2017

Quantifying the influence of false data injection attacks on power supply adequacy

Zhilu Ding
University of Toledo

A Thesis

entitled

Quantifying the Influence of False Data Injection Attacks on Power Supply Adequacy

by

Zhilu Ding

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Master of Science Degree in Electrical Engineering

_____

Dr. Lingfeng Wang, Committee Chair

_____

Dr. Richard Molyet, Committee Member

_____

Dr. Hong Wang, Committee Member

_____

Dr. Patricia R. Komuniecki, Dean
College of Graduate Studies

The University of Toledo

May 2016

An Abstract of

Quantifying the Influence of False Data Injection Attacks on Power Supply Adequacy

By

Zhilu Ding

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Master of Science Degree in Electrical Engineering

The University of Toledo
May 2016

With the ongoing power grid modernization initiative, more cyber technologies are being deployed in the modern cyber-physical power systems. However, as a result, higher cyberattack risks will be brought about. Local load redistribution attack and unidentifiable attacks, which are two typical types of emerging false data injection attacks, could affect the outcomes of state estimation by compromising some meter measurements and thus misleading the power dispatch. Therefore, it is necessary to analyze the impact of these two types of cyberattacks on the power supply reliability. Here an optimal strategy for constructing the attack vector is studied. The procedure for incorporating the unidentifiable attacks and local load redistribution attacks into the power system reliability assessment framework using Monte Carlo Simulation is proposed. Simulation studies are conducted based on the IEEE 14-bus system. According to the simulation results, it is found that the long-term reliability of the power system could be impacted by the potential cyberattacks if they occur frequently. This study could provide some useful insights into the cybersecurity study of smart grid.

For my parents and friends

Acknowledgements

First, I would like to express my sincere gratitude to my advisor Dr. Lingfeng Wang for his continuous support, professional guidance and great patience for me. His insightful mentorship helped me understand the problem more clearly and come up with the solution more quickly. Without his advice and encouragement, I could not have completed this work.

I would like to thank the funding agency for this project. This work was in part supported by the National Science Foundation (NSF) under Award ECCS1128594.

I would also thank my committee members Dr. Richard Molyet and Dr. Hong Wang for their commitments to serving on this committee from their busy schedules.

I would take this opportunity to express my great thanks to Yichi Zhang, Yingmeng Xiang, Jun Tan, and all the other lab members, for their advice and discussions about my research and for their help on my life at the University of Toledo.

Last but not the least, I would like to thank my family. Without their constant support, encouragement and understanding, it would not have been possible for me to achieve the educational goals.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMI……..	Advanced metering infrastructure
CAIDI……..	Customer Average Interruption Duration Index
CAIFI……..	Customer Average Interruption Frequency Index
EENS……..	Expected Energy Not Supplied
EMS……	Energy Management System
HMI……	Human machine interface
KKT……	Karush–Kuhn–Tucker
LOLE …….	Loss of Load Expectation
LOLP……	Loss of Load Probability
LR……	Load Redistribution
MCS…….	Monte Carlo simulation
MTTF……..	Mean Time to Failure
MTTR…….	Mean Time to Repair
MTUs……..	Master Terminal Units
NERC…….	North American Electric Reliability Council
NIST……...	National Institute of Standards and Technology
OPF…….	Optimal Power Flow

RTUs……	Remote Terminal Units
RUS…….	Rural Utility Service
SCADA……	Supervisory Control and Data Acquisition

Chapter 1

Introduction

1.1 Smart Grid

The traditional electrical power grid is an out-of-date infrastructure. It is generally used to carry power from a few central generators to a large number of users or customers [1]. It has met the needs in the past, however, with the development of our society, this old power system is becoming increasingly overloaded and unsecure. This more and more unstable system has more chances of causing problems and losses, such as blackouts, to the society [2]. For instance, the great blackout, which happened in 2003 in North America, led to billions of dollars losses.

The smart grid provides an answer to the need of the modern life, which is expected to make the electricity grid more intelligent, greener and more efficient. By using modern information technologies, the smart grid is capable of delivering power in more efficient ways and more responsive to various contingencies and events [3]. This more intelligent system will have a great control on the grid, and it is able to respond to events which occur in power generation, transmission and distribution, and even at the consumption ends. Also, the consumers and energy suppliers can take advantage of the convenience, reliability, and energy savings provided through real time energy management [4][5][6]. More specifically, the smart grid can be regarded as an electric system that uses information, two-way, cyber-

secure communication technologies, and computational intelligence in an integrated manner across electricity generation, transmission, substations, distribution and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient, and sustainable [7]. The main difference between the traditional power grid and the smart grid is illustrated in Table 1.1

Table 1.1 the comparison between the traditional grid and smart grid [2]

Existing Grid	**Smart grid**
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Manual monitoring	Self-monitoring
Manual restoration	Self-healing
Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

According to the report of the National Institute of Standards and Technology (NIST) [8], the smart grid has the following main characteristics:

1. Enabling active participation by consumers

2. Accommodating all generation and storage options

3. Enabling new products, services, and markets

4. Improving power quality and reliability

5. Asset utilization optimization and efficiency

6. Self-healing ability

7. Improving resilience operations to attacks and disruption

Also, the smart grid can be divided as three major parts from the technical perspective: smart infrastructure, smart management and smart protection system [2] [9] [10] [11].

- Smart infrastructure system: The smart infrastructure system is the energy, information, and communication infrastructure underlying the smart grid. It supports two-way flows of electricity and information. This features a great difference between the smart grid and the traditional power system. Different with the one-way flow in traditional grids which only deliver the power from the central generation plants to the customers through transmission and distribution systems. In smart grid, the users can not only have their power demand fulfilled by the utilities, bust also can feed the electricity back to the grid via distributed resources such as wind turbines, solar panels, electric vehicles, and so on. The smart infrastructure can also be divided into three sub-systems: the energy system, the information system, and the communication system. These sub-systems work together to improve the efficiency and security of the power supply service for customers [9].

- Smart management system: The smart management system is the subsystem in smart grid that provides advanced management and control services and functionalities. The management system is the key part for the smart grid to realize

their smartness such as energy efficiency improvement, operation cost reduction, demand and supply balance, emission control, and utility maximization [9] [10]. With the development of these management technologies, the smart grid equipped with more and more advance infrastructures can be smarter. The main objective of the management system of the smart grid is focused on energy efficiency and demand profile improvement; utility and cost optimization, and price stabilization and emission control.

- Smart protection system: The smart protection system is the subsystem that provides advanced grid reliability analysis, failure protection, and security and privacy protection services [9] [11]. With the development of smart grid, more and more information technologies are being integrated into the power system. At the same time, with these advance infrastructures, the smart gird is becoming more and more complex. Hence, the smart grid must provide a smarter protection system to effectively address the potential cyber security issues, respond and recover from the disruption, and protect the privacy of utilities and customers. The main objective of the protection system in smart grid is focused on failure prediction and prevention, failure identification, diagnosis, and recovery.

1.2 Cyber Security in Smart Grid

With the rapid development of computing, communication and information technologies in smart grid, more smart meters and other advanced cyber-based devices are being installed in the power grid for accomplishing various more effective measurement, control, monitoring, and protection tasks [12]. However, the corresponding cyberattacks

issues are being brought about to the smart grid as well. Figure 1-1 describes the sources which could cause cyber security issues in smart grid [13].

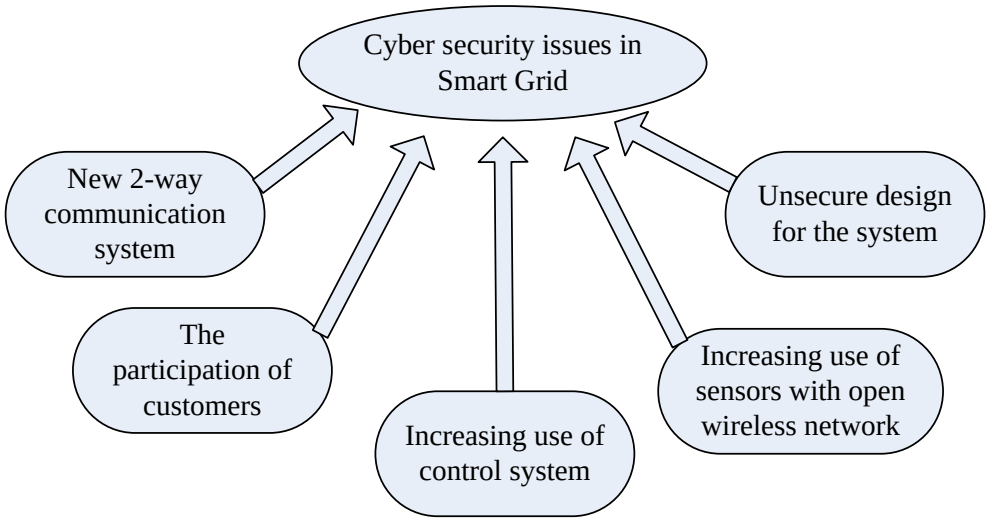

Figure. 1-1 The possible reasons for cyber security issues in smart grid

As a critical part of the modern power grid, the Supervisory Control and Data Acquisition (SCADA) system and Energy Management System (EMS) are adopting standard protocols and communication technologies to monitor and control the power system. Gradually, more and more smart devices and cyber technologies will be integrated into the power grid, and the cyber infrastructure will become a vital part of the entire cyber-physical power system. The increased utilization of smart grid technologies is promising to bring tremendous benefits to the power grid as well as the societal welfare. However, its associated cyber-vulnerability is becoming a pressing issue to the power grid. For example, the SCADA system with functions of transmitting measurements and commands between distributed devices and control centers is vulnerable to various cyberattacks [14]. As a key function in EMS for monitoring and estimating the real-time grid status, state estimation is also susceptible to cyberattacks. For example, false data injection [15] is a typical malicious cyberattacks against state estimation. The attackers could compromise the outcome of the

state estimation by intentionally changing some measurements of the power grid. This false data injection attack may successfully bypass the bad data detection mechanism without affecting the measurement residual. Once the attackers launch such attacks and manipulate the results of state estimation, the operators may make uneconomic, non-optimal or even harmful decision on power dispatch based on the false state estimation results

It is essential to understand what the security objectives and requirements are when people deal with the cyber security in energy supply and management. The guideline for cyber security of smart grid from the NIST can be listed as follows [14].

1. Availability. Availability of information refers to ensuring that the authorized parties are able to access the information when needed. The availability is very important for ensuring the smart grid security because a loss of availability will lead the disruption of access to some critical information, which may further undermine the power system operation.

2. Integrity. Integrity of information refers to protecting information from being modified by unauthorized parties. A loss of integrity is the unauthorized modification or destruction of information. It can further induce no-optimal or even incorrect decisions regarding power system operations and management.

3. Confidentiality. Confidentiality of information refers to protecting the information from disclosure to unauthorized parties. Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. It is particularly necessary to prevent unauthorized disclosure of information that is not open to the public and individuals [16].

As a complicated system, many aspects of the smart grid are vulnerable to the cyberattacks. The Advanced metering infrastructure (AMI) system is an essential system in the Smart Grid because it deploys communication networks to connect each customer's home-area network with utility companies, and consistently interacts with smart meters in home-area networks for scheduled energy management or demand response [17]. The AMI network is highly distributed in smart grid. At the same time, wireless networks are to be used for monitoring and communicating with these meters. However, the openness of the wireless communication medium could expose information exchange to attackers which could be used to compromise the data integrity and confidentiality. By eavesdropping on wireless communication channels, an attacker at a home-area network could possibly gain private information even if the information has been encrypted [11]. Similar to the Internet and data collection in sensor networks, conventional relay or man-in-the-middle attacks could possibly also be launched in the AMI network to inject malicious data during the communication process [18] [19]. What`s more, as a critical part of the smart grid, SCADA systems are vulnerable to cyberattacks. It generally consists of four parts [20]: field data interface device such as remote terminal units (RTUs), communication system, central master terminal units (MTUs), and human machine interface (HMI) software. The SCADA system monitors and controls the power transmission network in real-time through these critical parts. The control commands and access logs of the four parts are extremely important for power system operations. Any tampering or compromising on these data will damage the security and reliability of the system.

1.3 The Objective of Thesis

As a typical cyberattack against the power grid state estimation, the false data injection attack was studied in a number of literature in recent years. In [21] and [22], load redistribution and local load redistribution attack models are proposed respectively. These two kinds of attacks could cause the curtailment on some load buses by compromising the measurement data. In [23], the vulnerability of an unobservable false data injection attack on AC state estimation is analyzed. In [24], the impact of the false data injection attack on the power market is studied through a game-theoretic approach. In [25] a graphical method for cyber defense against the false data injection attack is investigated, and in [26] a novel sparse optimization method is proposed. In [27], the authors propose a typical false data injection attack termed unidentifiable attacks, which is different from the undetectable attack discussed in [21]-[26]. In the unidentifiable attacks, the bad data detector may detect some bad measurements, but it is unable to locate them because of the limitation of the identification algorithms such as the identification by elimination (IBE) algorithm. The detector may fail to identify the compromised data if these maliciously modified measurements are consistent. Compared with the undetected attack, fewer compromised measurements are needed in this type of attacks.

With the further development toward the envisioned smart grid, more information and communication technologies will be deployed in the power grid. If false data injection attacks occur in a frequent manner, negative impact will be brought to the power system reliability. Therefore, in this context, the false data injection attacks should be considered in the evaluation of the power grid reliability. In this thesis, two typical type false data injection attacks, the local load redistribution attack and unidentifiable attack, are

incorporated into the power system adequacy assessment, and its potential impact on the power system reliability is quantified and analyzed.

1.4 The Outline of Thesis

The remainder of this thesis is organized as follows. Chapter 2 introduces the background of the research field. Chapter 3 discusses the two false data injection attacks and proposes the scheme of adequacy evaluation with local load redistribution and unidentifiable attacks. Chapter 4 presents the case studies and simulation results. Chapter 5 draws the conclusion and presents the future work.

Chapter 2

Related Researches

In this chapter, the state estimation in power systems will be introduced. Also the false data injection attacks which may mislead the outcome of the state estimation will be discussed. The power system reliability concept will be studied in this chapter as well.

2.1 Power System State Estimation

System monitoring is very important for the system to ensure the reliable operation. Based on the measurements reading which are placed on the critical components of the power grid, the monitoring system can provide correct and useful information of the power grid. The main measurements may include the bus voltages, power injection measurements and power flow measurements in all the power system [28]. These measurements are transmitted to the SCADA system via the communication system which placed between the meters and the control center. Power systems are continuously monitored in order to maintain the operating conditions in a normal and secure state. State estimation function is used for this purpose. In order to identify the current operating state of the system, state estimators can help accurate and efficient monitoring the operation state of the system such as the transmission line load or bus load. They provide reliable data based on the real-time state of the system. Many operation of the system, such as contingencies analysis or power

dispatch, will be based on the accurate outcome of the state estimation. The state estimation typical including the following functions [29]:

- Topology processor: Gathers status data about the circuit breakers and switches, and configures the one-line diagram of the system.

- Observability analysis: Determines if a state estimation solution for the entire system can be obtained using the available set of measurements. Identifies the unobservable branches, and the observable islands in the system if any exist.

- State estimation solution: Determines the optimal estimate for the system state, which is composed of complex bus voltages in the entire power system, based on the network model and the gathered measurements from the system. Also provides the best estimates for all the line flows, loads, transformer taps, and generator outputs.

- Bad data processing: Detects the existence of gross errors in the measurement set. Identifies and eliminates bad measurements provided that there is enough redundancy in the measurement configuration.

- Parameter and structural error processing: Estimates various network parameters, such as transmission line model parameters, tap changing transformer parameters, shunt capacitor or reactor parameters. Detects structural errors in the network configuration and identifies the erroneous breaker status provided that there is enough measurement redundancy.

Thus, power system state estimator constitutes the core of the on-line security analysis function. It acts like a filter between the raw measurements received from the system and

all the application functions that require the most reliable data base of the current state of the system. A more clear definition of the state estimation of the power system can be given as following mathematical models [14]:

$$z = h(x) + e \tag{1}$$

where $z = (z_1, z_2, \cdots, z_m)^T$ denotes the meter measurements vector and m is the number of meter measurements. $x = (x_1, x_2, \cdots, x_n)^T$ is the state variables and n is the number of the state. Note that $m \geq n$, it can ensure the system observable. $h(x) = (h_1(x), h_2(x), \cdots, h_m(x))^T$ is the function of state variables x.

For state estimation using the DC power flow model, the relation between measurements and state variables can be represented by a linear regression model as follows [29]:

$$z = Hx + e \tag{2}$$

where *H* is an jacobian matrix of the system. Generally speaking, the measurement error vector *e* is assumed to Gaussian distribution with zero mean. The state estimation problem can be simply expressed as find the optimal state *x* to minimize the weighted least square of measurements error:

$$\text{minimize} \quad J(x) = r^T R^{-1} r \tag{3}$$

$$\text{s.t.} \quad r = z\text{-}HX \tag{4}$$

where *r* represents the estimated residual vector. *R* is diagonal matrix of the variances of the measurement errors. When meter error is assumed to be normally distributed with zero mean, the unique solution of the WLS estimate of state variable x is present as following matrix solution

$$\mathrm{x}(z) = (H^T R^{-1} H)^{-1} H^T R^{-1} z \tag{5}$$

where *R* is a diagonal matrix whose elements are reciprocals of the variances of the meter errors. It can be represent as below:

$$\mathrm{R} = \begin{bmatrix} \sigma_1^{-2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_m^{-2} \end{bmatrix} \tag{6}$$

where σ_i^{-2} denotes the variance of i-th meter.

2.2 False data injection attacks

As a typical cyberattack against the state estimation, false data injection attacks are first proposed by Liu.et [14]. It is assumed that there are *m* meters and *n* state variables in the power system. The relationship between the measurements vectors and the state variables can be represent by the Jacobian matrix H. Generally speak, the matrix H is determined by the topology information and the line impedances of the system. At the same time, it is assumed that the attackers have the access to gain the whole information of the matrix H and can inject malicious measurements to alter the meter readings. The model for the attack can be represented as follows:

$$z_a = z + a \tag{7}$$

where z_a denotes the vector of the malicious measurements. $z = (z_1, z_2, \cdots z_m)^T$ represents the original measurements and $a = (a_1, a_2, \cdots a_m)^T$ is the malicious data injected into the original measurements. The *i*th element a_i being nonzero means that the attacker compromises the ith meter and replaces the original measurements z_i with $z_i + a_i$.

The attacker can choose any nonzero arbitrary vector as the attack vector a, and then construct the malicious measurements vector as equation (7). The traditional bad measurement detection approach computes the 2-Norm of the measurement residual to check whether there exist bad measurements or not. It can be denoted as follows [30]:

$$\mathrm{r} = \ ||\mathrm{z} - H\hat{x}|| \tag{8}$$

where *r* denotes the measurements residual and $\hat{x}$ represents the estimated states.

However, such a detection approach can be bypassed if the attack vector a is a linear combination of the column vectors of jacobian matrix H if the original measurements z can pass the bad measurements detection algorithm. That can be represented as follows:

$$\begin{aligned} \hat{x}_a &= \ (H^T R H)^{-1} H^T R z_a \\ &= (H^T R H)^{-1} H^T R (z + a) \\ &= \hat{x} + (H^T R H)^{-1} H^T R a \end{aligned} \tag{9}$$

If a is a linear combination of the column vectors of H which means $a = Hc$, and c is an vector with arbitrary nonzero numbers. Then the 2-Norm of the measurements residual can be represented as:

$$\begin{aligned} \left||z_a - H\hat{x}_a|\right| &= ||z + a - H(\hat{x} + (H^T R H)^{-1} H^T R a)|| \\ &= ||z - H\hat{x} + (a - H(H^T R H)^{-1}) H^T R a|| \\ &= ||z - H\hat{x} + (Hc - H(H^T R H)^{-1}) H^T R H c|| \\ &= ||z - H\hat{x} + (Hc - Hc)|| \\ &= ||z - H\hat{x}|| \end{aligned} \tag{10}$$

From the equation (10), it can be referred that, if the original measurements can bypass the bad data detection algorithm, the malicious measurement which is constructed with the

manner mentioned above, it will also cannot be detected by the detector. Hence the injection error vector can be denoted as:

$$\hat{x}_a - \hat{x} = H(H^T R H)^{-1} H^T R a$$
$$= c \tag{11}$$

By launching the false data injection attacks, the attacker can manipulate the injected false data without being detected by the system. This will mislead the outcome of the state estimation which may lead to damage to the power system operation when considering the significance of the state estimation.

In recent years, a significant deal of research was focused on false data injection attacks. The main literatures can be divided into two category: the damage of the false data injection attacks and the defend approaches for this type cyberattacks. In [21], the load redistribution attack was developed, and immediate Load redistribution (LR) attack was modeled by a bilevel optimization problem and solved by Bender's decomposition with a restarting framework while the delayed LR attack was modeled by a trilevel optimization problem and solved by Karush–Kuhn–Tucker (KKT) method. It get the conclusion that with the false data injection attack, some curtailment will occur in some transmission lines if the system is operating close to the transmission line capacity limit. In [31], the false data injection attacks against the electricity market was studied. By injecting this type cyberattacks, the line congestion will be modified to be increasing or decreasing and the attackers can gain financial benefit from it. Also, another false data injection attacks against electricity market proposed by [32]. They construct the ramp induce attack against the real-time electricity market which is based on the look-ahead dispatch model. This ramp attack can withhold or withdraw the capacity of generators without being detected by the system.

This may result in more power supplying the excess demand which leads to higher electricity price inevitably.

On the other hand, some countermeasures against the false data injection attacks have been proposed in the existing research. In [33], the authors proposed a method to purposefully select meter measurements for protection, and these measurements are called the basic measurements. The protection scheme is costly in that the size of a set of basic measurements is the same as the number of unknown state variables in the state estimation problem, which could be up to several hundred in a large scale power system. In [28], the researchers proposed graphical methods to study defensive mechanisms against false data injection attacks on power system state estimation. Some measurements are secured to avoid being injected by the false data attack. This problem is characterized as a variant Steiner tree problem in a graph. And they also proposed both exact and reduced complexity approximation algorithms. In [23], the authors introduced the vulnerability analysis of state estimation when it is injected by false data injection attacks in the AC model. Considering most research about defending the false data injection attacks is focused on DC model, the authors proved the AC state estimation has the advantage in protecting the power system from such false data injection attacks.

2.3 Power System Reliability

Generally speaking, the concept of reliability indicates the ability of a system to perform its intended function, where past experiences help form reasonable estimates of its future performance [34]. According to the definition from North American Electric Reliability Council (NERC), power system reliability indicates the degree to which the performance of the elements of the electrical system results in electric power being

delivered to consumers within accepted standards and in the amount desired [35]. In other words, reliability indicates the ability of the power system to supply power with quantity and quality requirement to the customers.

Reliability is often measured by frequency, duration and extent of power system disturbances and outages. The disturbance could be any unplanned event which leads to an abnormal system condition. The outage can be described in terms of frequency, duration, and unmet load demand. The reliability of a power system is very significant for its operation, and any abnormal condition could lead to system damage. For example, the voltage disturbance could lead to a sudden and short-term reduction of the normal power supply. Load interruptions could lead to a long period of completely interrupted services. These factors may result in the malfunction of components in power grid.

In a power system, the main components consist of lines, generators, transformers and loads. The reliable function of each individual component as well as the dispatch strategy plays critical roles in ensuring the reliable power supply. Monte Carlo simulation is being widely applied to evaluate the power grid reliability. It generally consists of four major steps [36]:

1. Modeling the reliability characteristics of individual component and load demands in the power system.
2. Randomly sampling a system state.
3. Evaluating the system state obtained in step (2). The evaluation is usually achieved by an OPF analysis.
4. Calculating the reliability indices.

There is a set of indices which could indicate the overall reliability of the power system. According to the definitions from the Institute of Electrical and Electronics Engineers, the main reliability indices can be illustrated as follows [37]:

1. CAIFI (Customer Average Interruption Frequency Index) is the average number of interruptions for customers who experience interruptions during the year. It is calculated by dividing the total annual number of interruptions of power to customers by the total number of customers affected by interruptions during the year. This index gives the average frequency of sustained interruptions for customers who experience sustained interruptions.
2. CAIDI (Customer Average Interruption Duration Index) represents the average time required to restore service to the average customer per sustained interruption.
3. LOLE (Loss of Load Expectation), also referred to as Loss of Load Probability, forecasts the expected number of days in the year when the daily peak demand will exceed the available generating capacity. This number is obtained by calculating the probability of daily peak demand exceeding the available capacity for each day and adding these probabilities for all the days in the year.
4. RUS (Rural Utility Service) is used to determine the average outage hours for customers in rural areas. These customers may experience longer recovery periods from disturbances than other customers do because of the lower density of loads along rural feeders.

The objective of performing reliability evaluation is to derive suitable measures to quantify the overall system performance when some components are in failure states. Specifically, as a critical part of the power system, the generation reliability studies are very important. The indices used to measure generation reliability are probabilistic

estimates of the ability of a generation configuration to supply the load demand. The analytical approach for the generations are based on the loss of load and the frequency and duration. In this thesis, the following two type indices are used to model the reliability of the system.

A loss of load indicates the number of the system load exceeds the generation capacity. The overall probability that the generation capacity will not met the load demand is defined as the loss of load probability (LOLP). This LOLP can be calculated as [37]:

$$\text{LOLP} = \sum_j P[C_A = C_j] \cdot P[L > C_j] \tag{12}$$

Where C_A is the capacity of the generation. L is the load demand.

The expected energy not supplied (EENS) is another important index which indicates the reliability of the power system from a different perspective. It can be represented as follows:

$$\text{EENS} = \sum_k C_k F_k D_k \tag{13}$$

where C_k is the load curtailment of system state k; and F_k and D_k are the frequency and the duration of system state k.

Chapter 3

Problem Formulation

The proposed method for integrating false data injection attacks into the power system reliability will be studied in this chapter. Two specific false data injection attacks: local load redistribution attacks and unidentifiable attacks will be discussed in this chapter. Further, the procedure integrating these attacks into power system reliability evaluation will be proposed in this chapter.

3.1 Local load redistribution attacks

In [14], Liu et al. demonstrated that an attacker can inject false data into the power system state estimation without being detected if the attacker can obtain the whole information on the power grid. The basic principle of false data injection attack can be represented as follows:

$$z_a = Hx_a \tag{14}$$

where z_a denotes the attack vector of the measurements, x_a is the desired state variation vector, and H represents the Jacobian matrix of the power grid. Recently as a viable false data injection attack, load redistribution attack [21] is proposed based on the practical

condition where only load and line flow measurements can be attacked. An LR attack can be expressed as follows:

$$\sum_{l=1}^{N_l} \Delta L_l = 0 \tag{15}$$

$$\Delta PF = -SF \cdot KL \cdot \Delta L \tag{16}$$

$$-\tau L_l \leq \Delta L_l \leq \tau L_l \qquad \forall l \tag{17}$$

where ΔL_l is the attack on load demand measurement l; *SF* is shift factor matrix; *KL* is the bus-load matrix; τ is the limit of load attack magnitude. Equation (15) indicates the total load demand should be unchanged. Equation (16) implies that the power flow varies based on the power balance equation, and (17) indicates the upper and lower bounds of the load measurement attack magnitude.

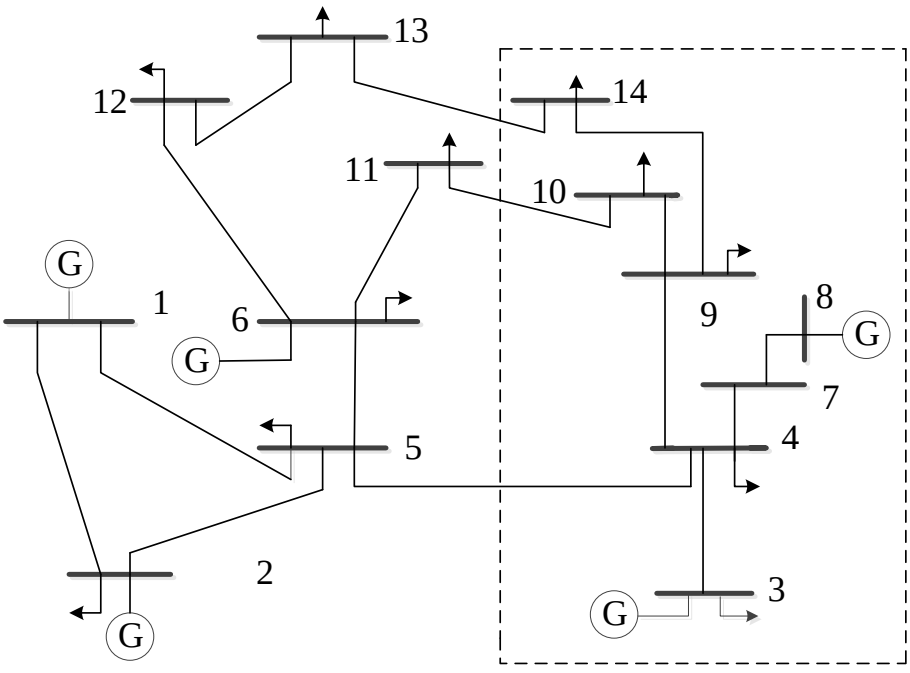

Fig.3-1 Local load redistribution attack scheme.

Local load redistribution attack [22] is developed from LR attack and it is found that the attacker can compromise the outcome of state estimation by just compromising the

measurements in a local region. The model for local LR attack can be mathematically represented as follows [22]:

$$B_a \Delta\theta_a = -KL_a \cdot \Delta L_a \tag{18}$$

$$\Delta\theta_i = \Delta\theta_j \quad i,j \in boundary\ of\ A \tag{19}$$

where ΔL_a is the load measurement variation at load bus in attack region A; B_a is susceptance matrix and KL_a is the bus-load matrix; $\Delta\theta_a$ is the variations of phase angles in attack region; and $\Delta\theta_i$ and $\Delta\theta_j$ denote the variations of the boundary in region A.

Fig. 3-1 depicts an example on how a local LR attack can be constructed. The power grid is decomposed into two interconnected regions: the local attack region A is circled by the dashed line and the rest of the system is the non-attack region N. Then the buses 4, 10 and 14 are boundary buses in attack region A. It is proven that if the false data injection vector ΔL_A ensures the changes on the voltage phase angles of all boundary buses in the attacking region A are the same (i.e., $\Delta\theta_4=\Delta\theta_{10}=\Delta\theta_{14}$), then the false data injection will not impact the power flows in the non-attacking region N. The fulfillment of this rule ensures the success of launching an LR attack as it is limited to the local region.

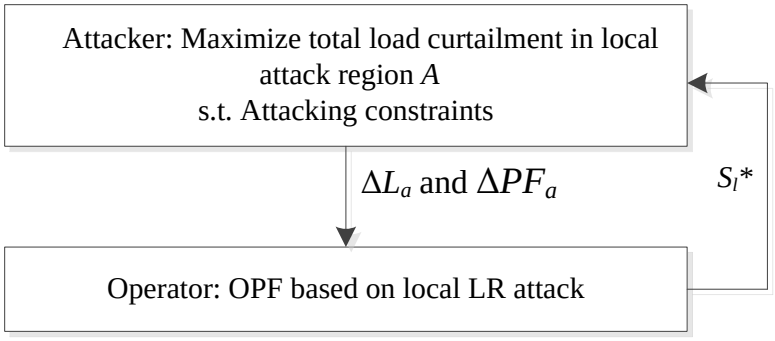

Fig.3-2 The bilevel model for the local LR attack

The attacker may aim to maximize the damage in term of load curtailment considering the remedial actions S_l taken by the power system operator to minimize the damage. In [21], a bilevel model is proposed to assess the LR attack. In this study, to achieve the biggest damage of the local LR attack, an improved bilevel optimization model is formulated for the attacker as shown in Fig. 3-2. It can be mathematically represented as follows:

$$\max_{\Delta L_a} \sum_l S_{l,a}^* \tag{20}$$

subject to:

$$\sum_l \Delta L_{l,a} = 0 \tag{21}$$

$$\Delta PF_a = -SF_a \cdot KL_a \cdot \Delta L_a \tag{22}$$

$$-\tau L_{l,a} \le \Delta L_{l,a} \le \tau L_{l,a} \tag{23}$$

$$B_a \Delta\theta_a = -KL_a \cdot \Delta L_a \tag{24}$$

$$\Delta\theta_i = \Delta\theta_j \quad i,j \in boundary\ of\ A \tag{25}$$

$$\{S^*\} = \arg\{\min \sum_l S_l\} \tag{26}$$

subject to:

$$\sum_g P_g = \sum_l (L_l - S_l) \tag{27}$$

$$PF = SF \cdot KP \cdot P - SF \cdot KL \cdot (L + \Delta L - S) \tag{28}$$

$$-PF_b^{max} \le PF_b \le PF_b^{max} \tag{29}$$

$$P_g^{min} \le P_g \le P_g^{max} \tag{30}$$

$$0 \le S_l \le L_l + \Delta L_l \tag{31}$$

where a represents the attack region; g and b indicate the index of the generator and branch, respectively; KP is the bus-generator matrix; PF is the line power flow; and S_l denotes the shedding of load l.

The attacker is represented by the upper-level problem (20)-(26). The upper-level objective function (20) is to maximize the system damage. Constraints (21)-(23) ensure the attack is a typical LR attack, and constraints (24)-(26) guarantee this LR attack just occurs in a local region of the system. The system operator is represented by an OPF model in the lower-level problem (27)-(31). The lower-level objective function (27) is to minimize the system damage, considering the constraints (28)-(31).

Compared to the LR attack against the whole network, the local LR attack features some advantages for avoiding the detection. Recently, some approaches are proposed to prevent the injected attack such as protecting some "basic measurements" to defend against the attack [26]. So, if an adversary just attacks a local region without being safeguarded, it will bypass these protected measurements and escape the detection. Further, the common method for detecting the bad data is developed based on the L2-norm algorithm. It calculates every measurement residual and compares it with a certain threshold. If the residual exceeds the threshold, the bad data will be detected. This implies that if more measurements are compromised by attackers, the probability of being detected by the control center will be higher. However, if attackers just launch a local region attack, the number of manipulated measurements will decrease and the probability of escaping from detection will inevitably increase. Therefore, attackers may choose a local region attack with the advantages of bypassing some protected measurements and lower probability of being detected. Over a long period of time, the power system's operational state varies with the failure and recovery of physical components. For a given system state, there might be

multiple suitable attacking regions and the attacker may compromise different regions with different probabilities, considering the consequence and the difficulty of the attack.

To incorporate the local LR attack into the adequacy assessment for a given power system state, there is a need to obtain the meaningful possible candidate local LR attack scenarios against different attack regions. To achieve this, the scheme of selecting meaningful attack regions is proposed in this study as depicted in Fig 3-3. The whole system is denoted as G, and G_{ij} is a subset of G indicating the jth scenario of the attack region with i edges. Generally speaking, every G_{ij} could be attacked. Therefore, the bilevel model is used to check whether it is a valid attack region which may cause load curtailment. For a meaningful subset G_{ij}, it should satisfy two conditions. First, it must ensure the changes on the voltage phase angles of all boundary buses in the attacking region are the same, which is described by equation (18) and (19). This condition will make the local LR attack will bypass the detector when just attacking on a local region. Second, it must ensure the attack will have a damage on the system which is evaluated by the curtailment. When the curtailment occurs in some states, it will impact the reliability of the power system.

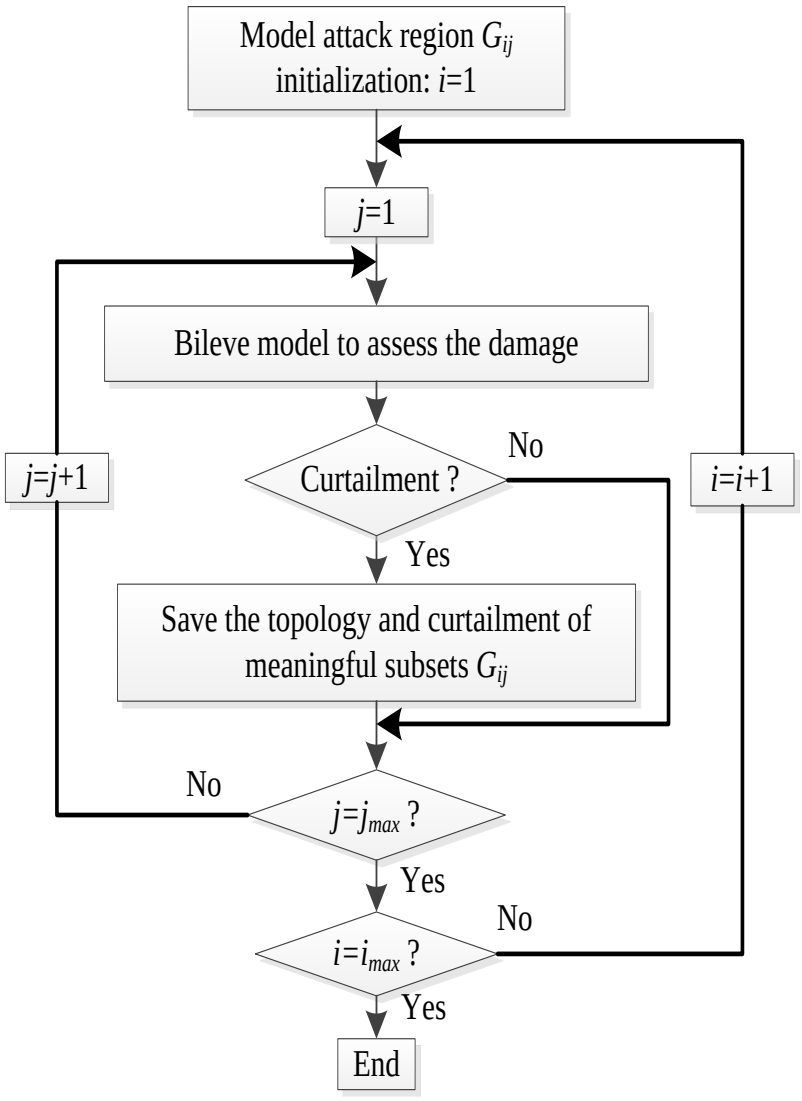

Fig. 3-3 The scheme of selecting meaningful attack regions

There are numerous lines and substations in a bulk power grid, and their criticalities are different although each component plays an important role. An effective metric for indicating the criticality of a line can be its betweenness considering the line power flow. The betweenness of a line in network is defined as the number of shortest paths going through it [38]. So we can calculate the normalized betweenness for each line as follows:

$$B_{nm} = \frac{N_{nm}}{\sum N_{ab}} \tag{32}$$

where B_{nm} is the normalized betweenness of the line from bus n to bus m, $\sum N_{ab}$ denotes the total number of the shortest paths from arbitrary bus a to bus b, and N_{nm} indicates the number of the shortest paths between arbitrary two buses which contain the line from bus n to bus m. For deciding the criticality of substations, the entropic degree [38] is applied in this study. Considering W_{nm} as the normalized weight of the line between bus n and bus m, the following relationship can be found [39]:

$$W_{nm} = B_{nm} / \sum B_{nm} \tag{33}$$

where B_{nm} indicates the betweenness of the line connected from bus n to m considering the actual power flow of each line. The entropic degree g_n of bus n can be defined using entropy as follows:

$$g_n = (1 - \sum W_{nm} \, log \, W_{nm}) \sum_m B_{nm} \tag{34}$$

Then, for a meaningful attack region G_{ij}, we can define the significance Q as the sum of the betweenness for each line and entropic degree for each bus. It is represented as follows:

$$Q = \sum B_{nm} + \sum g_n \tag{35}$$

Generally speaking, the more important a component is, the stronger its routine protection measure will be - thus it will be more difficult for the adversary to launch a successful attack against it. In this study, we assume that the probability of choosing an attack region features an inversely proportional relationship with the significance of the attack region. The probability K can be represented as follows:

$$K \propto \frac{1}{Q} \tag{36}$$

3.2 Unidentifiable attacks

The unidentifiable attack is first proposed in [27], which is different from the undetectable attack. In unidentifiable attacks, the state estimator installed in the control center can find that bad measurements exist. However, it cannot identify which meters have been attacked. For the unidentifiable attacks, it should satisfy two conditions: 1) The whole measurement vector is not consistent, which entails it cannot bypass the norm of residual test. This condition ensures that the state estimator is able to detect the existence of the bad data. 2) The measurements compromised by attackers should be consistent. These conditions guarantee that the identification algorithm embedded in the state estimator, such as the identification by elimination (IBE) algorithm, will fail to delete the compromised data because the malicious measurements are consistent. Outcomes of the state estimation obtained from these compromised data may mislead the power system operator, so non-optimal, uninformed, or even wrong decisions may be made.

The unidentifiable attack also demands fewer compromised measurements to construct a feasible attack compared with the undetected attack. It does not need to modify a large number of meters to make the whole measurements consistent. The attack only needs to bypass the identification algorithm embedded in the state estimator. Thus, the unidentifiable attack could be a preferred choice for an attacker with limited resources.

Since the control center and the power plant have direct communications, the attack on the generators' power output is in fact not viable. Thus the load redistribution attack is proposed [21]. It is known that when the power system operates close to their lines capacity limit, it is quite vulnerable to load redistribution attack. According to this characteristic, the scheme to construct the attack vector of unidentifiable load attack is proposed. Assume the

attacker is able to compromise at most R measurements, and r_b and r_{br} denote the numbers of compromised buses and branches, respectively. The goal of the attacker is to make the line flow exceed the transmission capacity with the least resource. To save the attack resource, it is assumed when one line is compromised, the bus that has heavier load at two ends of this line will be changed correspondingly. To ensure condition 2, $r_b + 2r_{br} \leq R$ should also be satisfied. In practice, the attacker will attempt to compromise the largest number of the line flows to maximize the variation of the power flow, so $r_{br} = \lfloor R/3 \rfloor$. This problem can be formulated as follows:

$$\max \sum_i^{r_{br}} \Delta PL_i \tag{37}$$

subject to:

$$\Delta PL_i = -SF \cdot KL_i \cdot \Delta D \quad i = 1,2,\cdots,r_{br} \tag{38}$$

$$\Delta D_j = \tau_j D_j \qquad j = 1,2,\cdots,r_b \tag{39}$$

$$\sum_{j=1}^{r_b} \Delta D_j \leq \sum_{g=1}^{N_g} g\_max_g - \sum_{d=1}^{N_d} D_d \tag{40}$$

$$0 \leq \tau_j \leq \tau \tag{41}$$

where ΔPL_i is the variation of line flow measurement and i indicates the i_{th} line close to the transmission capacity. ΔD_j represents the load measurement augment at bus j. N_g and N_d denote the total number of generators and the total number of load buses, respectively. g_max_g represents the maximal output of the generator g. τ is the limit of the load measurement variation. Equation (37) indicates the attacker aims to maximize the variation of the line. Equation (38) implies that the line r_{br} which is closer to the transmission capacity limit is compromised, and it also ensures the compromised measurements are consistent so as to avoid being deleted by the IBE algorithm in the state estimator. Formula (39) and (40)

guarantee that the variation of the load will not exceed the magnitude limit and the total generator capacity, respectively. Equation (41) represents the maximal magnitude of the variation on the load buses.

When these attacked measurements are transmitted to the control center, the norm residual testing algorithm will detect the presence of an attack. However, the state estimator cannot find the compromised measurements, and this is because at least two feasible measurement sets exist. Hence, an identification approach IBE is used to delete these bad data [29]. The IBE algorithm works as follows:

1. The bad data set $A = \emptyset$.
2. The measurements used for state estimation M={all meters}; M\A represents the complement set of A.
3. While the norm of residuals of $M \backslash A \geq \beta$
4. Put the meter which has the largest residual in M to set A;
5. Run SE with meter M\A;
6. Search the meter which has the largest residual;
7. End

Using this IBE approach, the state estimator is able to locate the bad data. However, as described in [29], by eliminating the measurement with the largest residual until the remaining ones are consistent cannot include all compromised meters. This is because of the drawback of these identification algorithms. Most identification algorithms in the state estimator only focus on the bad data caused by system errors. However, most system errors are always non-consistent. As a result, they will fail to identify the maliciously modified data when the measurements are compromised consistently.

When these 'identified' measurements pass the residual test, the control center will run the state estimation program based on these compromised data to obtain system states. In the state evaluation stage of reliability assessment, the operator's aim is to minimize the overall load curtailment based on the optimal power flow (OPF) procedure. These steps can be modeled as follows:

$$\text{Min } \sum_{d=1}^{N_d} S_d \tag{42}$$

subject to:

$$\mathrm{PL}_l = \mathrm{SF}_l[\cdot \mathrm{P} - \mathrm{KD}_d \cdot (\mathrm{D} - \mathrm{S})] \tag{43}$$

$$\sum_{g=1}^{N_g} P_g = \sum_{d=1}^{N_d} (D_d - S_d) \tag{44}$$

$$-PL_l^{max} \leq PL_l \leq PL_l^{max} \tag{45}$$

$$P_g^{min} \leq P_g \leq P_g^{max} \tag{46}$$

$$0 \leq S_d \leq D_d \tag{47}$$

where *l, d* and *g* denote the branch index, load index and generator index, respectively; N_g represents the total number of generators; PL_l is the power flow on the line *l; P* and *D* are the generator vector and the load vector, respectively; *SF* is the shift factor, which is determined by the system topology information; *KP* is the bus-generator incidence matrix; and *KD* is the bus-load incidence matrix. Objective function (42) aims to minimize the curtailment in the system. Equation (43) represents the power flow. Equation (44) implies the total generator output should be equal to the difference between the total load and the total curtailment. Inequality (45) indicates the line capacity limit. Inequality (46) is the

constraint for the generators output. Inequality (47) ensures the curtailment will not exceed the load on this bus.

3.3 Power System Reliability Modeling

In a power system, the main components include lines, generators, transformers and loads. The dependable operation of each individual component and the proper dispatch strategy play critical roles in ensuring the reliable power supply for offering the desired quality of services to customers. Monte Carlo simulation (MCS) is widely applied to model and assess the power grid reliability [36]. This approach mainly consists of three steps. 1) Randomly sample a system state based on the reliability model of individual components. 2) Assess the sampled state and usually an OPF procedure is applied. 3) If the sampling is sufficient, the desired power system reliability indices are calculated; or go back to step 1. The commonly used reliability indices include loss of load probability (LOLP) and expected energy not supplied (EENS), etc.

3.3.1 Power System Reliability Incorporating with Local LR attacks

It is critical to assess the frequency of local LR attacks which are fundamentally different from the physical failures. The frequency of cyberattack is determined by the behaviors of cyber attackers while the frequency of physical component failures is determined by the inherent physical characteristics of the respective components. Thus, it is reasonable to study the long-term human behavior pattern for modeling the frequency of the local LR attack.

Recently it was found in the area of human dynamics that for many kinds of human behaviors, for example message sending and movie rating, satisfy the power law distribution. Also some social behavior like wars or terrorism events can be described by power law as well [40]. The cyberattacks, as the typical behaviors of human, has many similarity with the war and terrorism. For example cyberattacks may from some terrorists or enemy organizations which want to damage the county`s security and economy. So it is very reasonable to describe the cyberattacks behavior by the power law distribution. The time intervals between two consecutive activities T and its associated probabilities P follow the power law distribution [41]:

$$P(T) \propto T^{-\tau} \tag{48}$$

A large number of human behaviors fall into two general pattern categories: $\tau = 1$ and $\tau = 1.5$ [42]. This power law distribution reveals that human behaviors share certain common characteristics. These two pattern categories are used in this study for simulating the time intervals between two local LR attacks.

The combination of the local LR attack and the statues of the physical components in the power system adequacy assessment is illustrated in Fig.3-4. There are three critical aspects in incorporating the local LR attack into the adequacy assessment: 1) when will the attack occur? 2) how will it impact the grid? and 3) how long will its impact last? In this study, the time interval described by the power law distribution is used to model how often the local LR attack occurs. The impact of each local LR attack is described in the bilevel model from (20)-(31). The duration of each local LR attack is assumed to be 15 minutes as the power grid operator could detect the local LR attack with periodic updates of the measurements.

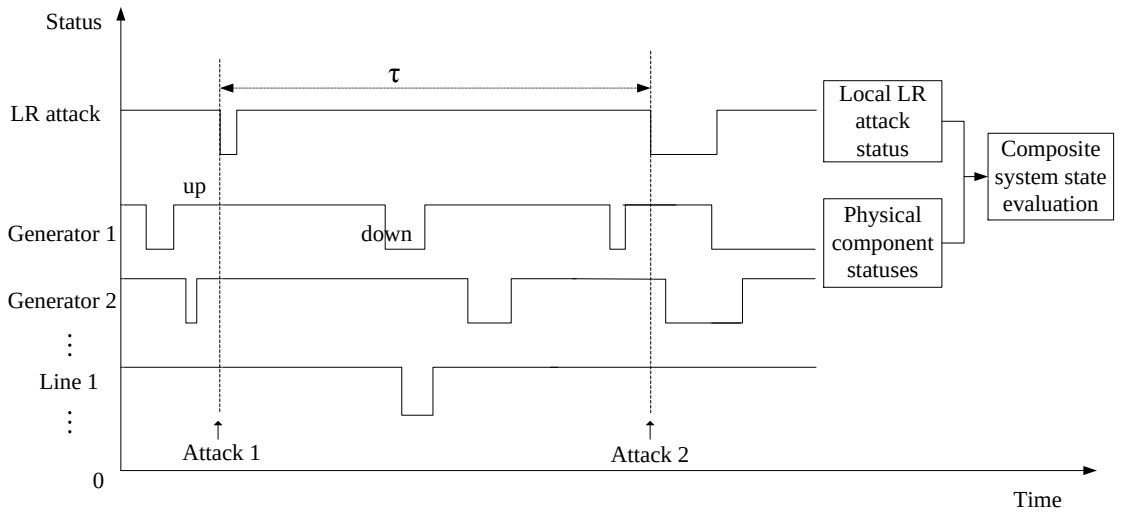

Fig.3-4 Consideration of local LR attack in adequacy assessment

In this study, an integral framework for power system adequacy evaluation considering the local LR attack is proposed based on sequential MCS as shown in Fig.3-5. The basic procedure is described as follows.

1. Model the working status of the system and the reliability of each generator, each line, etc. For example, the reliability of a generator can be modeled by the mean time to failure (MTTF) and mean time to repair (MTTR). The working status for each major physical component is modeled by a time sequence.

2. Generate a time sequence of local LR attack statuses based on the power law distribution describing the attack interval and its probabilities. Denote the status as "1" if there is a local LR attack and "0" if there is no attack. The simulation time interval in this study is 15 minutes.

3. Choose a composite system state - which is composed of the local LR attack status and the physical component statuses - in a time step based on the time sequences obtained in step 1 and step 2.

4. Check whether the local LR attack exists in the selected composite system state. If there is no local LR attack, go to step 7, otherwise go to step 5.

5. Select the attack region. For a physical system state, there are multiple suitable attack regions, and for each suitable attack region, the attack difficulty is different. The selection of the attack region is conducted considering its difficulty level – this implies that the more difficult an attack region is, the less likely this attack region will be selected.

6. Evaluate the composite power system state based on the physical status and the local LR attacks status. Then go to step 8.

7. Evaluate the system state based on OPF. DCOPF is used in this study.

8. Check whether the stopping criterion is satisfied. In this study, the maximum number of sampling years is 25 for ensuring the convergence of the reliability index. If the stopping criterion is satisfied, go to the next step; otherwise go to step 3.

9. Calculate the reliability index. In this study, the commonly used loss of load probability (LOLP) and the expected energy not supplied (EENS) are derived.

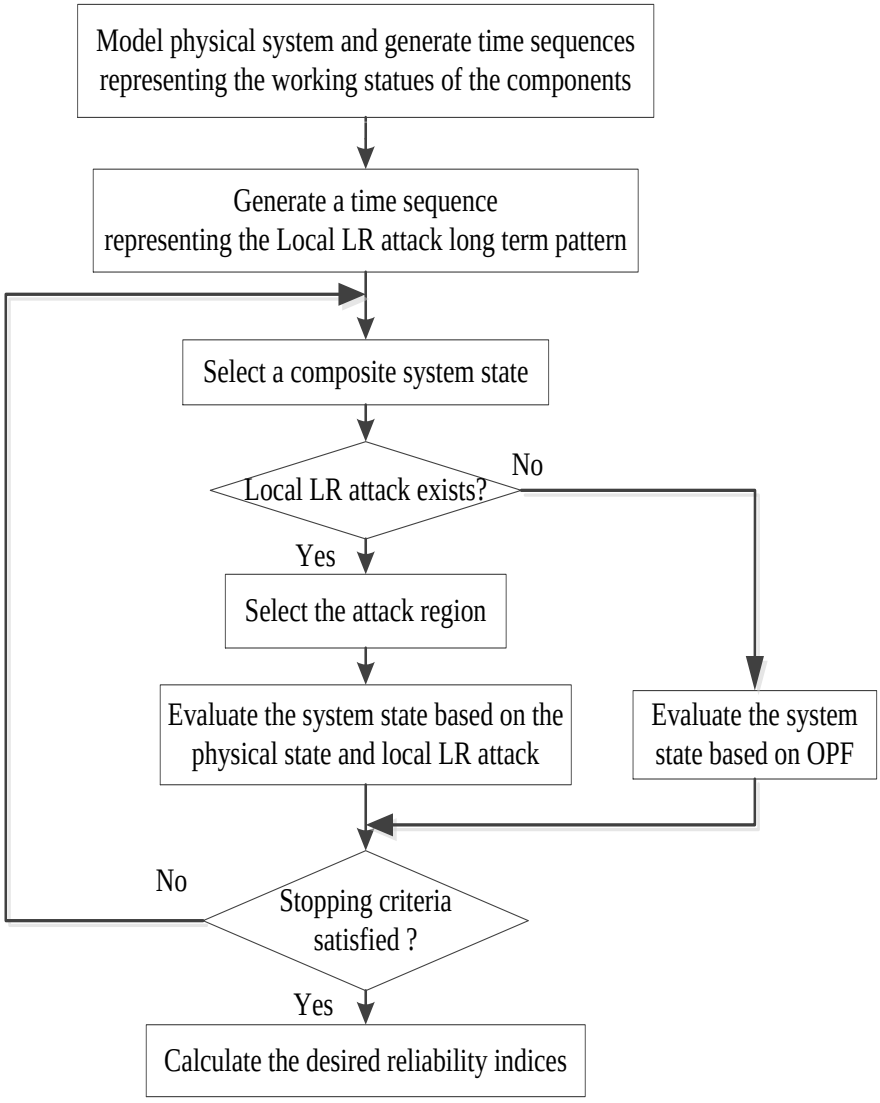

Fig. 3-5 Framework for power system adequacy assessment incorporating the local LR attack

3.3.2 Power System Reliability Incorporating with Unindentifiable attacks

In general, conventional power system reliability assessment abides by one critical assumption that the power system operator has a complete and accurate understating of the power system and thus he/she can always make an informed decision on power dispatch.

However, with the development of smart grid technologies applied to traditional power grids, cyberattacks might be a great challenge for this underlying assumption. The unidentifiable attack, which is a type of typical false data injection attacks, may compromise the outcome of the state estimation and mislead the power gird dispatch. In this case, it is not correct to estimate the power system status totally based on OPF. So it is critical to assess the impact of these kinds of attacks on the overall reliability of the power system.

The unidentifiable attack occurs randomly, and it is independent of the system component failures. It should be noted that the unidentifiable attack does not have a direct impact on the physical status of the line, generator, or load demand. However, it may compromise the outcome of state estimation, and might mislead the operator to take uninformed or wrong power dispatch actions (e.g., load shedding) which are actually not needed. Also, the attack can be characterized by the attack magnitude τ and mean time to repair (MTTR).

In unidentifiable attacks, the bad data detector may detect there exist some bad measurement which is different with the local LR attack, but it is unable to locate them because of the disadvantage of the identification algorithm, such as identification by elimination (IBE) algorithm. The detector may fail to erase the compromised data if these malicious measurements are consistent. Based on this attacking principle, the attacker will have no interest in attacking in a local region to bypass the protection. Because this type attack just need to satisfy that the measurements are compromised consistently. Hence, the protection level of the attacking buses and lines is not suit for unidentifiable attacks to calculate the frequency of the occurrence. Simply, we just assume this attack will occur several hundred times in one year. At the same time, the impact of the unidentifiable attacks

is modeled by (37)-(47). The duration of the unidentifiable attacks is assumed as 15 minutes as well.

The major steps of the MCS method for assessing the power system reliability incorporating unidentifiable attacks are illustrated in Fig. 3-6. The main procedures are introduced as follows.

1. Model the physical component and the attack process.
2. Obtain the system status. Randomly choose a physical system state based on the MCS sampling mechanism.
3. Check the sampled physical system state. If there is any physical failure, go to step 6. Otherwise go to the next step.
4. Evaluate the system state. System state evaluation is conducted based on the OPF analysis.
5. Check the existence of the unidentifiable attack. The existence of the attack sampled using MCS is determined by (49):

$$f_a = \begin{cases} 1 & s_a < p_a \\ 0 & s_a > p_a \end{cases} \tag{49}$$

where s_a denotes a random number derived from [0 1]; and p_a is the probability of the attack that can be executed successfully in one year, which is calculated by

$$p_a = \frac{n_a \times MTTR}{8760} \tag{50}$$

where n_a is the number of occurrences of attacks in one year; "1" indicates an attack is sampled, otherwise no attack is sampled; and MTTR refers to the duration of loss of load caused by an unidentifiable attack.

6. Select the attack level and obtain the attack consequence according to the model (37)-(47).
7. Update the reliability indices. In this step, the influences of the physical failure and cyberattacks are combined.
8. If the stopping criterion is not satisfied, go to step 2.
9. Calculate the system reliability indices.

Note that, in step 6 if no load curtailment is caused by physical failures, the original load demand will serve as the input for the possible unidentifiable attack. Otherwise, the remaining load demand is obtained as the input for the possible unidentifiable attacks.

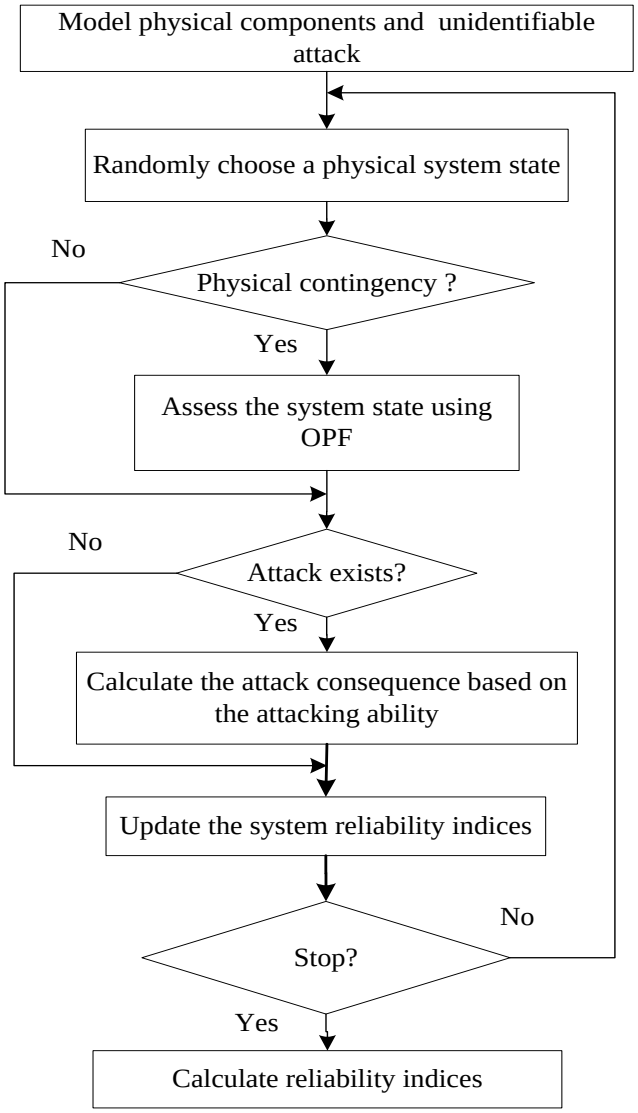

Fig. 3-6 Flowchart for power grid reliability assessment considering unidentifiable attacks

Chapter 4

Simulations Results and Analysis

4.1 System Parameters and Configuration

This section presents the case study based on a modified IEEE 14 bus system as shown in Fig. 4-1. The major configuration data and reliability parameters of generation and transmission are listed in Table 4.1 and Table 4.2, respectively. The transmission capacity of the first line is 160 MW, and the capacity of each of other lines is 115MW. All other configurations and parameters are obtained from the related files in the MATPOWER package [42].

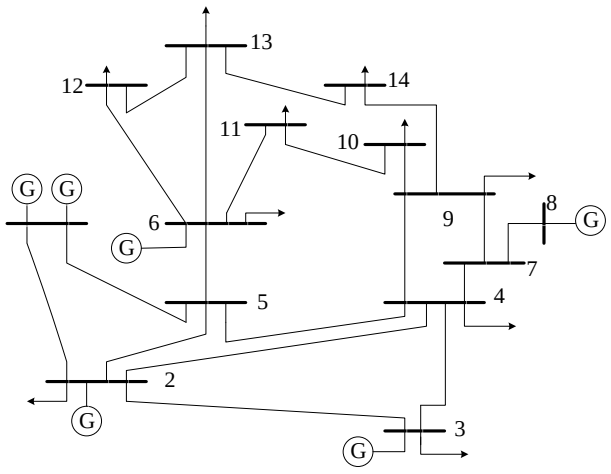

Fig.4-1 Modified IEEE 14 bus system

Table 4.1 Generation parameters

Number	Bus	Generation capacity (MW)	MTTF (h)	MTTR (h)
1	1	300	4990	10
2	2	50	1980	20
3	3	30	1950	50
4	6	50	1980	20
5	8	20	1950	50

Table 4.2 Transmission line parameters

Line	Outage rate (1/yr)	Outage duration (h)	Line	Outage rate (1/yr)	Outage duration (h)
1-2	0.08	8	6-11	0.18	10
1-5	0.1	10	6-12	0.2	10
2-3	0.1	10	6-13	0.08	10
2-4	0.15	10	7-8	0.02	30
2-5	0.15	10	7-9	0.02	25
3-4	0.15	10	9-10	0.02	25
4-5	0.02	30	9-14	0.02	20
4-7	0.18	10	10-11	0.15	11
4-9	0.2	10	12-13	0.08	11
5-6	0.15	18	13-14	0.4	11

4.2 Local Load Redistribution Attacks Incorporated into Power system Adequacy

To successfully launch a local LR attack, the attack region should be of an appropriate size. If the size of the attack region is too small, then too few measurements could be attacked and damage might not be made. If the size is too large, then such attacks could be easily detected. In this study, for simplicity the size of the attack region is measured by the number of lines in this attack region -- and we only consider the attack region with no fewer than 5 lines and no more than 8 lines. For most of the time period the power system operates without any contingency or with the first-order contingency. Partial results on load curtailment for the attack region are shown in Table 4.3, and these load curtailments are caused by the physical failure coupled with the local LR attack. The total number of valid attack regions and the range of load curtailment are given. From Table 4.3, we can find that when the attackers choose different local regions to attack, the curtailments may vary greatly. For example, if no contingency occurs in the system and the local LR attack is launched by the adversary, there are only 59 valid attack regions with the maximum load curtailment of 2.9 MW and the minimum load curtailment of 1.5 MW.

Table 4.3 Partial results for the first-order contingency

Failure component	Total valid attack regions	Maximum curtailment (MW)	Minimum curtailment (MW)
No failure	59	2.9	1.5
Line 1-2	171	13.3	1.5
Line 2-5	197	33.2	26.1
Line 4-5	104	18.5	16.1
Line 4-7	203	24.0	21.5
Line 5-6	31	18.5	12.1
Line 6-11	51	22.3	17.8
Line 9-10	37	12.1	10.7
Line 12-13	57	10.7	9.3
Generator 3	59	32.9	31.5
Generator 5	59	22.9	21.5

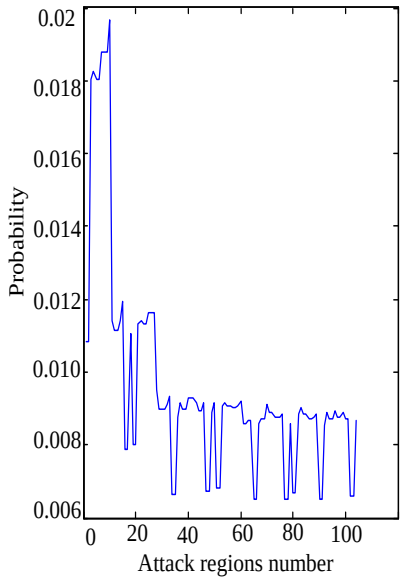

Fig. 4-2 Probabilities of attack regions for system state with line 4-5 failure

For each system state, there may be multiple candidate attack regions. Considering the difficulty associated with the attack region, the probability of choosing an attack region is different. For instance, there are 104 valid candidate attack regions for the system state with line 4-5 failure, the probability of each attack region is shown in Fig. 4-2 and these probabilities feature significant variations.

Here adequacy evaluation is performed considering the local LR attack and the results are shown in Table 4.4. It is concluded that the local LR attack has a significant impact on the power system reliability if occurring frequently in the future smart grid. And the attacker's behavior has a non-negligible influence on the power system adequacy. The power system adequacy decreases with the increasing number of attacks.

Table 4.4 Simulation outcome for system adequacy with local LR attack

Scenario	LOLP	EENS (MWh/yr)
No LR attack	0.063	13081
Attack interval following power law when $\boldsymbol{\tau = 1}$	0.098	14130
Attack interval following power law when $\boldsymbol{\tau = 1.5}$	0.153	14728

4.3 Unidentifiable Attacks Incorporated into Power system Adequacy

The unidentifiable attacks is different from the undetectable attack discussed in [21] and [22]. In the unidentifiable attacks, the bad data detector may detect some bad measurements, but it is unable to locate them because of the limitation of the identification algorithms such as the identification by elimination (IBE) algorithm. The detector may fail to identify the compromised data if these maliciously modified measurements are consistent. Compared with the undetectable attack, fewer compromised measurements are needed in this type of attacks. With the further development toward the envisioned smart grid, more information and communication technologies will be deployed in the power grid.

If unidentifiable attacks occur in a frequent manner, negative impact will be brought to the power system reliability.

In the IEEE14-bus system, if fully measured, it should have 54 measurements. Measurements 1-14 are the power injection measurements, 15-34 represent the power flow measurements at the sending end, and 35-54 are measurements for power flow at the receiving end. When an attacker constructs unidentifiable attacks with attack resources R=6, the lines working close to the line capacity will be the priority attack targets. This can cause the maximal variation of the line flow according to the model described in (2)-(6). The attacked measurements can be found in Table 4.5. In the first scenario, it is indicated that the measurements 3, 4, 17, 21, 37, and 41 are compromised by the attacker. When these maliciously modified data enter the state estimator, the residual test cannot pass because the whole system is not consistent. However, when these data go through the IBE algorithm, only the modified measurements 3 and 41 are deleted rather than all the compromised data. This is because the compromised measurements are consistent. This consistent manner will help the compromised measurements to successfully pass the IBE algorithm for modifying the outcome of state estimation.

Table 4.5 Compromised measurements and eliminated measurements

Scenarios	Compromised measurements by attacks	Deleted measurements by IBE
Attack resource R=6	3, 4, 17, 21, 37, 41	3, 41
Attack resource R=10	2, 3, 4, 9, 16, 17, 20, 21, 37, 41	3, 9, 17, 37

Table 4.6. Unidentifiable attack and undetectable attack

Scenarios	Unidentifiable attack	Undetectable attack
Attack magnitude	τ=0.7	τ=0.7
Attack resource	R=10	R=20
Attack results	Load shedding 2.21MW on bus 4	Load shedding 14.27MW on bus 3

From Table 4.5, it is found that the IBE method is not able to identify all the maliciously modified measurements if they are compromised in a consistent manner. Then these malicious measurements can lead to the wrong state estimation results. With these maliciously altered estimation results, the power grid could be at the risk of unnecessary load shedding due to the probable wrong power dispatch decision. Table 4.6 presents the results due to different attacks between the unidentifiable attack and the undetectable attack (local load redistribution attack [22]). In this table, it is indicated that more curtailments

occur in the face of the undetectable attack. However, the unidentifiable attack requires less attack resources compared with the undetectable attack. This is a compelling metric of the unidentifiable attack, especially for the attacker who possesses limited attack ability and resources.

Different attacks have different influences on the power system reliability. To assess the impact of the attacks, different factors are considered in this simulation. The simulation results are illustrated as follows. Fig. 4-3 shows the influence of the occurrence of the unidentifiable attack in one year on the power system reliability. It can be seen from Fig. 4-3 that the reliability of the power system is significantly impacted when more attacks are executed successfully in a long time period.

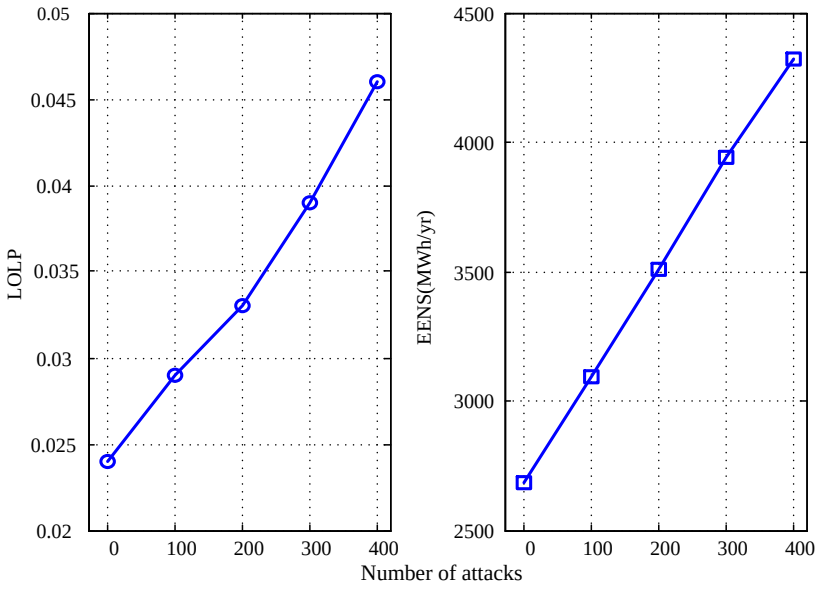

Fig. 4-3 Influence of the number of attacks on system reliability

Another parameter affecting the intensity of the attack is the magnitude limit of the attack vector. According to Fig. 4-4, it can be found when the attack magnitude varies from

0.5 to 0.9, the power system reliability indices LOLP and EENS both increase because of the unidentifiable attacks.

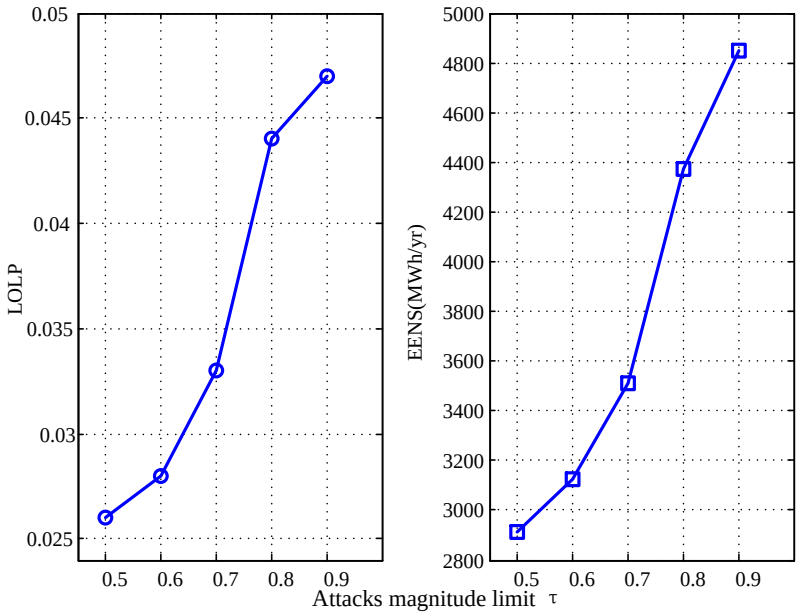

Fig. 4-4 Influence of the attacks magnitude limit on system reliability

The attack resource is also an important factor which will impact the attack results. Fig. 4-5 shows the simulation results for the average compromised measurements. Similar to the attack magnitude, when more measurements are compromised, larger LOLP and EENS values are resulted in correspondingly. Therefore, it is very important to enforce the protection of measurement meters in electric power systems

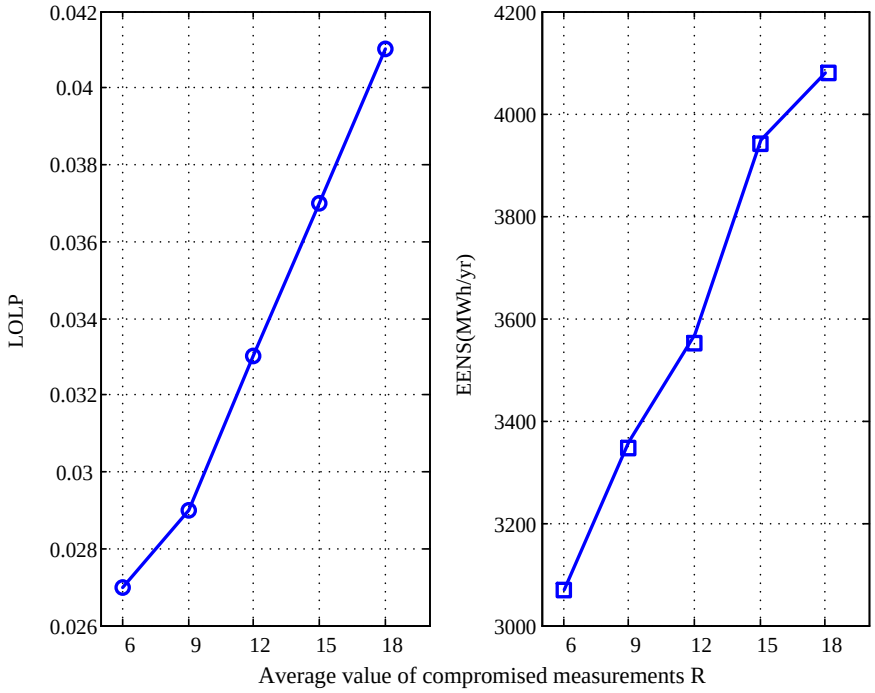

Fig. 4-5 Influence of compromised measurements on power system reliability

Chapter 5

Conclusions and Future Work

5.1 Conclusions

In this study, first an integrated procedure for quantifying the influence of local LR attack on power supply adequacy is proposed. The occurrence of the local LR attack in a long period of time is modeled by the power law distribution. And for major system states, the valid attack regions are counted and the probability of choosing the attack region is modeled based on the difficulty of the attack region. The consequence of each local LR attack scenario is modeled as a bilevel optimization problem. The results show the local LR attack has a significant impact on the power system reliability if occurring frequently.

Then, an improved procedure for evaluating the influence of unidentifiable attacks on power supply reliability is proposed. Both physical failures and unidentifiable attacks are considered in the power system reliability assessment. Also, several factors which may impact the attack outcomes are investigated including the frequency of the occurrence of the attacks, the attack magnitude and the attack resource. Simulations are conducted based on the modified IEEE 14-bus system and various attack-related results are obtained. It is concluded that the increase of the attack frequency, the attack resource and the attack magnitude will lead to the weakened overall power system reliability.

5.2 Future Work

For the future research, there are several directions that can be further explored based on the features of false data injection attacks:

- The current attack model will be improved by incorporating more factors which may impact the outcome of cyberattacks.
- Another improvement can be focused on the countermeasure development against the false data injection attacks such as undetectable attacks and unidentifiable attacks.
- Considering the function of sate estimation, the influence of false data injection attacks on power markets could be investigated in a systematic manner.

References

1. U.S. Department of Energy. (2008). *The Smart Grid: An Introduction*. Available: http://www.oe.energy.gov/SmartGridIntroduction.htm,
2. X. Fang, S. Misra, D. Yang. *Smart Grid – The new and Improved Power Grid: A Survey*. IEEE Communication Surveys & Tutorials, vol. 14, no. 4, (p. 944-980) 2012.
3. Office of Electricity Delivery and Energy Reliability, ″Smart grid,″ Online: http://www.oe.energy.gov/ smartgrid.htm, Accessed: August 2009.
4. R. Hassan, G, Radman. Survey on Smart Grid. IEEE Southeastcon, pages 210-213, 2010.
5. M. L. Tuballa, M. L. Abundo. *A Review of the Development of Smart Grid Technoloyies* Renewable and Sustainable Energy Reviews 59 (2016) 710-725.
6. J. Gao, Y. Xiao, J. Liu, W. Liang, C. Chen. *A survey of communication network smart grids*. Future Generation Computer System 2012; no.28 pp: 391–404.
7. R.E. Brown, *″Impact of Smart Grid on Distribution System Design,″* IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Page(s):1 – 4, July 2008.
8. Office of the National Coordinator for Smart Grid Interoperability , *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Available: http://www.nist.gov/public_affairs/.../smartgrid_interoperability_final.pdf.

9. J.A. Monoh, *" Smart grid design for efficient and flexible power networks operation and control*, *"* IEEE/PES Power Systems Conference and Exposition, PES '09, Page(s):1 – 8, March 2009.
10. T.-I. Choi, K.Y. Lee, D.R. Lee, J.K. Ahn, *Communication system for distribution automation using CDMA*, IEEE Transactions on Power Delivery 23 (2008) 650–656.
11. H. Sui, H. Wang, M.-S. Lu, W.-J. Lee, *An AMI system for the deregulated electricity markets*, IEEE Transactions on Industry Applications 45 (6) (2009) 2104–2108.
12. W. Wang, Z. Lu, *Cyber security in the smart Grid: Survey and Challenges, Computer Networks* 57 (2013) 1344-1371.
13. Pitchengine, The "smarter" the Smart Grid, the Greater Potential for security issues. Available:http://new.pitchengine.com/pitches/cea17e32-9ea8-4e3f-8b53-79f27d02f0ce.
14. NIST, *Guidelines for Smart Grid Cyber Security*: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NISTIR 7628," 2010. [Online]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html.
15. 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.
16. P. McDaniel and S. McLaughlin, *Security and Privacy Challenges in the Smart Grid*," IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5054916.
17. Bennett, C. & Highfill, D. (2008). *Networking AMI Smart Meters*. Energy 2030 Conference, 2008. ENERGY 2008. [

18. G.N. Ericsson, *Cyber security and power system communication –essential parts of a smart grid infrastructure*, IEEE Transactions on Power Delivery 25 (2010) 1501–1507.
19. M. LeMay, R. Nelli, G. Gross, C.A. Gunter, *An integrated architecture for demand response communications and control*, in: Proc. of 41th Hawaii International Conference on System Sciences (HICSS' 08), 2008.
20. Y. Yan, Y. Qian, H. Sharif, D. Tipper, *A survey on cyber security for smart grid communications*, IEEE Communications Surveys and Tutorials 14 (2012) 998–1010.
21. 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.
22. 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.
23. G. Hug and J. A.Giampapa, "*Vulnerability Assessment of AC state Estimation With Respect to False Data Injection Cyber-Attacks*," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1362–1370, Jul. 2012.
24. M. Esmalifalak, G. Shi, Z. Han and L.Y. 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.
25. S. Bi and Y. J. Zhang, "*Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation*," IEEE Trans. Smart Grid, vol. 5, no. 3, pp. 1216–1227, May 2014.
26. L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "*Detecting False Data Injection Attacks on Power Grid by Sparse Optimization*," IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 612–621, Mar. 2014.

27. Z. R. Qin, Q. Li and M. C. Chuah, "*Defending against Unidentifiable attacks in Electric Power Grids*," IEEE Trans. on Parallel and Distributed System, vol. 24, no. 10, pp. 1961–1971, Oct. 2013.
28. H.J. Zhou, C.X. Guo, J. Qin, *Efficient application of GPRS and CDMA networks in SCADA system*, in: Proc. of IEEE power and Energy Society General Meeting (PES '10), 2010.
29. A. Abur and A. Gómez Expósito, *Power System State Estimation: Theory and Implementation*. New York: Marcel Dekker, 2004.
30. E. N. Asada, A. V. Garcia, and, R. Romero, *Identifying multiple interacting bad data in power system state estimation*. In Proceedings of the IEEE Power Engineering Society General Meeting. IEEE, Los Alamitos, CA, pp 571–577, 2005.
31. 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.
32. D. H. Choi and L. Xie "*Ramp-Induced Data attacks on Look-Ahead Dispatch in Real-Time power markets*," IEEE Transsactions on Smart Grid, vol. 4, no. 3, Sept, 2012.
33. R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "*Detecting false data injection attacks on DC state estimation*," in CPSWEEK 2010.
34. J. Osborn and C. Kawann. Reliability of the U.S Electricity System; Recent Trends and Current Issues. LBNL-47043.
35. Cibulka, Lloyd. "*Defining and managing power quality and reliability*." www.utilityautomation.com. (April): 17-21. 2000.
36. R. Billinton and W. Li, Reliability Assessment of Electric Power Systems using Monte Carlo Methods. New York; London: Plenum, 1994.

37. J. F. Prada, *The Value of Reliability in Power Systems – Pricing Operating Reserves*. Energy Laboratory of MIT EL 99-005 WP. 1999.

38. R. Albert, I. Albert, and G. Nakarado, "*Structural vulnerability of the North American power grid*," Phys. Rev. E, vol. 69, no. 2, p. 025103, Feb. 2004.

39. E. Bompard, R. Napoli, and F. Xue, "*Analysis of structural vulnerabilities in power transmission grids*," Int. J. Crit. Infrastruct. Prot., vol. 2, no. 1–2, pp. 5–12, May 2009.

40. 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

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

42. MATPOWER, A MATLAB Power System Simulation Package [Online]. Available: http://www.pserc.cornell.edu/matpower/.