall i = 1, \cdots, k \tag{6.20}$$

$$\sum_{l\in \boldsymbol{L}} w_l \leq r^d \qquad \forall w_l \in \{0,1\} \tag{6.21}$$

$$P_l^{f,i}(s) = \left[w_l + \widehat{v}_l^{\,i}(s) - w_l \widehat{v}_l^{\,i}(s)\right] \frac{\delta_{o(l)}^i(s) - \delta_{d(l)}^i(s)}{x_l} \;\; \forall l \in \boldsymbol{L}, \;\; \forall s \in \boldsymbol{S}, \; \forall i = 1, \cdots, k \tag{6.22}$$

$$\sum_{j\in \boldsymbol{J}_n} P_j^{g,i}(s) - \sum_{l|o(l)=n} P_l^{f,i}(s) + \sum_{l|d(l)=n} P_l^{f,i}(s) + \Delta P_n^{d,i}(s) = P_n^d \qquad \forall n \in \boldsymbol{N},\ \forall s \in \boldsymbol{S},\ \forall i = 1,\cdots,k \qquad (6.23)$$

$$0 \le P_j^{g,i}(s) \le \overline{P}_j^g \ \ \forall j \in \boldsymbol{J},\ \ \forall s \in \boldsymbol{S},\ \forall i = 1,\cdots,k \qquad (6.24)$$

$$-\overline{P}_l^f \le P_l^{f,i}(s) \le \overline{P}_l^f \quad \forall l \in \boldsymbol{L},\ \forall s \in \boldsymbol{S},\ \ \forall i = 1,\cdots,k \qquad (6.25)$$

$$0 \le \Delta P_n^{d,i}(s) \le P_n^d \ \ \forall n \in \boldsymbol{N}, \forall s \in \boldsymbol{S},\ \ \forall i = 1,\cdots,k \qquad (6.26)$$

In the objective function (6.19), the security personnel try to minimize ξ, which is the maximization of the expected damages in *k* offensive strategy combinations. The remedial power re-dispatch at the bottom-level is considered for each attack scenario and each offensive strategy combination, thus $\delta_{o(l)}^i(s)$, $\delta_{d(l)}^i(s)$, $P_j^{g,i}(s)$, $P_l^{f,i}(s)$ and $\Delta P_n^{d,i}(s)$ are calculated for each attack scenario *s* and each offensive strategy combination *i*.

As there are nonlinear terms in the constraint (6.22), the big-M method is adopted to linearize it, as shown below [101], [102]-[103].

$$x_l P_l^{f,i}(s) - \left[\delta_{o(l)}^i(s) - \delta_{d(l)}^i(s)\right] \le M\left[1 - w_l - \widehat{v}_l^{\,i}(s) + w_l \widehat{v}_l^{\,i}(s)\right] \quad \forall l \in \boldsymbol{L},\ \ \forall s \in \boldsymbol{S},\ \forall i = 1,\cdots,k \qquad (6.27)$$

$$x_l P_l^{f,i}(s) - [\delta_{o(l)}^i(s) - \delta_{d(l)}^i(s)] \ge -M\left[1 - w_l - \widehat{v}_l^{\,i}(s) + w_l \widehat{v}_l^{\,i}(s)\right] \quad \forall l \in \boldsymbol{L},\ \ \forall s \in \boldsymbol{S},\ \forall i = 1,\cdots,k \qquad (6.28)$$

$$-\overline{P}_l^f\left[w_l + \widehat{v}_l^{\,i}(s) - w_l \widehat{v}_l^{\,i}(s)\right] \le P_l^{f,i}(s) \le \overline{P}_l^f\left[w_l + \widehat{v}_l^{\,i}(s) - w_l \widehat{v}_l^{\,i}(s)\right] \quad \forall l \in \boldsymbol{L},\ \ \forall s \in \boldsymbol{S},\ \forall i = 1,\cdots,k \qquad (6.29)$$

where *M* is a sufficiently large number.

As can be seen in (6.20)-(6.26), each possible offensive resource scenario *s* and its probability Ω(s) is considered to minimize the expected load loss using stochastic programming.

6.3.2 **Lower-Level Problem**

The LLP calculates the expected damage ζ caused by the attacker in all the attack scenarios, which are represented as follows.

$$\zeta = \sum_{s\in \boldsymbol{S}}[\Omega(s)\eta\ (s)] \tag{6.30}$$

where $\eta\ (s)$ is the damage in scenario *s*.

Note that in each attack scenario with a given offensive resource, the attacker tries to maximize the damage considering the power system operator's response to minimize the damage. In each scenario, the interaction is modeled as a max-min bilevel problem which is illustrated as follows.

$$\eta\ (s) = \max_{v\in \boldsymbol{V}(s)} \min_{\substack{\{\delta(s),\, P^g(s),\\ P^f(s), \Delta P^d(s)\}}} \sum_{n\in \boldsymbol{N}} \Delta P_n^d\ (s) \tag{6.31}$$

$$\sum_{l\in \boldsymbol{L}}(1 - v_l(s)) \leq r^a(s) \quad \forall s \in \boldsymbol{S} \quad \forall v_l \in \{0,1\} \tag{6.32}$$

$$P_l^f(s) = \left(\widehat{w}_l + v_l(s) - \widehat{w}_l v_l(s)\right)\frac{\delta_{o(l)}(s) - \delta_{d(l)}(s)}{x_l} \forall l \in \boldsymbol{L}, \forall s \in \boldsymbol{S} \qquad (\mu_l(s)) \tag{6.33}$$

$$\sum_{j\in \boldsymbol{J}_n} P_j^g(s) - \sum_{l|o(l)=n} P_l^f(s) + \sum_{l|d(l)=n} P_l^f(s) + \Delta P_n^d(s) = P_n^d \quad \forall n \in \boldsymbol{N}, \forall s \in \boldsymbol{S} \ \ \left(\lambda_n(s)\right) \tag{6.34}$$

$$0 \leq P_j^g(s) \leq \overline{P}_j^g \quad \forall j \in \boldsymbol{J}, \forall s \in \boldsymbol{S}\ (\overline{\gamma}_j(s)) \tag{6.35}$$

$$-\overline{P}_l^f \leq P_l^f(s) \leq \overline{P}_l^f \quad \forall l \in \boldsymbol{L}, \forall s \in \boldsymbol{S}\ (\underline{\emptyset}_l(s), \overline{\emptyset}_l(s)) \tag{6.36}$$

$$0 \leq \Delta P_n^d(s) \leq P_n^d \quad \forall n \in \boldsymbol{N}, \forall s \in \boldsymbol{S}\ (\overline{\alpha}_n(s)) \tag{6.37}$$

In this bilevel optimization, the lower-level (33)-(37) represents the power re-dispatch after certain lines are tripped due to the attack. As strong duality exits for the lower-level, the bilevel optimization is transformed into a single level maximization problem using the duality principle. The dual variables for each of the constraints (33)-(37) are given following the constraints, including $\mu_l(s)$, $\lambda_n(s)$, $\overline{\gamma}_j(s)$, $\underline{\emptyset}_l(s)$, $\overline{\emptyset}_l(s)$ and $\overline{\alpha}_n(s)$. The obtained single level problem is shown as follows. For brevity, the sign (s) denoting the attack scenario is omitted.

$$\eta = \max_{\{v_l, z_l, \bar{z_l}, k_l, \mu_l, \lambda_n, \overline{\gamma}_j, \underline{\emptyset}_l, \overline{\emptyset}_l, \overline{\alpha}_n\}} \{\textstyle\sum_{j\in \boldsymbol{J}} \overline{\gamma}_j \overline{P}_j^g + \sum_{l\in \boldsymbol{L}} (\overline{\emptyset}_l - \underline{\emptyset}_l) \overline{P}_l^f + \sum_{n\in \boldsymbol{N}} (\lambda_n + \overline{\alpha}_n) P_n^d\} \tag{6.38}$$

$$\textstyle\sum_{l\in \boldsymbol{L}} (1 - v_l) \le s \tag{6.39}$$

$$\textstyle\sum_{l|o(l)=n} \frac{\mu_l(\hat{w}_l + v_l - \hat{w}_l v_l)}{x_l} = \sum_{l|d(l)=n} \frac{\mu_l(\hat{w}_l + v_l - \hat{w}_l v_l)}{x_l} \quad \forall n \in \boldsymbol{N} \tag{6.40}$$

$$\lambda_n + \overline{\alpha}_n \le 1 \qquad \forall n \in \boldsymbol{N} \tag{6.41}$$

$$\lambda_{n|j\in \boldsymbol{J}_n} + \overline{\gamma}_j \le 0 \qquad \forall j \in \boldsymbol{J} \tag{6.42}$$

$$\mu_l - \lambda_{n|n=o(l)} + \lambda_{n|n=d(l)} + \underline{\emptyset}_l + \overline{\emptyset}_l = 0 \quad \forall l \in \boldsymbol{L} \tag{6.43}$$

$$\overline{\gamma}_j \le 0 \qquad \forall j \in \boldsymbol{J} \tag{6.44}$$

$$\underline{\emptyset}_l \ge 0 \qquad \forall l \in \boldsymbol{L} \tag{6.45}$$

$$\overline{\emptyset}_l \le 0 \qquad \forall l \in \boldsymbol{L} \tag{6.46}$$

$$\overline{\alpha}_n \le 0 \qquad \forall n \in \boldsymbol{N} \tag{6.47}$$

As there is a nonlinear term $\mu_l v_l$ in constraint (6.40), the big-M method is adopted to linearize this constraint:

$$\textstyle\sum_{l|o(l)=n} \frac{\mu_l \hat{w}_l + (1-\hat{w}_l) m_l}{x_l} = \sum_{l|d(l)=n} \frac{\mu_l \hat{w}_l + (1-\hat{w}_l) m_l}{x_l} \quad \forall n \in \boldsymbol{N} \tag{6.48}$$

$$m_l = \mu_l z_l \qquad \forall n \in \boldsymbol{N} \tag{6.49}$$

$$m_l \ge -M z_l \qquad \forall n \in \boldsymbol{N} \tag{6.50}$$

$$m_l \le M z_l \qquad \forall n \in \boldsymbol{N} \tag{6.51}$$

$$m_l \ge \mu_l + M z_l - M \quad \forall n \in \boldsymbol{N} \tag{6.52}$$

$$m_l \le \mu_l - M z_l + M \quad \forall n \in \boldsymbol{N} \tag{6.53}$$

6.3.3 **Overall C&CG Algorithm**

The proposed MAS defender-attacker-defender problem is decomposed into an ULP and an LLP as described previously. The C&CG algorithm is adopted to solve the overall MAS defender-attacker-defender problem based on the ULP and the LLP. The basic idea to implement the C&CG algorithm is shown in Fig. 6.3.

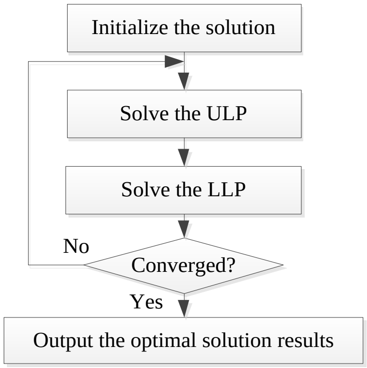


Figure 6. 3 Overview of the C&CG algorithm

The implementation of the C&CG algorithm is explained in detail as follows [94]-[96].

Step [1]. Initialize the upper bound and lower bound as $UB = \infty$ and $LB = -\infty$, respectively. Initialize the set of offensive strategy combinations $\hat{\boldsymbol{V}}$ with a random feasible offensive strategy combination. Set the iteration index *k*=1.

Step [2]. Solve the ULP with (6.17)-(6.29) to get ξ and $\hat{w}_l$. As the ULP is a MILP problem, it can be resolved with solvers like CPLEX. Update *UB* with the obtained ξ.

Step [3]. Solve the LLP, which involves two sub-steps. In the first sub-step, the optimization problem consisting of (6.30)-(6.53) is solved with the $\hat{w}_l$ obtained in step [2], η (s) and $\hat{v}^k(s)$ are obtained. This calculation should be performed for n_S times until all the attack scenarios are analyzed. In the second sub-step, ζ is calculated with (6.30), also $\hat{\boldsymbol{V}}^k$ is obtained using (6.18) by combining all $\hat{v}^k(s)$ $s \in \boldsymbol{S}$. Update *LB* with ζ. Importantly, add $\hat{\boldsymbol{V}}^k$to $\hat{\boldsymbol{V}}$.

Step [4]. If UB and LB are equal, the convergence is reached, go to next step; otherwise, k=k+1, go to step [2].

Step [5]. Output the optimal values, including ξ which is the optimal expected damage, $\widehat{w}_l$ which is the optimal defensive resource allocation, and $\hat{v}^k(s)$ which is the optimal offensive strategy in attack scenario s.

The C&CG method can converge within a finite number of iterations. As can be seen from the above descriptions on the solution method, the overall solution method is the C&CG method that solves the ULP and LLP iteratively until convergence is achieved; while in the ULP the stochastic programming is applied and in the LLP the primal-dual method is used.

6.4 Case Studies

The case studies are carried out on the two test systems, the IEEE RTS79 system [48] and the IEEE 57-bus system. The case studies are performed based on the Matlab simulation environment and IBM CPLEX [78].

6.4.1 IEEE RTS79 system

The IEEE RTS79 system has 24 buses, 12 generation units, and 38 lines. Each line is denoted by the combination of its origin and destination buses. If there are parallel transmission lines with the same origin and destination buses, they are regarded as individual lines.

A) Benefits of the Proposed Model

Case study 1: The power grid is vulnerable to cyber intrusions launched by determined and skilled cyber attackers. Attackers may exploit the vulnerabilities in the SCADA network and/or the substations, and send false commands to trip the lines after gaining the privileges needed. It is not a trival task to hack the power system, and the cyber attacker usually has long-time reconnaissance to seek the access points and discover the vulnerabilities, as shown in the 2015 Ukraine power grid cyber- attack. As the cyber network activities are monitored by firewalls and intrusion detection systems (IDSs), the attacker's abnormal activies can be possibly detected by the IDSs, which generate alarms to notify the power system administrator. The administrator needs to make efforts to prevent the intrusion, such as intensified scanning. Although the alarms can warn the attacker of the intrusions, it is very hard to accurately know the capabilities of the attacker. Attackers of different skill levels could disrupt different numbers of lines; for example, an expert attacker usually has the skill to trip more lines than a novice attacker.

Table 6. 1 Simulation results for case 1

Variables	Result
Expected load loss (MW)	386.4
Defended lines	14-16, 16-19
Attacked lines in attack scenario 1 (Offensive resource is 3)	15-21, 15-21, 16-17
Attacked lines in attack scenario 2 (Offensive resource is 5)	3-24, 9-11,10-11, 12-13, 12-23
Load loss in attack scenario 1 (MW)	212
Load loss in attack scenario 2 (MW)	648

As an example, if based on the cyber forensics information, the cybersecurity experts estimate that the attacker has a probability of 0.6 to be a novice capable of attacking 3 lines, and a probability of 0.4 to be an expert attacker capable of attacking 5 lines. Then, the possible attack scenario set is $\boldsymbol{S} = \{3, 5\}$ with the corresponding probabilities $\Omega = \{0.6, 0.4\}$. Also, it is assumed that the security operator can protect only two transmission lines.

Using the proposed mathematical model and solution method, the results are shown in Table 6.1. The two lines to be defended are 14-16, 16-19, and this decision is made by considering the possible consequences of the two attack scenarios, and the expected load loss is minimized. The computation is conducted using an ordinary laptop with 8 GB memory and four 2.9 GHz cores, and it takes 380 seconds to complete the computation.

To demonstrate the benefit of the proposed MAS DAD model over the conventional DAD model, comparative studies are provided. In the conventional model, if the security personnel only consider scenario 1, the defended lines are {15-21, 20-23}. It is noted here that robust optimization usually considers the worst-case scenario, thus if it is applied to this problem, only the worst-case scenario would be considered which is scenario 2. Similarly, the defended lines are {9-12, 12-23} if only scenario 2 is considered. For each defense strategy, the load losses in scenario 1 and scenario 2, as well as the expected load loss which considers the attack scenario set {3, 5} and related probabilities {0.6, 0.4} are given in Table 6.2.

Table 6. 2 Comparative studies for case 1

Defended lines	Load loss (MW)		
	Attack scenario 1	Attack scenario 2	Expected
14-16, 16-19	212	648	386.4
15-21, 20-23	194	842	453.2
9-12, 12-23	309	617	432.2

It can be seen that for the proposed MAS defender-attacker-defender model, although the load loss in certain single attack scenario may not be the least, the expected load loss for multiple attack scenarios is the least. Thus, although the conventional defender-attacker-defender model can be used to develop the optimal strategy for defending against a presumed single attack, the performance of its obtained defensive strategy is compromised when an attack scenario different from the presumed one occurs. Rather, the proposed MAS defender-attacker-defender model is suitable for developing an optimal defensive strategy when there are uncertainties related to the attacker, i.e., when multiple presumed attack scenarios need to be considered. By comparison, the expected load loss with the proposed model and solution method is 386.4 MW, which is smaller than the value of 432.2 MW obtained by the robust optimization. Thus the benefit of the approach is demonstrated.

Case study 2: Besides cyber intrusions, the transmission lines are also vulnerable to physical attacks. Assume a possible future scenario, the power system administrators receive warning from the homeland security agency that a group of terrorists are preparing to launch an attack and disrupt the transmission lines. The homeland security agency does not have the accurate information about the number of terrorists, thus the number of lines they can trip. But the homeland security agency estimates that the number of terrorists is between two to five, and the probabilities are assessed as {0.2, 0.3, 0.4, 0.1}. Based on the information from the security agency, the proposed method can be adopted to decide the transmission lines to be hardened. If the power company has a limited budget and security personnel can patrol only three lines, the defended lines are 14-16, 15-21 and 16-19. The detailed results are shown in Table 6.3, and the attacked lines for each specific attack scenario is given in Fig. 6.4.

This case study involves more attack resource possibilities, and the calculation time is 1,097 seconds. It can be seen that the calculation time increases with the increase of the possibilities of offensive resources.

As a comparison, the defense strategy can be developed based on the most serious scenario (i.e., attacking five lines) or the most likely scenarios (i.e., attacking four lines), or others. To demonstrate the benefit of the proposed method, the defended lines and the consequence for these alternative strategies are studied and compared. The optimal defensive strategy is to protect lines {4-9, 6-10, 14-16}, {11-14, 16-17, 16-19}, {11-13, 14-16, 15-21} and {10-12, 12-23, 14-16} for defending against single attack scenarios 1 (offensive resource is 2), scenarios 2 (offensive resource is 3), scenarios 3 (offensive resource is 4), scenarios 4 (offensive resource is 5), respectively. Similar to Case 1, comparative study results are provided to show the performance of different defensive strategies under different attack scenarios, as shown in Table 6.4.

Table 6. 3 Simulation results for case 2

Variables	Result
Expected load loss (MW)	282.8
Defended lines	14-16, 15-21, 16-19

Table 6. 4 Comparative studies for case 2

Defended lines	Load loss (MW)				
	Attack scenario 1	Attack scenario 2	Attack scenario 3	Attack scenario 4	Expected
14-16, 15-21, 16-19	136	180	342	648	282.8
4-9, 6-10, 14-16	71	309	387	648	326.5
11-14, 16-17, 16-19	136	180	516	842	371.8
11-13, 14-16, 15-21	136	309	322	648	314.5
10-12, 12-23, 14-16	136	309	387	448	319.5

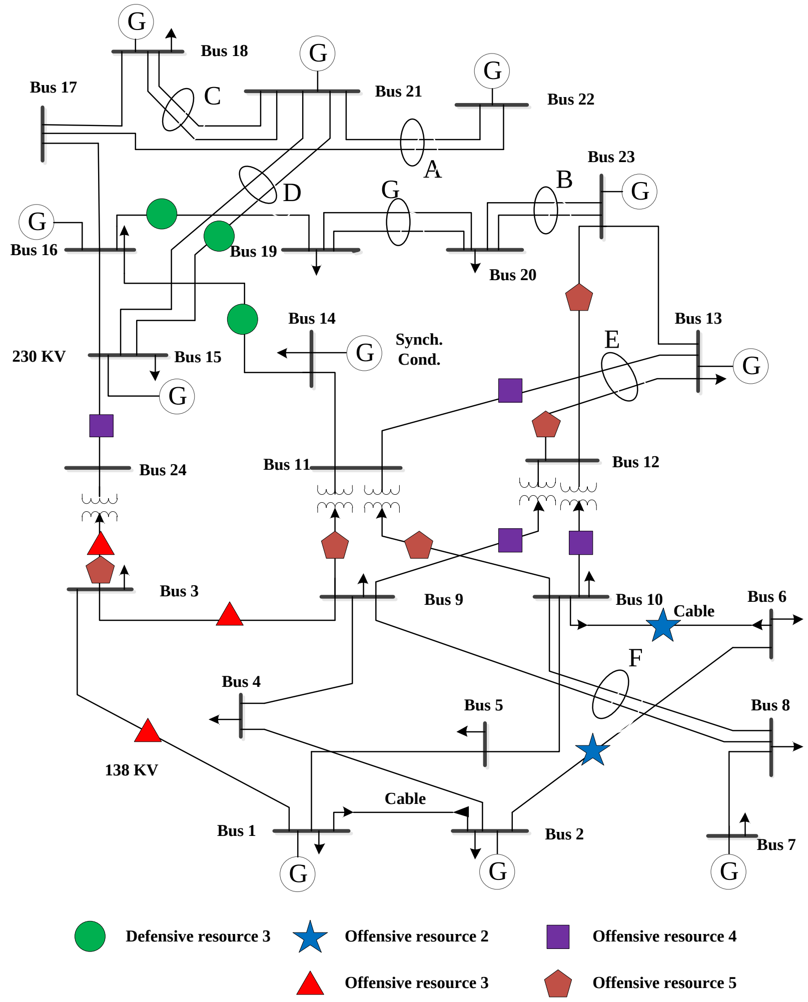


Figure 6. 4 Illustration of the attack and defense strategies for case 2

By comparing the expected load losses, it can be concluded that the value of the expected load loss obtained based on the proposed model is the least. Thus it is concluded that the proposed MAS defender-attacker-defender can minimize the expected load curtailment considering a set of multiple offensive resources, and the performance of the proposed method is better than the robust optimization.

B) Sensitivity Study of the Attack Scenario Probabilities

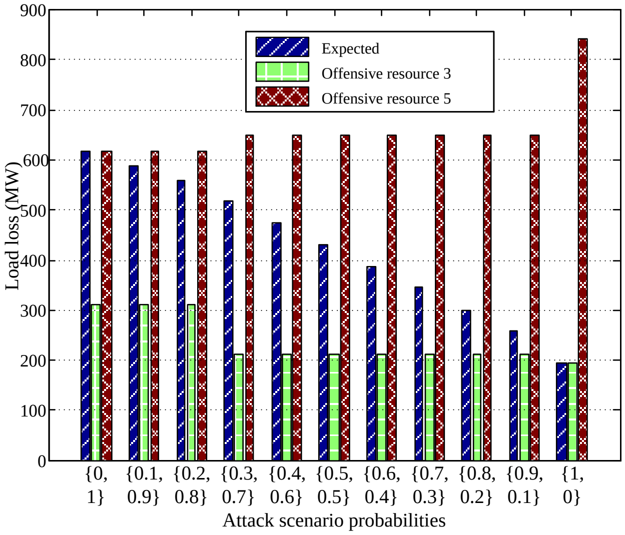


Figure 6. 5 Consequences for the sensitivity study of the attack scenario probabilities

In order to check the impact of the attack scenario probabilities, i.e., the uncertainty related to the offensive resource, case studies are performed by assuming two attack scenarios, i.e., attacking three lines and attacking five lines. The defensive resource is 3, i.e., the defender can harden three lines. The probabilities of these two attack scenarios vary from {0, 1} to {1, 0} with the step 0.1, and there are total 11 cases. By solving the proposed MAS defender-attacker-defender model, the defensive strategy and the associated offensive strategy for each attack scenario in each case are shown in Table 6.5. Also, the expected load loss and the load loss for each attack scenario in each case are shown in Fig. 6.5.

It is shown in Table 6.5 that the defensive strategy can change with the probabilities of the attack scenarios. For example, the defended lines are {10-12, 12-23, 14-16} when the probabilities are {0.1, 0.9} while the defended lines are {14-16, 16-17, 16-19} if the probabilities are {0.7, 0.3}. Also, it is found that in some cases the defensive strategy is sensitive to these probabilities: a small variation of these probabilities can result in different defense strategies; while in some other cases, it is not that sensitive. For example, the defended lines for the probabilities {0.7, 0.3} are different from those for the probabilities {0.6, 0.4} and the probabilities {0.8, 0.2}. The defended lines for the probabilities {0, 1} are the same for those for the probabilities {0.1, 0.9}, which indicates in this case the defensive strategy will not be affected by a small error in the estimation of the probabilities.

Table 6. 5 Defensive and offensive strategies for the sensitivity study of the attack scenario probabilities

Probabilities of scenarios	Defended lines	Attacked lines	
		Offensive resource 3	Offensive resource 5
{0, 1}	10-12, 12-23, 14-16	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.1, 0.9}	10-12, 12-23, 14-16	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.2, 0.8}	9-12, 12-23, 14-16	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.3, 0.7}	9-12, 12-23, 14-16	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.4, 0.6}	3-24, 14-16, 15-24	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.5, 0.5}	10-12, 12-23, 14-16	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.6, 0.4}	3-24, 14-16, 15-24	16-19, 20-23, 20-23	11-14, 15-16, 16-17, 20-23, 20-23
{0.7, 0.3}	14-16, 16-17, 16-19	1-3, 3-9, 3-24	3-24, 9-11, 9-12, 10-11, 10-12
{0.8, 0.2}	14-16, 15-21, 16-19	1-3, 3-9, 3-24	3-24, 9-11, 10-11, 12-13, 12-23
{0.9, 0.1}	14-16, 15-21, 16-19	1-3, 3-9, 3-24	3-24, 9-11, 10-11, 12-13, 12-23
{1, 0}	11-14, 16-17, 16-19	1-3, 3-9, 3-24	3-24, 11-13, 12-13, 12-23, 14-16

As for the resultant consequences related to these probabilities, it is shown in Fig. 6.5 that the expected value of the load loss decreases with the increasing probability of attacking 3 lines and the decreasing probability of attacking 5 lines.

C) Impact of the Defensive Resource

In this part, case studies are carried out to check the impact of the defensive resource on the optimal defensive strategy development. Under a given offensive resource set {2, 3, 4, 5} with the corresponding probabilities {0.2, 0.3, 0.4, 0.1}, the defensive resource varies from 1 to 5 with the step 1. The defensive and offensive strategies are presented in Table 6.6, and the corresponding consequences are shown in Fig. 6.6. From Table 6.6 and Fig. 6.6, it is demonstrated that with the increase of the defensive resource, some critical lines which are targets of attacks will be protected, leading to decreased expected load loss. It should be noted that the consequence caused by a specific attack scenario does not necessarily decrease with the increase of the defensive resource. For example, in Fig. 6.6 the load loss caused by the scenario of attacking two lines is the least when the defensive resource is 4, and that is less than the corresponding load loss when the defensive resource is 5. This is because the proposed model aims to minimize the expected load loss considering all the possible attack scenarios and their related probabilities.

Table 6. 6 Defensive and offensive strategies for the impact of the defensive resource

Defensive resource	Defended lines	Attacked lines			
		Offensive resource 2	Offensive resource 3	Offensive resource 4	Offensive resource 5
1	14-16	2-6, 6-10	16-19, 20-23, 20-23	7-8, 15-21, 15-21, 16-17	3-24, 9-11, 10-11, 12-13, 12-23
2	14-16, 20-23	2-6, 6-10	15-21, 15-21, 16-17	7-8, 15-21, 15-21, 16-17	9-12, 10-12, 11-13, 11-14, 15-24
3	14-16, 15-21, 16-19	2-6, 6-10	1-3, 3-9, 3-24	9-12, 10-12, 11-13, 15-24	3-24, 9-11, 10-11, 12-13, 12-23
4	2-6, 14-16, 16-17, 16-19	2-4, 4-9	1-3, 3-9, 15-24	11-13, 12-13, 12-23, 15-24	3-24, 9-12, 10-12, 11-13, 11-14
5	3-24, 14-16, 15-24, 16-17, 16-19	2-6, 6-10	7-8, 8-9, 8-10	9-11, 9-12, 10-11, 10-12	11-13, 12-13, 12-23, 20-23, 20-23

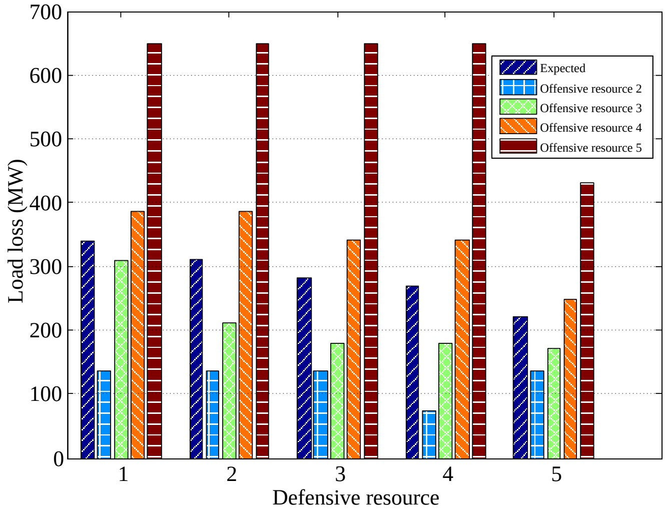


Figure 6. 6 Consequences for the impact of the defensive resource

In addition, this kind of sensitivity analysis for the defensive resource can provide information about the amount of defensive resource needed to maintain a certain security level. For example, it is demonstrated in Fig. 6.6 that the minimum defensive resource required is 3 in order to ensure the expected load loss below 300 MW.

6.4.2 IEEE 57-bus system

In order to further illustrate the computation time of the proposed approach, more simulation studies are conducted based on a larger system, i.e., the IEEE 57-bus system. This test system has 57 buses, 80 transmission branches, and 7 generation units. The capability of each transmission line is set to 110 MVA, and more detailed information can be found at [79].

As an example, the cyber security expert receives intrusion alarm from the IDS and estimates the attacker may be capable of attacking 2 or 3 lines with the probabilities of 0.8 and 0.2, respectively. The defense strategy is to defend line 1-16, 1-17, and 7-29 if the defender has the resource to defend three lines. The expected load loss is 42.6 MW as shown in Table 6.7. As a comparison, if assuming the most possible offensive resource, i.e., 2 lines, the obtained defense strategy can lead to the expected load loss of 54.2 MW; if assuming the worst-case offensive resource, i.e., 3 lines, the expected load loss is 43.9 MW. By comparison, it shows that the proposed approach is the most effective one.

Table 6. 7 Comparative studies for IEEE 57-bus system

Defended lines	Load loss (MW)		
	Attack scenario 1	Attack scenario 2	Expected
1-16, 1-17, 7-29	39	57	42.6
1-16, 1-17, 32-33	35.8	128	54.2
1-15, 3-15, 7-29	43	47.6	43.9

The calculation time is 1,354 seconds. Compared with the calculation time for the RTS79 system, it can be shown that the calculation time increases with the system size.

6.5 Conclusions

Considering the fact that the defender often faces uncertainties related to the offensive resource of the attacker when making defense plans, this chapter proposes an MAS defender-attacker-defender model, which captures the uncertainties of the attacker's offensive resource as well as the interaction between the security personnel, the attacker, and the power system operator. The MAS defender-attacker-defender model is decomposed into an ULP and an LLP. The C&CG algorithm is implemented based on the ULP and the LLP to solve the overall MAS defender-attacker-defender problem, while stochastic programming technique is applied in the ULP. Case studies are performed based on representative IEEE test systems, and different offensive resources and defensive resources are considered in the case studies. The comparative studies validate that the proposed MAS defender-attacker-defender model can minimize the expected load loss considering a group of attack scenarios which represents the uncertainty related to the attacker. This proposed approach has the potential to be implemented in the decision-making part of the defensive system of the transmission system.

7. Conclusions and Future Work

This chapter concludes the whole dissertation and provides future research directions.

7.1 Conclusions

This dissertation studies the impacts of various kinds of attacks on power system reliability, and proposes defense methods against the attacks. The work in each chapter is summarized as follows.

- Chapter 2 is focused on quantifying the impact of substation cyber vulnerabilities on power supply adequacy. The temporal occurrence pattern of cyber attacks is statistically analyzed based on the human dynamics theory. Also, the attack/defense interactions of intelligent attackers and defenders are modeled by static and Markov games in different attack scenarios. A novel power system adequacy evaluation framework is proposed by incorporating both physical failures and cybersecurity risks. Simulation studies are performed on a typical IEEE reliability test system, and the influences of critical factors related to cybersecurity are carefully investigated. These quantitative studies show that implementing effective cyber security measures and making informed decisions about the allocation of limited resources are beneficial to enhancing the overall adequacy of contemporary cyber-physical power systems.
- Chapter 3 quantifies the influence of load redistribution attack on the long-term power supply reliability. The intrusion process for manipulating the measurements is modeled by the semi-Markov models. Considering the practical cross-check for suspicious measurements, the regional load redistribution attack model is proposed. A holistic framework incorporating the physical failures and the LR attack is proposed for cyber-physical power system reliability evaluation. The simulation is carried out on the IEEE RTS79 system. The influences of critical

factors and strategies are analyzed. It is concluded that the LR attacks have a non-negligible impact on the power system reliability.

- Chapter 4 studies coordinated attacks against power systems; in this chapter the cyber-physical security of the power system is analyzed and probable coordinated attack scenarios are proposed. Two typical attack coordination examples are studied in detail: the coordination between load redistribution attack and attacking generators; and the coordination between LR attack and attacking lines. They are formulated as bilevel optimization problems, where the attacker at the upper level aims to maximize the load curtailment while the defender at the lower level makes an effort to reduce the load curtailment. The case studies conducted based on a modified IEEE 14-bus system demonstrate the potential damaging effects of the coordinated attacks. And it is shown that coordinated attacks could cause higher load curtailment than the standalone attacks.
- Chapter 5 studies power system robust operation strategy; a holistic robustness framework is proposed by extending the conventional security-constrained optimal power flow analysis to incorporate the risk caused by attacks. The corresponding solution methodology is proposed by combining particle swarm optimization and primal-dual interior point methods. Case studies conducted based on several test systems demonstrate that the proposed SCOPF model is able to reduce the consequence of attacks. This study can provide some insight into improving the power system operation robustness in the face of significant attacks.
- Chapter 6 addresses the allocation of the defensive resource to minimize the damage when there are uncertainties regarding the resource that the attacker has. A Multiple-Attack-Scenario defender-attacker-defender model is proposed by extending the conventional trilevel defender-attacker-defender model. The proposed model considers the uncertainties related to

the offensive resource and the interactions involving the security personnel at the top-level, the attacker at the middle-level, and the power system operator at the bottom-level. The Column-and-Constraint Generation algorithm is implemented by decomposing the MAS defender-attacker-defender model into an upper-level problem for the security personnel, and a lower-level problem for the attacker involving the optimal power flow analysis-based corrective power re-dispatch implemented by the power system operator. Case studies are performed based on the IEEE RTS79 and 57-bus systems, and the results validate that the proposed method is able to minimize the damage when uncertainties are involved in the offensive resource.

7.2 Future Work

The future work can be explored in such directions as described as follows.

- Analyzing the impact of more types of attacks on power system reliability;
- Studying the occurrence frequency of attacks considering more statistical data and more advanced human dynamics models;
- Investigating the cyber intrusion paths in more detail;
- Developing power system robust optimization against false data injection attacks;
- Identifying the critical substations, generators, measurements in case of attacks with uncertainties.

REFERENCES

[1] H. Sui, H. Wang, M. Lu, and W. Lee, “An AMI System for the Deregulated Electricity Markets,” *IEEE Trans. Ind. Appl.*, vol. 45, no. 6, pp. 2104–2108, 2009.

[2] N. Liu, J. Zhang, and X. Wu, “Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems—Part II: Application in Substation,” *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 876–881, Apr. 2011.

[3] X. Zhang, K. Tomsovic, and A. Dimitrovski, “Optimal Investment on Series FACTS Device Considering Contingencies,” in *Proc. of the 48th North American Power Symposium (NAPS)*, Denver, CO, USA, 2016.

[4] X. Zhang, K. Tomsovic, and A. Dimitrovski, “Security Constrained Multi-Stage Transmission Expansion Planning Considering a Continuously Variable Series Reactor,” *IEEE Trans. Power Syst.*, in press

[5] C. Yuan, M. S. Illindala, and A. S. Khalsa, “Co-Optimization Scheme for Distributed Energy Resource Planning in Community Microgrids,” *IEEE Trans. Sustain. Energy*, vol. 8, no. 4, pp. 1351–1360, Oct. 2017.

[6] C. Yuan, M. A. Haj-ahmed, and M. S. Illindala, “Protection Strategies for Medium-Voltage Direct-Current Microgrid at a Remote Area Mine Site,” *IEEE Trans. Ind. Appl.*, vol. 51, no. 4, pp. 2846–2853, Jul. 2015.

[7] http://news.sky.com/story/1414477/militant-attack-plunges-pakistan-into-darkness [Accessed: 30 March 2017].

[8] http://www.securityfocus.com/news/6767 [Accessed: 30 March 2017].

[9] http://www.zerohedge.com/news/2016-04-27/german-nuclear-power-plant-confirms-it-was-infected-computer-viruses [Accessed: 30 March 2017].

[10] http://news.cnet.com/CIA-Cyberattack-caused-multiple-city-blackout/2100-7349_3-6227090.html [Accessed: 30 March 2017].

[11] Electricity information sharing and analysis center, “Analysis of the Cyber Attack on the Ukrainian Power Grid.” March, 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-SAC_SANS_Ukraine_DUC_18Mar2016.pdf

[12] https://thehackernews.com/2016/01/power-grid-cyberattack.html [Accessed: 19 November 2017].

[13] http://www.breitbart.com/london/2015/01/12/green-energy-leaves-national-grid-more-vulnerable-to-constant-cyber-attacks/ [Accessed: 30 March 2017].

[14] North American Electric Reliability Corporation (NERC), "The High-Impact, Low-Frequency Event Risk to the North American Bulk Power System", 2009.

[15] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems --- Attacks, Impacts, and Defense: A Survey," *IEEE Trans. Ind. Informatics*, vol. 13, no. 2, pp. 411–423, 2016.

[16] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[17] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1609–1624, 2017.

[18] A. Anwar, A. N. Mahmood, and M. Pickering, "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 58–72, 2017.

[19] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 3–13, Jan. 2014.

[20] Y. Xiang, L. Wang, and Y. Zhang, "Adequacy Evaluation of Electric Power Grids Considering Substation Cyber Vulnerabilities," International Journal of Electrical Power and Energy Systems, in press.

[21] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

[22] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "Resilience Analysis of Power Grids under the Sequential Attack," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2340 - 2354, 2014.

[23] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "Joint Substation-Transmission line Vulnerability Assessment against the Smart Grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 1010–1024, May 2015.

[24] A. Ghaedi, A. Abbaspour, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Toward a Comprehensive Model of Large-Scale DFIG-Based Wind Farms in Adequacy Assessment of Power Systems," *IEEE Trans. Sustain. Energy*, vol. 5, no. 1, pp. 55–63, Jan. 2014.

[25] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Safdarian, "Impact of WAMS Malfunction on Power System Reliability Assessment," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1302–1309, Sep. 2012.

[26] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Khodaei, “Observability enhancement by optimal PMU placement considering random power system outages,” *Energy Syst.*, vol. 2, no. 1, pp. 45–65, Mar. 2011.

[27] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Khodaei, “Probabilistic multistage PMU placement in electric power systems,” *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 841–849, Apr. 2011.

[28] Y. Wang, W. Li, J. Lu, and H. Liu, “Evaluating multiple reliability indices of regional networks in wide area measurement system,” *Electr. Power Syst. Res.*, vol. 73, no. 10, pp. 1353–1359, Oct. 2009.

[29] Y. Wang, W. Li, and J. Lu, “Reliability analysis of wide-area measurement system,” *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1483–1491, Jul. 2010.

[30] NERC, Definition of Adequate Level of Reliability, Dec. 2007. [Online]. Available: http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf

[31] H. Holm, “A Large-Scale Study of the Time Required to Compromise a Computer System,” *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 1, pp. 2–15, Jan. 2014.

[32] B. Gonçalves and J. Ramasco, “Human dynamics revealed through Web analytics,” *Phys. Rev. E*, vol. 78, no. 2, p. 026123, Aug. 2008.

[33] T. Zhou, H. A. T. Kiet, B. J. Kim, B.-H. Wang, and P. Holme, “Role of activity in human dynamics,” *EPL (Europhysics Lett.)*, vol. 82, no. 2, p. 28002, Apr. 2008.

[34] J.-F. Zhu, X.-P. Han, and B.-H. Wang, “Scaling property and opinion model for interevent time of terrorism attack,” [Online]. Available: http://arxiv.org/abs/0910.3985

[35] N. Johnson, M. Spagat, J. Restrepo, J. Bohorquez, N. Suarez, E. Restrepo, and R. Zarama, “From old wars to new wars and global terrorism,” [Online]. Available: http://arxiv.org/abs/physics/0506213.

[36] [Online]. Available: http://hackmageddon.com/cyber-attacks-timeline-master-indexes/

[37] A.-L. Barabási, “The origin of bursts and heavy tails in human dynamics.,” *Nature*, vol. 435, no. 7039, pp. 207–11, May 2005.

[38] A. Vazquez, “Impact of memory on human dynamics,” *Phys. A Stat. Mech. its Appl.*, vol. 373, pp. 747–752, Jan. 2007.

[39] Z. Jun-Fang, H. Xiao-Pu, and W. Bing-Hong, “Statistical Property and Model for the Inter-Event Time of Terrorism Attacks,” *Chinese Phys. Lett.*, vol. 27, no. 6, p. 068902, Jun. 2010.

[40] N. Liu, J. Zhang, H. Zhang, and W. Liu, “Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM,” *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

[41] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, “Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation,” *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379 - 4394, 2016.

[42] Y. Liu, H. Man, and C. Comaniciu, “A Game Theoretic Approach to Efficient Mixed Strategies for Intrusion Detection,” in *2006 IEEE International Conference on Communications*, 2006, vol. 5, pp. 2201–2206.

[43] M. J. Eppstein and P. D. H. Hines, “A ‘Random Chemistry’ Algorithm for Identifying Collections of Multiple Contingencies That Initiate Cascading Failure,” *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[44] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, “Markov Game Analysis for Attack-Defense of Power Networks Under Possible Misinformation,” *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1–1, 2012.

[45] T. Alpcan and T. Basar, Network Security: A Decision and Game Theoretic Approach, Cambridge, U.K.: Cambridge Univ. Press, 2010.

[46] J. Stamp, A. McIntyre, and B. Ricardson, “Reliability impacts from cyber attack on electric power systems,” in *Proc. IEEE Power Systems Conference and Exposition*, pp. 1-8, Seattle, WA, March 2009.

[47] R. Billinton and W. Li, Reliability Assessment of Electric Power Systems Using Monte Carlo Methods. New York; London: Plenum, 1994.

[48] P. M. Subcommittee, “IEEE reliability test system,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov. 1979.

[49] Y. Yan, Y. Qian, H.Sharif, and D.Tipper, “A Survey on Cyber Security for Smart Grid Communications,” *IEEE Communications Surveys and Tutorials*, vol. 14, fourth quarter, 2012.

[50] Y. Liu, P. Ning, and M. K. Reiter, “False Data Injection Attacks Against State Estimation in Electric Power Grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[51] Y. Yuan, Z. Li, and K. Ren, “Modeling Load Redistribution Attacks in Power Systems,” *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[52] Y. Zhang, L. Wang, and Y. Xiang, “Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems,” *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669-683, 2016.

[53] J. Almasizadeh and M. A. Azgomi, “Intrusion Process Modeling for Security Quantification,” in *2009 International Conference on Availability, Reliability and Security*, 2009, pp. 114–121.

[54] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, “A method for modeling and quantifying the security attributes of intrusion tolerant systems,” *Perform. Eval.*, vol. 56, no. 1–4, pp. 167–186, Mar. 2004.

[55] N. Limnios, “Dependability analysis of semi-Markov systems,” *Reliab. Eng. Syst. Saf.*, vol. 55, no. 3, pp. 203–207, Mar. 1997.

[56] K.S. Trivedi, “Probability and Statistics with Reliability, Queuing, and Computer Science Applications”, 2nd ed., Wiley, New York, 2001.

[57] T. Sommestad, M. Ekstedt, and L. Nordstrom, “Modeling Security of Power Communication Systems Using Defense Graphs and Influence Diagrams,” *IEEE Trans. Power Deliv*., vol. 24, no. 4, pp. 1801–1808, Oct. 2009.

[58] M. Majdalawieh, F. P.-Presicce, and D. Wijesekera, “DNPSec: Distributed network protocol version 3 (DNP3) security framework,” Advances in Computer, Information, and Systems Sciences, and Engineering, Springer Netherlands, 2006, 227-234.

[59] T. Radu and S. Mircea, “Evaluation of DES, 3 DES and AES on Windows and UNIX platforms,” *in 2010 IEEE International Joint Conference on Computational Cybernetics and Technical Informatics* (ICCC-CONTI), 2010.

[60] S. Manuel, “Classification and generation of disturbance vectors for collision attacks against SHA-1,” Designs, Codes and Cryptography 59.1-3 2011, 247-263.

[61] Lee, D.; Kim, H.; Kim, K.; Yoo, P.D. “Simulated Attack on DNP3 Protocol in SCADA System,” in *Proceedings of the 31th Symposium on Cryptography and Information Security*, Kagoshima, Japan, 21–24 January 2014.

[62] I. Nai Fovino, A. Carcano, M. Masera and A. Trombetta, "An experimental investigation of malware attacks on SCADA systems", *Int. J. Critical Infrastructure Protection*, vol. 2, no. 4, 2009

[63] U. Meyer and S. Wetzel, “On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks,” in *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications* (IEEE Cat. No.04TH8754), vol. 4, pp. 2876–2883.

[64] A. Myasnikov, V. Shpilrain and A. Ushakov, " A Practical Attack on a Braid Group Based Cryptographic Protocol", in *25th Annual International Cryptology Conference*, vol. 3621, pp 86-96, 2005.

[65] G. Kapoor and S. Piramuthu, “Vulnerabilities in Some Recently Proposed RFID Ownership Transfer Protocols,” in *2009 First International Conference on Networks & Communications*, 2009, pp. 354–357.

[66] I. Arce and E. Levy, “An analysis of the slapper worm,” *IEEE Secur. Priv. Mag.*, vol. 1, no. 1, pp. 82–87, Jan. 2003.

[67] Y. Yuan, Z. Li, and K. Ren, “Quantitative analysis of load redistribution attacks in power systems,” *IEEE Trans. Parallel Distrib. Syst*., vol. 23, pp. 1731–1738, 2012.

[68] NERC, "Cyber attack task force final report," May, 2009. [Online]. Available:http://www.nerc.com/docs/cip/catf/12-ATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf

[69] X. Liu and Z. Li, "Local Load Redistribution Attacks in Power Systems With Incomplete Network Information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[70] Z. Ding, Y. Xiang, and L. Wang, "Quantifying the influence of local load redistribution attack on power supply adequacy," in *2016 IEEE Power and Energy Society General Meeting*, 2016.

[71] Z. Ding, "Quantifying the Influence of False Data Injection Attacks on Power Supply Adequacy," Master thesis, EECS department, University of Toledo, 2016.

[72] M.A. McQueen, W.F. Boyer, M.A. Flynn and G.A. Beitel, &ldquo, "Time-to-Compromise Model for Cyber Risk Reduction Estimation", in *Proc. ACM Conf. Computer and Comm. Security Workshop Quality of Protection*, Sept. 2005.

[73] M. Kaâniche, E. Alata, V. Nicomette, Y. Deswarte, and M. Dacier, "Empirical analysis and statistical modeling of attack processes based on honeypots". in *WEEDS 2006 -Workshop on Empirical Evaluation of Dependability and Security* (in conjunction with the International Conference on Dependable Systems and Networks, DSN 2006), Jun 2006.

[74] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004. [Online]. Available: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf [Accessed: 30 March 2017].

[75] S. Mei, Y. Ni, G. Wang, and S. Wu, "A Study of Self-Organized Criticality of Power System Under Cascading Failures Based on AC-OPF With Voltage Stability Margin," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.

[76] J. Salmeron, K. Wood, and R. Baldick, "Analysis of Electric Grid Security Under Terrorist Threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[77] J. M. Arroyo and F. D. Galiana, "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.

[78] IBM CPLEX. [Online]. Available: http://www-03.ibm.com/software/products/en/ibmilogcpleoptistud [Accessed: 30 May 2017].

[79] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[80] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber Attacks against the Economic Operation of Power Systems: A Fast Solution," *IEEE Trans. Smart Grid, pp. 1–1, 2016.*

[81] R. Arghandeh, A. v. Meierb, L. Mehrmanesh, and L Mili, “On the definition of cyber-physical resilience in power systems,” *Renewable and Sustainable Energy Reviews*, vol.58, pp. 1060–1069, May 2016.

[82] National Infrastructure Advisory Council, “Strengthening Regional Resilience through National, Regional, and Sector Partnerships.” Nov., 2013. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/niac-rrwg-report-final-review-draft-for-qbm.pdf

[83] Q. Zhu and T. Basar, “Robust and resilient control design for cyber-physical systems with an application to power systems.” in *50th IEEE Conference on Decision and Control and European Control Conference,* 2011.

[84] S. Pan, T. Morris, and U. Adhikari, “Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems,” *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.

[85] National Terrorism Advisory System. [Online]. Available: http://www.dhs.gov/national-terrorism-advisory-system [Accessed: 30 May 2017].

[86] J. Yan, H. He, and Y. Sun, “Integrated Security Analysis on Cascading Failure in Complex Networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 3, pp. 451–463, Mar. 2014.

[87] R. Fitzmaurice, A. Keane, and M. O’Malley, “Effect of Short-Term Risk-Aversive Dispatch on a Complex System Model for Power Systems,” *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 460–469, Feb. 2011.

[88] F. Capitanescu and L. Wehenkel, “A New Iterative Approach to the Corrective Security-Constrained Optimal Power Flow Problem,” *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1533–1541, Nov. 2008.

[89] Y. Xu, Z. Y. Dong, R. Zhang, K. P. Wong, and M. Lai, “Solving Preventive-Corrective SCOPF by a Hybrid Computational Strategy,” *IEEE Trans. Power Syst.*, vol. 29, no. 3, pp. 1345–1355, May 2014.

[90] J. Cao, W. Du, and H. F. Wang, “An Improved Corrective Security Constrained OPF with Distributed Energy Storage,” *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1537-1545, 2016.

[91] J. Kennedy and R. Eberhart, “Particle swarm optimization,” in *IEEE Proceedings of ICNN’95 - International Conference on Neural Networks*, 1995, vol. 4, pp. 1942–1948.

[92] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, Power generation, operation, and control. 2nd ed. New York: John Wiley & Sons, Inc.; 1996.

[93] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, “Power System Structural Vulnerability Assessment based on an Improved Maximum Flow Approach,” *IEEE Trans. Smart Grid*, in press.

[94] W. Yuan, L. Zhao and B. Zeng, "Optimal power grid protection through a defender–attacker–defender model," *Reliability Engineering & System Safety*, vol. 121, pp. 83-89, Jan. 2014.

[95] N. Alguacil, A. Delgadillo, and J. M. Arroyo, "A trilevel programming approach for electric grid defense planning," *Computers & Operations Research*, vol. 41, pp. 282-290, Jan. 2014.

[96] B. Zeng, and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Operations Research Letters*, vol. 141, pp. 457-461, Sept. 2013.

[97] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[98] L. Wei, A. Sarwat, W. Saad, and S. Biswas, "Stochastic Games for Power Grid Protection Against Coordinated Cyber-Physical Attacks," *IEEE Trans. on Smart Grid*, 2016, in press.

[99] X. Wu and A. J. Conejo, "An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning," *IEEE Trans. Power Syst.*, 2016, in press.

[100] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.

[101] G. P. McCormick, "Computability of global solutions to factorable nonconvex programs: Part I — Convex underestimating problems," *Mathematical Programming*, vol. 10, pp. 146–175, 1976.

[102] X. Zhang, D. Shi, Z. Wang, etc., "Optimal Allocation of Static Var Compensator via Mixed Integer Conic Programming," in *Proc. IEEE PES General Meeting*, Chicago, IL, USA, 2017.

[103] X. Zhang, D. Shi, Z. Wang, etc., "Bilevel Optimization Based Transmission Expansion Planning considering Phase Shifting Transformer," in *Proc. of the 49th North American Power Symposium (NAPS)*, Morgantown, WV, USA, 2017.

CURRICULUM VITAE

YINGMENG XIANG

EDUCATION

Ph.D. in Electrical Engineering Aug. 2014 – Dec. 2017
The University of Wisconsin-Milwaukee, Milwaukee, WI GPA 4.0/4.0

Ph.D. Student in Electrical Engineering Jan. 2013 – July 2014
The University of Toledo, Toledo, OH GPA 3.9/4.0

M.S. in Electrical Engineering Sept. 2010 – Dec. 2012
Huazhong University of Science and Technology, Wuhan, China GPA 3.6/4.0

B.S. in Electrical Engineering Sept. 2006 – June 2010
Chongqing University, Chongqing, China GPA 3.5/4.0

WORK EXPERIENCES

R&D Intern/Research Associate, GEIRINA, CA May 2017 – Dec. 2017

- Developed a cloud based smart plug firmware device for online power monitoring and control
- Proposed a robust optimization strategy for transmission defense against sequential attacks.
- Incorporated load and renewable uncertainties into the defender-attacker-operator model.

RESEARCH EXPERIENCES

Research Assistant, UWM, Milwaukee, WI Aug. 2014 – Present

- Proposed a robust operation strategy considering malicious attacks and cascading failures.
- Constructed a trilevel robust optimization model for identifying critical transmission lines.
- Explored dynamic thermal rating, transmission switching, and network topology optimization.
- Investigated plausible cyber attack scenarios against the SCADA system.
- Analyzed the optimal coordinated attack strategies combining different attack scenarios.
- Proposed an efficient method for identifying contingencies that initiate cascading failures.

- Assessed the impact of false data injection attacks against state estimation on power adequacy.
- Developed game-theoretical methods for defending against false data injection attacks.
- Developed two software tools for water/wastewater infrastructure reliability evaluation.

Research Assistant, University of Toledo, Toledo, Ohio Jan. 2013-Aug. 2014

- Proposed a holistic power system reliability assessment model.
- Investigated attack paths for tripping the substation breakers.
- Studied the cyber vulnerabilities of unified power flow controller.
- Assessed the impacts of electric vehicle on the distribution network and environment.

Student, Wuhan National High Magnetic Field Center, Wuhan, China Sept. 2010-Dec. 2012

- Designed, built, and tested a 10 kW/10 kV LLC capacitor charging hardware device.
- Designed and manufactured multiple transformers (20 kW/20 kV/15 kHz).
- Proposed a new 10 kW repetitive pulsed system, and generated 8 Tesla/1.2 Hz magnetic field.

FELLOWSHIPS AND AWARDS

- Excellent Reviewer Award, Journal of Modern Power Systems and Clean Energy, Dec. 2016
- Distinguished Graduate Student Fellowship, UWM, Mar. 2016
- Best Reviewer Award of IEEE Transactions on Smart Grid, Nov. 2015
- Outstanding Student Awards, Huazhong University of Science & Technology, 2010-2012
- Outstanding Graduate Award, Chongqing University, Jun. 2010
- China National Scholarship, Ministry of Education of China, Nov. 2009

PROFESSIONAL ACTIVITIES

- Student member of IEEE and IEEE Power & Energy Society.
- Member of American Association for the Advancement of Science (AAAS).
- Reviewer for prestigious journals, including
    - IEEE Transactions on Smart Grid
    - IEEE Transactions on Power Systems
    - IEEE Power Engineering Letters
    - IEEE Access

International Transactions on Electrical Energy Systems
Sustainable Energy Technologies and Assessments- Elsevier
Intelligent Industrial Systems-Springer
Journal of Modern Power Systems and Clean Energy

- Actively Served on international conference Technical Program Committee, including
  2018 IEEE International Conference on Communications (ICC)
  2015-2017 IEEE International Conference on Smart Grid Communications

PEER-REVIEWED PUBLICATIONS

Peer-Reviewed Journal Publications:

[1] **Y. Xiang**, L. Wang, and Y. Zhang, "Adequacy Evaluation of Electric Power Grids Considering Substation Cyber Vulnerabilities," *International Journal of Electrical Power and Energy Systems,* Accepted.

[2] **Y. Xiang**, L. Wang, and N. Liu, "A Robustness-Oriented Power Grid Operation Strategy Considering Attacks," *IEEE Transactions on Smart Grid*, Accepted.

[3] **Y. Xiang**, Z. Ding, Y. Zhang and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889-901, 2017.

[4] **Y. Xiang**, L. Wang, and N. Liu, "Coordinated Attacks on Electric Power Systems in a Cyber-Physical Environment," *Electric Power Systems Research*, vol. 149, pp. 156–168, Aug. 2017.

[5] **Y. Xiang**, and L. Wang, "A Game-Theoretic Study of Load Redistribution Attack and Defense in Power Systems," *Electric Power Systems Research*, vol. 151, pp. 12–25, Oct. 2017.

[6] 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.

[7] M. Wang, **Y. Xiang**, and L. Wang, "Identification of Critical Contingencies Using Solution Space Pruning and Intelligent Search," *Electric Power Systems Research*, vol. 149, pp. 220–229, Aug. 2017.

[8] Y. Zhang, L. Wang, **Y. Xiang**, and C.-W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[9] Y. Zhang, L. Wang, and **Y. Xiang**, "Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 669 - 683, 2015.

[10] Y. Zhang, L. Wang, **Y. Xiang**, and C.-W. Ten, "Power System Reliability Evaluation with SCADA

Cybersecurity Considerations," *IEEE Transactions on Smart Grid,* vol. 6, no. 4, pp. 1707 - 1721, 2015.

[11] R. Yang, H. Ding, Y. Xu, L. Yao, and **Y. Xiang**, "An Analytical Steady-State Model of LCC type Series–Parallel Resonant Converter with Capacitive Output Filter," *IEEE Transactions on Power Electronics,* vol. 29, no. 1, pp. 328–338, Jan. 2014.

[12] Y. Xu, **Y. Xiang,** Q. Wan, R. Yang, H. Xiao, H. Ding, and L. Li, "A Dual-Capacitors Type Energy Recovery Power System for Repetitive Pulsed High Magnetic Fields," *Journal of Low Temperature Physics,* vol. 170, no. 5–6, pp. 488–495, Oct. 2012.

[13] Y. Xu, R. Yang, **Y. Xiang**, H. Ding, T. Ding, and L. Li, "Design of a Novel Pulsed Power System for Repetitive Pulsed High Magnetic Fields," *IEEE Transactions on Applied Superconductivity*., vol. 22, no. 3, Jun. 2012.

Peer-Reviewed Conference Publications:

[14] M. Liao, D. Shi, Z. Yu, W. Zhu, Z Wang, and **Y. Xiang**, "Recover the lost Phasor Measurement Unit Data Using Alternating Direction Multipliers Method,"*2018 IEEE PES T&D Conference and Exposition*, Accepted.

[15] **Y. Xiang**, L. Wang, and N. Liu, "A Framework for Modeling Load Redistribution Attacks Coordinating with Switching Attacks," in *2017 IEEE Power and Energy Society General Meeting*, 2017.

[16] **Y. Xiang** and L. Wang, "A Robust Optimization-Based Strategy for Optimal Power System Protection Considering Uncertainties," in *2017 IEEE Power and Energy Society General Meeting*, 2017.

[17] **Y. Xiang**, L. Wang, N. Liu, R. Xiao, and K. Xie, "A Resilient Power System Operation Strategy Considering Presumed Attacks", *International Conference on Probabilistic Methods Applied to Power Systems*, 2016.

[18] **Y. Xiang**, L. Wang, R. Xiao, and K. Xie, "Impact of Network Topology Optimization on Power System Reliability", *International Conference on Probabilistic Methods Applied to Power Systems*, 2016.

[19] R. Xiao, **Y. Xiang**, L. Wang, and K. Xie, "Bulk Power System Reliability Evaluation Considering Optimal Transmission Switching and Dynamic Line Thermal Rating", *International Conference on Probabilistic Methods Applied to Power Systems*, 2016.

[20] M. Wang, **Y. Xiang**, L. Wang, J. Jiang, R. Xiao, and K. Xie, "Identification of Critical Line-Generation Combinations for Hypothesized Joint Line-Generation Attacks", *International Conference on Probabilistic Methods Applied to Power Systems*, 2016.

[21] H. Li, L. Wang, **Y. Xiang**, J. Tan, R. Xiao, and K. Xie, "Reliability Evaluation of Active Distribution Systems Considering Energy Storage and Real-Time Electricity Pricing", *International Conference on Probabilistic Methods Applied to Power Systems*, 2016.

[22] Z. Ding, **Y. Xiang** and L. Wang, "Quantifying the Influence of Local Load Redistribution Attack on Power Supply Adequacy," in *2016 IEEE Power and Energy Society General Meeting*.

[23] M. Wang, **Y. Xiang**, L. Wang, D. Yu and J. Jiang, “Critical Line Identification for Hypothesized Multiple Line Attacks Against Power Systems,” in *2016 IEEE PES T&D Conference and Exposition*.

[24] **Y. Xiang**, L. Wang, D. Yu, and N. Liu, “Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks,” in *2015 IEEE Power & Energy Society General Meeting*, 2015.

[25] **Y. Xiang** and L. Wang, “A game-theoretic approach to optimal defense strategy against load redistribution attack,” in *2015 IEEE Power & Energy Society General Meeting*, 2015.

[26] **Y. Xiang**, L. Wang, and Y. Zhang, “Power grid adequacy evaluation involving substation cybersecurity issues,” in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015.

[27] **Y. Xiang**, Z. Ding, and L. Wang, “Power system adequacy assessment with load redistribution attacks,” in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015.

[28] **Y. Xiang**, L. Wang, and T. Fu, “A preliminary study of power system reliability considering cloud service reliability,” in *2014 International Conference on Power System Technology*, 2014, pp. 2031–2036.

[29] Y. Zhang, L. Wang, and **Y. Xiang**, “Power grids reliability appraisal with intrusion tolerant capability in SCADA systems,” in *2014 International Conference on Power System Technology*, 2014, pp. 2025–2030.

[30] Y. Zhang, **Y. Xiang,** and L. Wang, “Reliability Analysis of Power Grids with Cyber Vulnerability in SCADA System,” in *2014 IEEE Power and Energy Society General Meeting*, 2014.

[31] **Y. Xiang**, L. Wang, and Y. Zhang, “Power System Adequacy Assessment with Probabilistic Cyber Attacks against Breakers,” in *2014 IEEE Power and Energy Society General Meeting*, 2014.

[32] **Y. Xiang**, J. Tan, and L. Wang, “A particle swarm optimization based control strategy for plug-in hybrid electric vehicles at residential networks level,” in *2014 IEEE PES T&D Conference and Exposition*, 2014.

[33] **Y. Xiang**, Y. Zhang, L. Wang, and W. Sun, “Impact of UPFC on power system reliability considering its cyber vulnerability,” in *2014 IEEE PES T&D Conference and Exposition*, 2014.