ATTACK AND DEFEND MECHANISMS FOR STATE ESTIMATION IN SMART GRID

A Dissertation
Presented to
the Faculty of the Electrical and Computer Engineering Department
University of Houston

in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in Electrical Engineering

by
Mohammad Esmalifalak
December 2013

ATTACK AND DEFEND MECHANISMS FOR STATE ESTIMATION IN SMART GRID

Mohammad Esmalifalak

Approved:

Chair of the Committee
Dr. Zhu Han, Associate Professor
Electrical and Computer Engineering

Committee Members:

Dr. Haluk Ogmen, Professor
Electrical and Computer Engineering

Dr. Rong Zheng, Associate Professor
Computer Science

Dr. Amin Khodaei, Assistant Professor
Electrical and Computer Engineering

Dr. Le Xie, Assistant Professor
Electrical and Computer Engineering
Texas A&M University, College Station, TX

Dr. Suresh K. Khator, Associate Dean,
Cullen College of Engineering

Dr. Badrinath Roysam, Professor and Chairman,
Electrical and Computer Engineering

Acknowledgements

First, I would like to express appreciation to my advisor, Dr. Zhu Han, for his guidance, valuable advice, and patient support during my entire course of studies at University of Houston. His profound academic knowledge and illuminating comments about my research were very valuable and helpful, not only to my doctoral study, but also to my future research and work.

Besides my advisor, I would like to thank the rest of my dissertation committee: Professor Haluk Ogmen, Professor Rong Zheng, Professor Amin Khodaei, and Professor Le Xie for their precious time and support. My appreciation also goes to my colleagues (Nam Nguyen, Najmeh Forouzandeh Mehr, Lanchao Liu, Yanrun Zhang, Zhou Yuan, and Yi Huang), who have provided me the perfect working environment.

I had the pleasure to meet wonderful friends like the Seifert family, Green family and my best friend, Matthew Albin, and his wife Jaclyn Albin. They were my second family in the US and lonely Houston days would have been unbearable without them.

Finally, I would like to thank my mother, father, brother and sister for their encouragement, patience, and love. They are always my best friends who never leave.

ATTACK AND DEFEND MECHANISMS FOR STATE ESTIMATION IN SMART GRID

An Abstract
of a
Dissertation
Presented to
the Faculty of the Electrical and Computer Engineering Department
University of Houston

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in Electrical Engineering

by
Mohammad Esmalifalak
December 2013

Abstract

Aging power industries together with an increase in the demand from industrial and residential customers are the main incentive for policy makers to define a road map to the next generation power system called the smart grid. Changing the traditional structure of power systems and integrating communication devices are beneficial for better monitoring and decision making by the system operators, but at the same time it increases the risk of cyber attacks. Power system blackout in 2003 created serious problems for customers in the eastern US and Canada. Although different investigations report reasons other than cyber attack for the blackout, many researchers believe a similar tragedy could happen with targeted cyber attacks. Later in 2007, researchers at the Idaho National Lab tried to attack a synchronous generator. The attack was successful and the generator was self-destroyed in a couple of minutes. This attack alarmed cyber-security decision makers, motivating them to define a critical infrastructure that is vulnerable to cyber-attack. An example of this vulnerability is the current bad data detection routine in state estimation, which is not able to detect a certain type of cyber attack called *stealth attack*. Stealth attacks are able to manipulate the state estimation results in order to take economical advantages or make technical problems for power grid.

In this dissertation, we analyze the cyber attack against state estimation, from both the attacker and defender points of views. We first review the structure of the electricity market, and then we present the way that the attacker alters the congestion in the ex–post market (in the desired direction) and makes financial profits. We investigate the case that attackers without prior knowledge of the power grid topology, try to make inferences through phasor observations. The inferred structural information is used to launch stealth attacks. This attack is formulated to change the price of electricity in the real-time market.

Second, we look at the false data injection from the defender point of view. Because of a huge number of measurements in the network, attacking and defending all measure-

ments are impossible for the attacker and defender, respectively. This situation is modeled as a zero-sum game between the attacker and the defender, and we describe how the interest of one party (attacker or defender) can influence the other's interest. The results of this game defines the proportion of times that the attacker and defender will attack and defend different measurements, respectively.

Finally, we illustrate how the normal operations of power networks can be statistically distinguished from the case under stealthy attacks. We first propose two machine learning based techniques for stealthy attack detection. The first method utilizes the supervised learning over labeled data and trains a support vector machine. The second method requires no labeled outputs for training data and detects deviation in the measurements. In both methods, principle component analysis is used to reduce the dimensionality of the data to be processed, which leads to lower computational complexities.

Table of Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction and Background

1.1 Overview

Recently, power systems are becoming more and more sophisticated in the structure and configuration because of the increasing electricity demand and the limited energy resources. In regulated power grids, a transmission system was commonly used to carry power from few central generating units to a large number of customers. Uncompetitive generation of electricity was the main drawback of the regulated environment in which having access to cheap generation was very limited to consumers all over the network. The right of having access to the transmission network for any entity that does not own transmission, is issued in the Energy Power Act by the Federal Energy Regulatory Commission (FERC) [2]. The main purpose of having open access to the transmission network, was to create a competitive market in which consumers were able to purchase their energy from cheap generating units. It also made the smaller generation units (distributed generation (DG)) more popular among the electricity suppliers [3, 4][1].

Today's power industry has integrated different new technologies and has been expanded in different levels (generation, transmission, and distribution). Meeting all technical and economical requirements in this complex system is becoming more and more sophisticated and almost all researchers in the power area believe that there is no unique solution to this challenge. Facing most of these challenges needs essential changes in operation and expansion of the power grid. The trend of these changes, is stimulated by the introduction of new-generation of the electricity grid which is also known as the smart grid. Smart grid uses bidirectional flows of the electricity and information to deliver power in more efficient ways responding to wide ranging conditions and events [5–10] (Fig. 1.1).

[1] These units need less starting time and are mainly used in peak consumption hours.

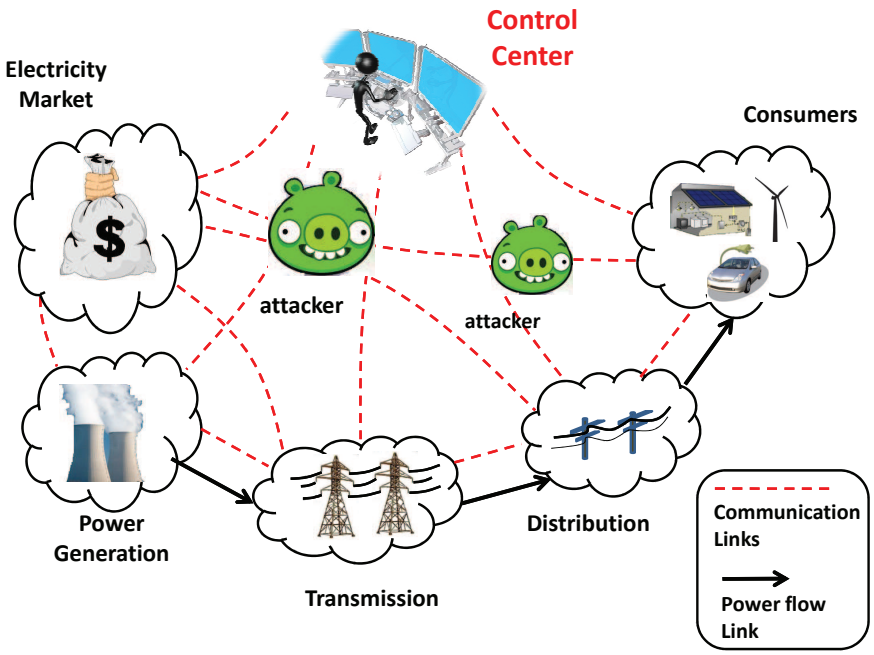


Figure 1.1 Flow of energy and data between different parts of smart grids.

Integration of renewable energies is another goal in the smart grid road map which improves the environmental requirements in power generation [11–15]. The amount of power generation in the renewable resources depends on the environmental situations, so their exploitation increases the intermittency of generation in the power network. Meeting demand in this intermittent situation is a challenging problem and mainly is studied in two directions, one group of researchers try to improve the prediction of intermittency in renewable resources by developing precise models [16–19]. Other group of researchers try to find the optimal way of integrating renewable recourses. The common goal of these studies is to maximize the integration of renewable resources without violating security constraints [20–22].

Indeed transition from conventional power grid to smart grid is happening in different parts of the power network. In generation level using clean and renewable energies is one of the main priorities [11–15]. Transmission system suffers from the centralized and

local observation of the network and main effort is focused on designing of a large distributed computing platform to overcome this deficiency [5–10]. Smart metering is another concept which tries to give an economical feedback to small and medium sized costumers of electricity in the distribution level [23–25]. These costumers traditionally have not been given the appropriate incentives to manage their consumption.

Online monitoring of smart grid is important for control centers in different decision making processes. State estimation (SE) is a key function in building real-time models of electricity networks in Energy Management Centers (EMCs) [26]. State estimators provide precise and efficient observations of operational constraints to identify the current operating state of the system in quantities such as transmission line loadings or bus voltage magnitudes. Accuracy of state estimation can be affected by bad data during the measuring process. Measurements may contain errors due to the various reasons such as random errors, incorrect topology information and injection of bad data by attackers. By integrating more advanced cyber technologies into the energy management system (EMS), cyber-attacks can cause major technical problems such as blackouts in power systems[2]. The attacks also can be designed to the attacker's financial benefit at the expense of the general consumer's net cost of electricity [28, 29].

1.2 Literature Review

Due to the importance of the smart grid studies, some surveys have classified the different aspects of smart grids [30–32]. In [30] the authors explore three major systems, namely the smart infrastructure system, the smart management system, and the smart protection system and also propose possible future directions in each system. In [31], a survey is designed to define a smart distribution system as well as to study the implications of the smart grid initiative on distribution engineering. In [32] relevant approaches are inves-

[2]Aurora attack involves a cyber attack against breakers in a generating unit. This experiment shows the abilities of cyber attackers in taking control over breakers and consequently, it reveals the technical problems of this attack for the power grid [27].

tigated to give concrete recommendations for smart grid standards, which try to identify standardization in the context of smart grids. National Institute of Standards and Technology (NIST) in [33], explains anticipated benefits and requirements of smart grid.

Some researches have been done over cyber security for smart grid [28, 29, 34–46]. In [40], the authors discuss key security technologies for a smart grid system, including public key infrastructures and trusted computing. Reliable and secure state estimation in smart grid from communication capacity requirement point of view is analyzed in [41]. In [42], a new criterion of reliable strategies for defending power systems is derived and two allocation algorithms have been developed to seek reliable strategies for two types of defense tasks. [38] surveys malicious attacks in three different categories based on the smart grid security objectives,

- *Attacks targeting availability:* Attackers try to delay, block or corrupt the communication in the smart grid (also called as denial-of-service attacks) [34–37]. [34] uses experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on a power substation network. Most of SCADA systems use DNP3 protocol to communicate the measurement values to the control center. [35] investigates the attack by implementing the attack in DNP3 Controlled SCADA Systems. Intrusion detection system (IDS) is an effective mechanism in detection of the malicious attack, [36] proposes an IDS to oppose the threats to an IEC61850-automated substation. Authors in [37] define a path identification mechanism to defend against distributed denial of service attacks.

- *Attacks targeting integrity:* Attacker attempts to illegally disrupt the data exchange [28, 29, 39, 43–49]. In [39], an undetectable attack by bad data detectors (BDD) is first introduced, where the attacker knows the state estimation Jacobian matrix (H) and defines an undetectable attack using this matrix. [28, 29, 43] investigate the economical effect of attack against state estimation in the power networks. [44] uses

independent component analysis (ICA), and inserts an undetectable attack even when Jacobian matrix (H) is unknown for the attackers. [45, 49] looks at the bad data injection problem from both attacker and defender point of views at the same time and describes how the interest of one party (attacker or defender) can influence the other's interest. Since there are many measurement devices in power systems, it is not reasonable to assume that all devices can be made encrypted overnight so [46] defines a security measure tailored to quantify how hard attacks are to perform, and describe an efficient algorithm to compute it. [47, 48] use the intrinsic low rank structure of temporal states of power grid as well as sparse nature of malicious attacks, to detect false data injection in state estimation.

- *Attacks targeting confidentiality:* Attacker tries to get unauthorized information from network resources [50–52]. While cryptography is broadly used to secure the communication links, [50] provides a simple security protocol against a wiretapping attack based on the network topology. The channel capacity requirement that ensures negligible information leakage to the eavesdropper is studied in [51] from the information theoretic perspective. Sharing data to ensure network reliability is beneficial to all remote terminal units(RTO's) but at the same time withholding data could be profitable for some of them. [52] investigates this competitive situation between RTOs in distributed state estimation.

Game theory is a mathematical framework for studying complex interactions among the independent rational entities. Psychology, economics, politics, and communication systems are the examples that game theory have been used successfully [53, 54]. The proliferation of advanced technologies and services in smart grid systems implies that disciplines such as game theory will naturally have an outstanding role in the design and analysis of smart grids [55]. The heterogeneous nature of the smart grid[3] and the need for low-

[3]Smart grid typically composed of a variety of networks such as micro-grids, smart meters, appliances, and others. Each of these networks have different capabilities and may follow different objectives.

complexity distributed algorithms for distributed operation of the smart grid nodes, are the examples that elucidate the application of the game theory in the smart grid studies.

Some applications of game theory in smart grids have been studied in [56–59]. In [56], the authors present a method for evaluating a fully automated electric grid in real time and finding potential problem areas or weak points within the electric grid by using the game theory. In [57], the authors propose a consumption scheduling mechanism for home and neighborhood area load demand management in smart grid using integer linear programming (ILP) and game theory. [58] is a survey about some of game theory-based applications to solve different problems in smart grid. In [59] the authors model and analyze the interactions between the retailer and electricity customers as a four-stage Stackelberg game.

Demand-side management (DSM), is another topic in smart grid which is recently considered by researchers. As a key component of smart grid emerging paradigm, the demand response helps reducing the electricity demand and shaving the peak demand, as well as, adjusts the controllable load to compensate power fluctuations. Utility companies and consumers are the main involved entities in demand–side management which may have different interest in some cases. Game theoretic approaches can model the interactions between these two entities and increase their welfare. For example costumers will increase their welfare with shifting their loads to the off–peak hours and this shift a) will delay the need for expansion of power generation, b) will increase the safety margin of the operation in peak hours (increasing welfare for utilities).

In [60] an intelligent management system is designed based on the objective of orderly consumption and demand-side management, under the circumstances of China's smart grid construction. An Intelligent Metering/Trading/Billing System (ITMBS) with its implementation on DSM is analyzed by [61]. [62] is a research on an autonomous and distributed demand-side energy management system among different users. Also there are

some papers that have focused on the modeling of specific appliances. For instance, [63] and [64] consider the electricity load control with thermal mass in buildings; [65] considers the coordination of charging PHEV with other electric appliances.

Microgrids are small-scale and low voltage supply networks which recently has been noticed in smart grids. These units are designed to supply electrical and heat loads for small consumers, such as academic or public communities, and manufacturing companies [66]. Microgrids can be separated from the main grid in contingencies and should provide electricity for their consumers with acceptable quality. Microgrids face several challenges in the real-time power management and control systems. Some of these challenges can be addressed by the optimization problems with different objectives such as, power demands, fuel consumption, environmental emissions, costs, dispatchable loads, etc. [67].

1.3 State Estimation

State estimation was first introduced by Fred Schweppe to identify the current operating state of the power network. State estimation plays an important role in online security assessment, so that current energy management systems (EMS) have an on-line state estimator among other application functions [1]. Figure 1.2 shows the functionality and role of the state estimation in online security assessments.

1.3.1 Weighted least squares state estimation

Static state estimation is the procedure of obtaining the voltage phasors at all buses of power network from a set of redundant measurements. These measurements are related to the state variables through nonlinear functions and can be written in the matrix format as follows,

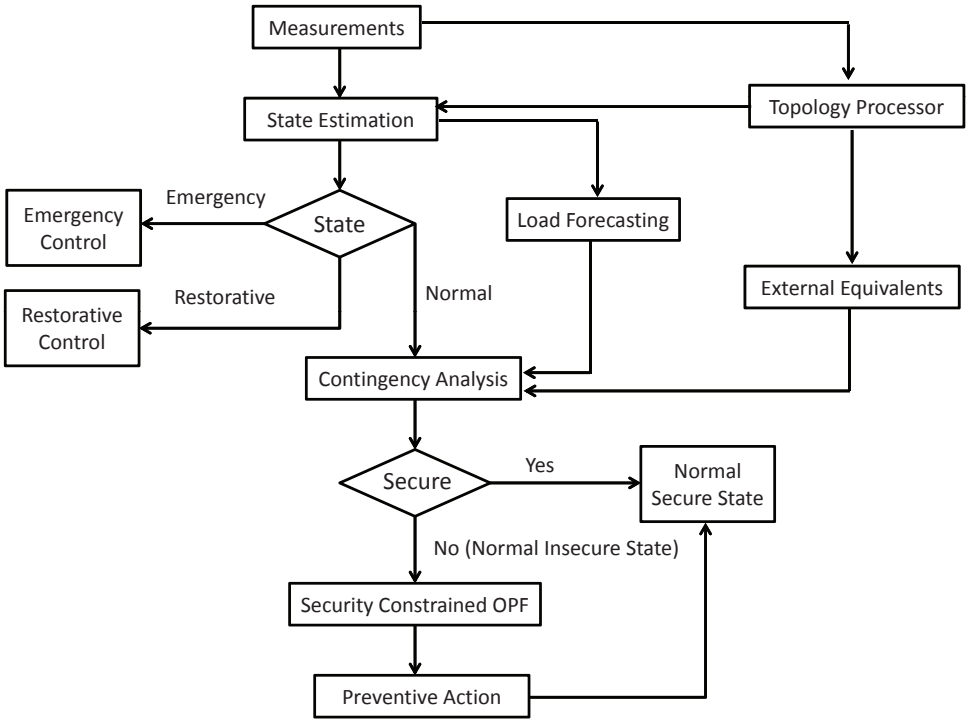


Figure 1.2 On–line Static Security Assessment: Functional Diagram [1].

$$\mathbf{z} = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} p_1(\theta_1, \theta_2, \cdots, \theta_n) \\ p_2(\theta_1, \theta_2, \cdots, \theta_n) \\ \vdots \\ p_m(\theta_1, \theta_2, \cdots, \theta_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} = \mathbf{p}(\theta) + \mathbf{e}, \tag{1.1}$$

where $\mathbf{z}^T = [z_1, z_2, \cdots, z_m]$ is the measurement vector and $\mathbf{e}^T = [e_1, e_2, \cdots, e_m]$ is the measurement error vector. Mathematically (1.2) is an over determined system because it has more equations (measurements) than unknowns (state variables). Weighted least square method is the common way of solving over–determined systems in which the goal is to solve the following optimization,

$$J(\theta) = [\mathbf{z} - \mathbf{p}(\theta)]^T R^{-1} [\mathbf{z} - \mathbf{p}(\theta)], \tag{1.2}$$

where $\mathbf{R} = diag(\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2)$ and σ_i^2 is the standard deviation of measurement i.

1.3.2 Linear state estimation

In power systems, transmission lines are used to transfer generated power to consumers. Theoretically, the transmitted complex power between bus i and bus j depends on the voltage difference between these two buses, and it is also a function of impedance between these buses. In general, transmission lines have high reactance over resistance (i.e. X/R ratio), and one can approximate the impedance of a transmission line with its reactance. The transmitted active power from bus i to bus j can be written as [68]:

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), \tag{1.3}$$

where V_i is the voltage magnitude, θ_i is the voltage phase angle in bus i, and X_{ij} is the reactance of transmission line between bus i and bus j. In DC power flow studies, it is assumed that the voltage phase difference between two buses is small and that the amplitudes of voltages in buses are near to unity. Transmitted power is approximated with a linear equation [69]

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}, \tag{1.4}$$

where θ_i is the voltage phase angle in bus i, and X_{ij} is the reactance of transmission line between bus i and bus j. In the state-estimation problem, the control center tries to estimate n phase angles θ_i, by observing m real-time measurements. In power flow studies, the voltage phase angle (θ_i) of the reference bus is fixed and known, and thus only $n-1$ angles need to be estimated. We define the state vector as $\theta = [\theta_1, \ldots, \theta_n]^T$. The control center observes a vector $\mathbf{z}$ for m active power measurements. These measurements can be either transmitted active power P_{ij} from bus i to j, or injected active power to bus i ($P_i = \sum P_{ij}$). The observation can be described as follows,

$$\mathbf{z} = \mathbf{P}(\theta) + \mathbf{e}, \tag{1.5}$$

where $\mathbf{z} = [z_1, \cdots, z_m]^T$ is the vector of measured active power in transmission lines, $\mathbf{P}(\theta)$ is the nonlinear relation between measurement z, state θ is the vector of n bus phase angles

θ_i, and $\mathbf{e} = [e_1, \cdots, e_m]^T$ is the Gaussian measurement noise vector with covariant matrix $\mathbf{\Sigma}_e$.

Define the Jacobian matrix $\mathbf{H} \in \mathbb{R}^m$ as

$$\mathbf{H} = \frac{\partial \mathbf{P}(\theta)}{\partial \theta} \mid_{\theta = \mathbf{0}} . \tag{1.6}$$

If the phase difference $(\theta_i - \theta_j)$ in (1.4) is small, then the linear approximation model of (1.5) can be described as

$$\mathbf{z} = \mathbf{H}\theta + \mathbf{e}. \tag{1.7}$$

The bad data can be injected to $\mathbf{z}$ so as to influence the state estimation of θ. Next, we describe the current bad data injection methods used in state estimators of different electricity markets. Given the power flow measurements $\mathbf{z}$, the estimated state vector $\hat{\theta}$ can be computed as,

$$\hat{\theta} = (\mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{z} = \mathbf{M}\mathbf{z}, \tag{1.8}$$

where

$$\mathbf{M} = (\mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}_e^{-1}. \tag{1.9}$$

Thus, the residue vector $\mathbf{r}$ can be computed as the difference between measured quantity and the calculated value from the estimated state,

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\theta}. \tag{1.10}$$

Therefore, the expected value and the covariance of the residual are,

$$E(\mathbf{r}) = 0 \text{ and } cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\mathbf{\Sigma}_e, \tag{1.11}$$

1.3.3 Bad data detection

False data detection can be performed using two methods, Chi–squares χ^2 test and maximum residue test methods.

1.3.3.1 Chi–squares χ^2 test

If N independent random variables $X_1, X_2, \cdots, X_N$ follow normal distribution $X_i \sim N(0,1)$, then new random variable $Y = \sum_{i=1}^{N} X_i^2$ follows χ^2 distribution with N degree of freedom ($Y \sim \chi^2_N$). The degrees of freedom N, represents the number of independent variables in the sum of squares. Now summation of square errors of measurements gives,

$$f(x) = \sum_{i=1}^{m} R_{ii}^{-1} e_i^2 = \sum_{i=1}^{m} (\frac{e_i}{\sqrt{R_{ii}}})^2 = \sum_{i=1}^{m} (e_i^N)^2, \tag{1.12}$$

where m is the total number of measurements, R_{ii} is the diagonal entry of the measurement error covariance matrix, and e_i is the i^{th} measurement error. If e_i's are Normally distributed random variables (with zero mean and R_{ii} variance), e_i^N's will follow a standard Normal distribution, (i.e. $e_i^N \sim N(0,1)$) and $f(x)$ will have a χ^2 distribution with at most $(m-n)$ degrees of freedom. As described before in state estimation we have more equation than unknowns i.e there are at least n measurements that have to satisfy the power balance equations so at most $(m-n)$ of the measurement errors will be linearly independent. This means, the largest degree of freedom can be $(m-n)$ (i.e. the difference between the total number of measurements and the system states). Now in order to have error free measurements we should have,

$$J(\hat{x}) \leq \chi^2_{(m-n),p}, \tag{1.13}$$

where $J(\hat{\theta})$ is the objective function of WLS estimation problem and should be obtained from solving (1.2). $\chi^2_{(m-n),p}$ is the value corresponding to a detection confidence with probability p and $(m-n)$ degrees of freedom which can be obtained from the Chi-squares distribution table.

1.3.3.2 Maximum normalized residue method

Chi–squares test approximates the residues between measured and estimated values and it might be inaccurate in some cases [1] so most of the state estimators use maximum (normalized) residue method. In this method, the hypothesis of not being attacked is accepted if

$$\max_i |r_i| \leq \gamma, \tag{1.14}$$

where γ is the threshold and r_i is the component of $\mathbf{r}$.

Recently, a certain type of attack was introduced by [39], which is not detectable by max residue vector r. In this attack, an attacker with knowledge of topology $\mathbf{H}$, can add $\mathbf{z}_{att} = \mathbf{Ha}$ to $\mathbf{z}_0$ (the measurement vector without attack). As a result,

$$\mathbf{z} = \mathbf{z}_0 + \mathbf{z}_{att} = \mathbf{z}_0 + \mathbf{Ha}. \tag{1.15}$$

Substituting (1.15) in (1.8) gives,

$$\hat{\theta} = \hat{\theta}_0 + \mathbf{a}, \tag{1.16}$$

where $\hat{\theta}_0 = \mathbf{M}\mathbf{z}_0$ and

$$\hat{\mathbf{z}} = \mathbf{H}\hat{\theta} = \mathbf{H}\hat{\theta}_0 + \mathbf{Ha}. \tag{1.17}$$

Substituting (1.15) and (1.17) in (1.10), we have

$$\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}} = \mathbf{z}_0 - \mathbf{H}\hat{\theta}_0. \tag{1.18}$$

Equation (1.18) shows that residue r will not be affected by the injected attack vector to measurements, since the resulting $\mathbf{r}$ has the same mean and variance as before attack. As a result, the hypothesis test fails in detecting the attacker. In fact, the control center believes that the true state is $\theta_0 + \mathbf{a}$. Consequently, this is called *stealth false data injection*.

1.4 Dissertation Contribution

Although using cyber technologies improves the quality of monitoring and decision making in smart grid, they make the network vulnerable to malicious attacks. This dissertation shows the possible cyber attacks in SCADA system and consequently possible defense mechanisms that can prevent these attacks. One important difference between false data due to *abnormalities of measurements* and *cyber attack* is that usually cyber attack has been planned to bypass the bad data detector while the measurements' abnormalities follow certain statistics that are not difficult to capture in many cases. Following are the main contributions of this dissertation,

Illustration of economical effect of the cyber attack. We first review the structure of electricity market and more specifically we describe day–ahead and real–time markets. Then we present the way that attacker changes the congestion of transmission lines without being detectable. Doing this, attacker alters the congestion in ex–post market (in the desired direction) and makes financial profit.

Inferring structural information and launching stealth attack. We investigate the case that the attackers without prior knowledge of the power grid topology, try to make inferences through phasor observations. We show that when the change of operating conditions is relatively mild and can be approximated linearly, linear independent component analysis can be applied to estimate the Jacobian matrix multiplied by the eigenvectors of the covariance matrix of the state variables. The inferred structural information then is used to launch stealth attacks. This attack is formulated to change the price of electricity in the real-time market.

Demonstration of possible competition between attacker and defender. Attacking and defending all measurements are impossible for the attacker and defender, respectively. This situation is modeled as a zero-sum game between the attacker and de-

fender and we describes how the interest of one party (attacker or defender) can influence the other's interest. The results of this game defines the proportion of times that the attacker and defender like to attack and defend different measurements, respectively.

Detection of stealth false data injection with machine learning techniques. We show how normal operations of power networks can be statistically distinguished from the case under stealthy attacks. We propose two machine learning based techniques for stealthy attack detection. The first method utilizes the supervised learning over labeled data and trains a support vector machine. The second method requires no training data and detects deviation in measurements. In both methods, principle component analysis is used to reduce the dimensionality of the data to be processed, which leads to lower computation complexities.

1.5 Dissertation Organization

The remainder of this dissertation is organized as follows: In Chapter 2, we analyze the economical effect of the bad data injection. Bad data injection in Chapter 2 needs knowledge about the structure of power network (matrix $\mathbf{H}$ in 1.7), in chapter 3 we show how attacker can infer this structure from the observed measurements and insert stealth false data. In the later part of the same chapter, we show how the attack can be formulated to change the electricity prices too. In Chapter 4, we analyze the situations that attacking and defending all measurements is not possible. This study gives a clear picture of actions for both attacker and defender in the situation that they have limitations in attacking and defending different measurements. In Chapter 5, we map the measurements' data to a low dimensional space and we show how the normal operating points are separable from the attacked points. Finally in Chapter 6 we explain the future researches and conclude this dissertation. For the sake of clarity, Table 1.1 and Table 1.2, show the abbreviations and

notations that is used in this dissertation respectively.

Table 1.1 Dissertation Abbreviation

BDD	Bad Data Detection
CC	Control Center
DG	Distributed Generation
DSM	Demand Side Management
ECC	Energy Control Center
ED	Economic Dispatch
EMC	Energy Management Center
FTR	Financial Transmission Right
ICA	Independent Component Analysis
IP	Integer Programming
ILP	Integer Linear Programming
ISO	Independent System Operator
LMP	Locational Marginal Price
LSE	Load Serving Entity
OPF	Optimal Power Flow
PCA	Principal Component Analysis
PJM	Pennsylvania, New Jersey, Maryland
PMU	Phasor Measurement Units
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SE	State Estimation
SVD	Singular Value Decomposition
SVM	Support Vector Machine
WLS	Weighted Least Squares

Table 1.2 Dissertation Notations

P_{ij}	Transmitted power from bus i to bus j
$\boldsymbol{\theta}$	$n \times 1$ vector of voltage angles
X_{ij}	Line reactance between bus i and bus j
$\mathbf{H}$	$m \times n$ Jacobian matrix
$\mathbf{r}$	$m \times 1$ residue vector for BDD
γ	Residue threshold in BDD
$\mathbf{\Sigma}_e$	$m \times n$ covariance matrix of measurements' errors
$\mathbf{z}'$	$m \times 1$ attacked measurement vector
$\mathbf{A}$	First-order coefficient matrix of the Taylor expansion
$\mathbf{K}$	Mixing matrix ($\mathbf{K} = \mathbf{HA}$)
$\mathbf{y_0}$	$C \times 1$ Independent component vector
$\mathbf{y_a}$	$C \times 1$ Attack vector
$\mathbf{y_a^{opt}}$	$C \times 1$ Optimal attack vector
C	Number of independent component in $\mathbf{y}$
C_{gi}	Generation cost at bus i in $\$/MWh$
N	Number of buses
G_i	Generation dispatch at bus i in (MWh)
D_i	Demand at bus i in (MWh)
GSF_{k-i}	Generation shift factor from bus i to line k
$\mathbf{Z_t}$	Measurement sets over m different time steps
$\mathbf{Z_{tr}}$	$m \times k$ reduced measurement matrix
$\boldsymbol{\varphi}$	SVM optimization parameter
$\mathbf{f^{(i)}}$	Similarity function for i^{th} sample
F_1	Metric for evaluating performance of clustering algorithms
ξ	Threshold for Anomaly Detection algorithm

Chapter 2

Effect Of Stealthy Bad Data Injection On Network Congestion In Market Based Power System

2.1 Introduction

In a smart grid, the strong coupling between cyber and physical operations makes power systems vulnerable to cyber attacks. Changing the traditional structure of power systems and integrating communication devices are beneficial for better monitoring and decisionmaking by System Operators but increases the chance of being maliciously attacked. The communication links can be hacked so that the attacker can alter the power flow and power injection measurements, which are used to estimate the states of power system. Power system blackout in 2003 created serious problems for the costumers in the eastern US and Canada. Although different investigations report reasons other than cyber attack for the blackout, but many researchers believe similar tragedy could happen with targeted cyber attack [70]. Later in 2007, researchers at the Idaho National Lab tried to attack a synchronous generator. The attack was successful and the generator was self-destroyed in a couple of minutes [27]. This attack alarmed cyber-security decision makers, motivating them to define critical infrastructure that is vulnerable to cyber-attack.

In this chapter we show that attacker can compromise measurements and insert false data into state estimation. This attack will be undetectable and stealthy enough to defeat traditional bad data detection methods and able to change the transmitted power in transmission lines. This change can increase or decrease the congestion level in the attacked lines, which in a market-based environment will change the price of congestion and Locational Marginal Prices. Our contribution is that the optimization problems are formulated to link the stealthy attack, power congestion and market prices. The simulation results on

IEEE 30-Bus test system shows the changing of the line congestion by a stealthy attack, which provides the financial benefits to attacker. The rest of the chapter is organized as follows. A rational attack is formulated from the attacker point of view in Section 2.2. The structure of the electricity market and the incentive for formulated attack is presented in Section 2.3. A formulated attack is tested on an IEEE-30 bus test system and the results are presented in Section 2.4.

2.2 Attack Against Voltage Angles in State Estimation

As described in Section 1.3.3, if the control center cannot detect the attacked measurements, the results of state estimation will be incorrect and have negative effects on the control center decisions. In this section, we will show that the attacker can compromise the measurement vector and change the state of the system. Change in transmitted power can modify congestion levels, which are closely related to the price at which electricity trades in most markets. We formulate the problem to increase or decrease transmitted active power in the desired transmission lines by injecting bad data as follows:

$$\min_{\mathbf{a}} \quad \sum_{\{ij\}\in\mathcal{M}} P_{ij} - \sum_{\{ij\}\in\mathcal{N}} P_{ij} = \left(\sum_{\{ij\}\in\mathcal{M}} \mathbf{H}_{ij} - \sum_{\{ij\}\in\mathcal{N}} \mathbf{H}_{ij} \right) \hat{\theta} \tag{2.1}$$

$$\text{s.t.} \begin{cases} \mathbf{Z_{min}} \leq \mathbf{Ha} \leq \mathbf{Z_{max}}, \\ C_{min} \leq \mathbf{C}_{att}^{T} \mathbf{Ha} \leq C_{max}. \end{cases}$$

The objective of the above optimization is to decrease and increase transmitted power, respectively, in group $\mathcal{M}$ and $\mathcal{N}$ of transmission lines represented by $\{ij\}$. $\mathbf{H}_{ij}$ are rows of $\mathbf{H}$ corresponding to each line $\{ij\}$, in which the attacker would like to decrease or increase transmitted power[1]. $\hat{\theta}$ is a function of attacking parameter $\mathbf{a}$ in (1.16). The two constraints impose limitations on injected measurement and total cost of attack, respectively, where

[1]From (1.4), transmitted power in some of lines could be negative which means the direction of power flow is opposite of primary assumed direction. Congestion in these lines means the active power flow wants to be less than minimum value which is specified in the OPF program. For removing congestion in these lines, attacker needs to maximize the power flow in the primary assumed direction in (2.1).

$\mathbf{C}_{att}$ is a vector representing the cost of attacking each line. Optimization problem in (2.1) tries to change the estimated transmitted power in the system (without triggering the bad data detection alarm). In order to describe potential benefits for the attacker, the following section will briefly introduce the structure of electricity market.

2.3 Optimal Power Flow (OPF) and DC Optimal Power Flow (DCOPF)

Security and optimality of power network operations are among the most important tasks in control centers, which can be achieved by efficient monitoring and decision making. After deregulation of electric industries, different services that can improve security and optimality of network can be traded in different markets. Energy market is one of these markets in which generation companies (GENCO's) and load serving entities (LSE's) compete to generate and consume energy. The control center, knowing the submitted prices and network constraints, tries to maximize social welfare for all participants. A well known program for solving this optimization is the Optimal Power Flow program. Linear form of the optimal power flow is called DCOPF and is used to define the price of electricity (Locational Marginal Price or LMP) in both day–ahead and real–time markets. In the following, the formulation of DCOPF together with the general structure of day–ahead and real–time markets is described.

In general, the LMP can be split into three components including the marginal energy price LMP_i^{Energy}, marginal congestion price LMP_i^{Cong}, and marginal loss price LMP_i^{Loss} [71]. A common model of the LMP simulation can be written as

$$\min_{\mathbf{G_i}} \qquad \sum_{i=1}^{N} C_{gi} \times G_i, \tag{2.2}$$

s.t.

$$\sum_{i=1}^{N} G_i - \sum_{i=1}^{N} D_i = 0, \tag{2.3}$$

$$\sum_{i=1}^{N} GSF_{k-i} \times (G_i - D_i) \leq F_k^{max},\ k \in \{all\ lines\}, \tag{2.4}$$

$$G_i^{min} \leq G_i \leq G_i^{max},\ \ i \in \{all\ generators\}, \tag{2.5}$$

where N is the number of buses, C_{gi} is the generation cost at bus i in ($/MWh), G_i is the generation dispatch at bus i in (MWh), D_i is the demand at bus i in (MWh), GSF_{k-i} is the generation shift factor from bus i to line k, F_k^{max} is the transmission limit of line, G_i^{max} is the upper generation limit for generator i, and G_i^{min} is the lower generation limit for generator i. Above optimization is called DC Optimal Power Flow program and is used in the formulation of LMP at bus i:

$$LMP_i = LMP^{energy} + LMP_i^{cong} + LMP_i^{loss}, \tag{2.6}$$

$$LMP^{energy} = \lambda, \tag{2.7}$$

$$LMP_i^{cong} = \sum_{i=1}^{L} GSF_{k-i} \times \mu_k, \tag{2.8}$$

$$LMP_i^{loss} = \lambda \times (DF_i - 1), \tag{2.9}$$

where L is the number of lines, λ is the Lagrangian multiplier of the equality constraint (2.3), μ_k is the Lagrangian multiplier of the k^{th} transmission constraint (2.4), and DF_i is delivery factor at bus i. If the optimization model in (2.2) ignores losses, we will have $DF_i = 1$ and $LMP_i^{loss} = 0$ in (2.6). In this work in order to emphasize the main point to be presented, the loss price is ignored. Control center uses the DCOPF program to define LMP's in the day-ahead and real-time markets defined as follows,

2.3.1 Day-Ahead Market

Based on the submitted bids (from generators and loads) and predicted network condition[2], the control center runs the DCOPF program. The output of this market specifies the dispatch schedule for all generators and defines the LMP in each bus of the power network. Trading electricity in most of electricity markets such as PJM Interconnection[3], New York, and New England markets is based on the LMP method.

2.3.2 Real–Time Market

In this market, the control center conducts the following: 1- Gathering data from the measurements that are installed in the physical layer (power network); 2- Estimating the states of the network (online monitoring of the network); 3- Running an incremental dispatch model based on the state estimation results. The obtained LMP's will be considered as the real-time price of electricity[4]. The common model for real–time (Ex–Post) market is as follows [72, 73]:

$$\min_{\mathbf{\Delta G_i}} \qquad \sum_{i=1}^{N} C_{gi}^{R} \times \Delta G_i, \tag{2.10}$$

$$\sum_{i=1}^{N} \Delta G_i - \sum_{i=1}^{N} \Delta D_i = 0, \tag{2.11}$$

$$\sum_{i=1}^{N} GSF_{k-i} \times (\Delta G_i - \Delta D_i) \leq 0,\ k \in \{CL\}, \tag{2.12}$$

$$\Delta G_i^{min} \leq \Delta G_i \leq \Delta G_i^{max}, \quad i \in \{QG\}, \tag{2.13}$$

$$\Delta D_i^{min} \leq \Delta D_i \leq \Delta D_i^{max}, \quad i \in \{DL\}, \tag{2.14}$$

[2]Such as the load level for the next day, which can be predicted by the historical load data from the past years.

[3]PJM Interconnection is a largest competitive wholesale electricity market and serves some eastern parts of US.

[4]Dispatch schedule will be similar to the day–ahead market and major changes in the load will be covered by the Ancillary Services.

where C_{gi}^{R} is the generation cost at bus i in $(\$/MWh)$[5], ΔG_i is the change in the output of generator i, and ΔD_i is the change in the demand of dispatchable load at bus i in (MWh), ΔG_i^{max} and ΔG_i^{min} are the upper and lower band for variations in the generation of each qualified generator (QG)[6]. Similarly, ΔD_i^{max} and ΔD_i^{max} are the upper and lower bands for changes in the consumption of each dispatchable load (DL). The above optimization problem shows that any change in the transmitted power in congested lines (CL), should be non–positive value.

Similar to the day–ahead market, LMP in bus i (without considering the effect of losses) will be,

$$LMP_i^{RT} = \lambda + \sum_{i=1}^{L} GSF_{k-i} \times \mu_k, \tag{2.15}$$

where L is the number of lines, λ is the Lagrangian multiplier of the equality constraint, and μ_k is the Lagrangian multiplier of the k^{th} transmission constraint in (2.12).

In addition to benefiting financially, an attacker could also cause power system black-out. Practically, a transmission line has different types of protecting relays. For example, in the case of overloading (e.g., the results of this chapter's simulated attack) special relays will disconnect the line (to prevent over-heating and physical damage). This line outage (especially during peak hours) would reduce the transmission capacity, increasing the chance of instability in the power system.

2.4 Simulation Results

In this section, we show the effects of the presented attack on the IEEE 30-Bus test system shown in Fig. 2.1. In order to define LMPs in the Ex-Ante market, the control center solves DC optimal power flow in (2.2). This optimization is solved by Matpower, a package of MATLAB M-files for solving power flow and optimal power flow problems [74]. The

[5]This price can be the same as the day–ahead market or can be changed by the generator at a specific time (i.e, 4P.M. – 6P.M. in the PJM market).

[6]All PJM generation units that are following PJM dispatch instructions, are eligible to participate in the real–time market (to set the real–time LMP values), these generation units are called qualified generators.

attack targets line 29 in the power system.

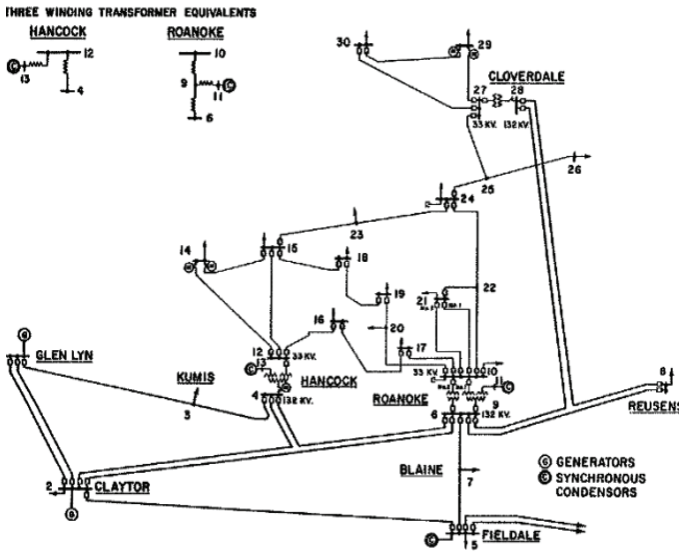


Figure 2.1 IEEE 30–Bus test system.

In Fig. 2.2, we show the voltage angles for different buses with and without attack. We can see that the phase estimation is modified without being detected. Consequently, simulation results show that line 29 (from bus 21 to bus 22) is congested in Fig. 2.3. For comparison, we also show in this figure the case without attack and the thermal limits. As described in Section 2.3, this congestion changes the marginal generator and as a consequence, the network will have different LMPs in its buses as shown in Fig. 2.4. The financial benefit is given by the following example.

Releasing congestion can change LMPs, so an attacker solves (2.1) and inserts an undetectable attack[7]. Due to the stochastic nature of loads, the control center believes that there is no congestion in the network (for example transmitted power through line 29, is less than its thermal limit). Based on these results, the control center will use the free (but fake) capacity in line 29 and run the Ex-Post program for the real-time market. This time, because of released congestion, LMPs will be the same in the network (Fig. 2.4). If, for example, attacker buys $P^{MW} = 10$ at bus 22 in the Ex-Ante market and sells it in the

[7]Practically attacker could insert false data to measurements by, changing the bias of measurements or hacking and sending the desired values to control center.

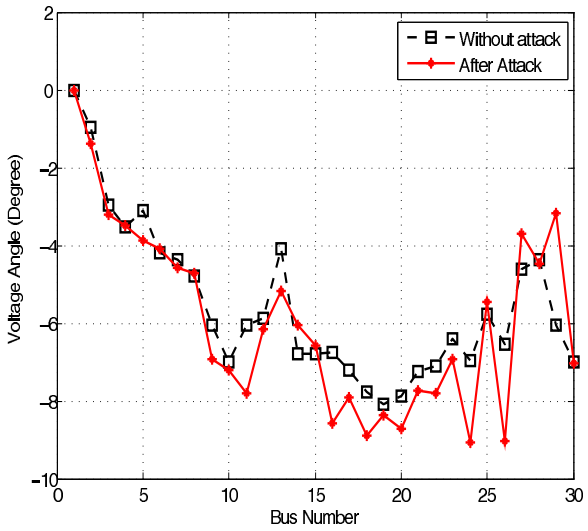


Figure 2.2 Voltage angles in different buses.

Ex-Post market in the same bus, the profit of this transaction will be:

$$Profit_{att}^{(\$/h)} = P^{MW}\left(LMP_{Ex-post}^{\$/MWh} - LMP_{Ex-Ante}^{\$/MWh}\right) = 10^{MW}(3.8^{\$/MWh} - 2.2^{\$/MWh}) = 16^{\$/h}. \tag{2.16}$$

In summary, the attacker can obtain the financial gain through changing power line congestion by stealthy bad data injection without being detected.

2.5 Conclusion

In this chapter, we demonstrate the effect of stealthy false data injection on power system congestion. We described the structure of electricity market and the economical incentive that attacker has in this market. The problem solution links stealthy attack, power congestion, and the resulting market price. We show that by changing congestion, the attacker can change LMPs and obtain financial benefit in an Ex-Post market. Besides financial misconduct, the attacker can also overload specific lines, which consequently increases the risk of line outages. We test our proposed attack in an IEEE 30-bus test system using MATPOWER and show the profitability of such an attack.

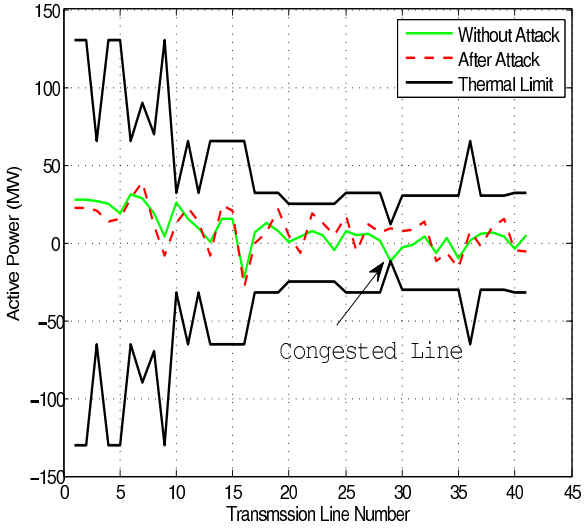


Figure 2.3 Transmitted active power in transmission lines.

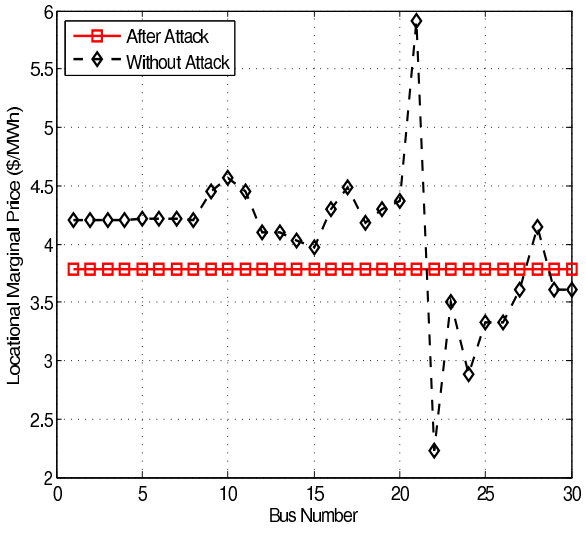


Figure 2.4 Locational marginal price in buses.

Chapter 3

Stealthy Attack Against Electricity Market using Independent Component Analysis

3.1 Introduction

In conventional and smart grid, state estimation is a key function in building real-time model of electricity networks in Energy Management Systems (EMS) [1, 26, 68, 75–77]. A real-time model is a quasi-static mathematical representation of the current conditions in an interconnected power network [26]. Measured data is telemetered to Control Center (CC) every few seconds. CC uses these data to define the mathematical representation for current conditions of the power network. Obtained real-time model will be used to make corrective decisions to bring the power network back to the optimal operating point (from both technical and economical point of views) [78]. Measuring all possible states in the network is not economical or even feasible. Thus, state estimation is a useful tool for estimating those states from a limited set of measurements. Two kinds of information are usually used for state estimation in power systems [68]: i) Analog data of the system such as Megavar flows on all major lines, active power and reactive power loading of generators and transformers, and voltage magnitudes at most of the buses of the system; ii) The on/off status of switching devices such as circuit breakers, reclosers, and transformer taps that determines the network topology. Control centers transfer these data to state estimator using communication networks that are sensitive to malicious attacks [79, 80].

In this chapter, we study a category of undetectable attack, named stealth false data injection attack. Unlike [28, 29, 39, 43, 49], the proposed stealth attack assumes no knowledge of the network topology and makes inferences from the correlations of the line measurements. At the core of the proposed attack, independent component analysis (ICA) is

utilized to infer the linear structure of the power flow measurements. Knowing this structure allows us to formulate an undetectable data injection to change the electricity prices. Simulation studies using the data generated by MATPOWER [74] demonstrate effectiveness of the proposed attack. Our findings reveal the potential vulnerability of smart grid, and make a case for more advanced methods to detect and protect power systems from data injection and manipulation by intruders.

The remainder of this chapter is organized as follows. The system model, false data injection and an undetectable attack are studied in Section 3.2. Formulation of stealth attack in the electricity market and its profit for the attacker is discussed in Section 3.3. The proposed scheme, ICA-based false data injection, is presented and analyzed numerically in Section 3.4. Finally, the conclusion is given in Section 3.5. Some important notations are listed in Table 3.1.

Table 3.1 Electricity Market Notations

P_{ij}	Transmitted power from bus i to bus j
$\boldsymbol{\theta}$	$n \times 1$ vector of voltage angles
X_{ij}	Line reactance between bus i and bus j
$\mathbf{H}$	$m \times n$ Jacobian matrix
$\mathbf{r}$	$m \times 1$ residue vector for BDD
γ	Residue threshold in BDD
$\mathbf{\Sigma}_e$	$m \times n$ covariance matrix of measurements' errors
$\mathbf{z}'$	$m \times 1$ attacked measurement vector
$\mathbf{A}$	First-order coefficient matrix of the Taylor expansion
$\mathbf{K}$	Mixing matrix ($\mathbf{K} = \mathbf{HA}$)
$\mathbf{y_0}$	$C \times 1$ Independent component vector
$\mathbf{y_a}$	$C \times 1$ Attack vector
$\mathbf{y_a^{opt}}$	$C \times 1$ Optimal attack vector
C	Number of independent component in $\mathbf{y}$
C_{gi}	Generation cost at bus i in $\$/MWh$
N	Number of buses
G_i	Generation dispatch at bus i in (MWh)
D_i	Demand at bus i in (MWh)
GSF_{k-i}	Generation shift factor from bus i to line k

3.2 System Model

As described in Section 1.3.2, the state-estimation problem is to estimate n phase angles θ_i's, by observing m real-time measurements. In Section 1.3.2 we showed that if phase difference is small, the relation between measurements and states can be approximated with $\mathbf{z} = \mathbf{P}(\boldsymbol{\theta}) + \mathbf{e}$, where $\mathbf{z} = [z_1, \cdots, z_m]^T$ is the vector of the measured active power in transmission lines. These measurements can be either transmitted active power from bus i to bus j (P_{ij}), or injected active power to bus i ($P_i = \sum_j P_{ij}$). $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n]^T$ is the state vector and $\mathbf{e} = [e_1, \ldots, e_n]^T$ is the measurements error vector. Note that $\mathbf{H}$ is unknown to the attackers but known to the ISO.

3.2.1 Bad data detection in linear state estimation

Given the power flow measurements $\mathbf{z}$, the least square estimated state $\hat{\boldsymbol{\theta}}$ can be computed as:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{z} = \mathbf{M}\mathbf{z}, \tag{3.1}$$

where $\mathbf{M} = \mathbf{H}(\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1}$. The difference between the measured quality and the calculated value from the estimated state is called the residue vector $\mathbf{r}$, and can be computed as the: $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}$. Therefore, the expected value and the covariance of the residual are:

$$E(\mathbf{r}) = 0 \text{ and } cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\boldsymbol{\Sigma}_e. \tag{3.2}$$

False data detection due to faulty sensors or topological errors can be performed using a threshold test [81]. The hypothesis of not being attacked is accepted if

$$\max_i |r_i| \leq \gamma, \tag{3.3}$$

where γ is the threshold and r_i is the i^{th} component of $\mathbf{r}$.

3.2.2 Stealth attack

From the discussion of the false data detection, we observe that if the attacker has knowledge on topology $\mathbf{H}$, it can add $\delta\mathbf{z} = \mathbf{H}\delta\boldsymbol{\theta}$ to

$$\mathbf{z_0} = \mathbf{H}\boldsymbol{\theta} + \mathbf{e}, \tag{3.4}$$

as a result,

$$\mathbf{z}' = \mathbf{H}(\boldsymbol{\theta} + \delta\boldsymbol{\theta}) + \mathbf{e}, \tag{3.5}$$

then the hypothesis test in (3.3) fails in detecting the attacker, since the control center believes that the true state is $\boldsymbol{\theta} + \delta\boldsymbol{\theta}$. This is called *stealth false data injection*. The Unobservable attack generally is the attack that passes the bad data detector. Stealth attack is a special case of unobservable attack. In the stealth attack, due to the configuration of attack, the expected value and the covariance of the residual remains unchanged.

Now the question is if the topology is not available to the attacker, can the attacker still successfully inject stealth false data? Our answer is, somewhat surprisingly, *yes*. The main idea is when system parameters (e.g., active or passive loads) vary in a small dynamic range, the structure (topology) information is in fact embedded in the correlations among power flow measurements. Let $\mathbf{z}(t)$ and $\boldsymbol{\theta}(t)$ be the measurements and state vectors at time t, respectively, where $\boldsymbol{\theta}(t)$ is unknown. At a particular t, it is impossible to infer $\mathbf{H}$ from $\mathbf{z}(t)$ alone. However, over time, if we have knowledge on some stochastic properties of the random process $\boldsymbol{\theta}(t)$, then we may be able to infer $\mathbf{H}$.

In power systems, the state variables are generally a (non-linear) function of the loads $\mathbf{y}$ and the topology $\mathbf{H}$, namely, $\boldsymbol{\theta} = f(\mathbf{y}, \mathbf{H})$. While the topology is static over the time[1], loads can be modeled as *random variables.* If the variations are sufficiently small, we can approximate f with $\boldsymbol{\theta} = \mathbf{A}\mathbf{y}$, where $\mathbf{A}$ is the first-order coefficient matrix of the Taylor

[1]During normal operation, all breakers are closed and transmission lines are connected to the network so the structure of power system will be static over the time.

expansion at $\mathbf{y}$, i.e.,

$$\mathbf{z} = \mathbf{HAy} + \mathbf{e} = \mathbf{Ky} + \mathbf{e}, \tag{3.6}$$

where y has the dimension of $C \times 1$. With $\mathbf{HA}$ and $\mathbf{y}$, we can carry out the false data injection attack by modifying the measurement data as $\mathbf{z}' = \mathbf{z} + \mathbf{HA}\delta\mathbf{y}$, where in section 3.3 attacker will choose $\delta\mathbf{y}$ in order to change the price of electricity. At the control center, from (3.1), we have $\hat{\boldsymbol{\theta}} = (\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}\mathbf{H})^{-1}\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}\mathbf{z}'$. Let $\delta\boldsymbol{\theta} = A\delta\mathbf{y}$. Since $\mathbf{r} = \mathbf{z}' - H\hat{\boldsymbol{\theta}} = \mathbf{z} + \mathbf{H}(\hat{\boldsymbol{\theta}} + \delta\boldsymbol{\theta})$, $E(\mathbf{r}) = 0$, $cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\boldsymbol{\Sigma}_e$. This shows that, the mean and variance of $\mathbf{r}$ remains unchanged for the attacked case, and thus the attack cannot be detected.

3.2.3 ICA algorithm

We use the ICA technique[2] in order to infer $\mathbf{HA}$ and $\mathbf{y}$. The linear ICA [83] is a signal decomposition technique in which the goal is to find a linear representation of the mixed observable signal so that components are as statistically independent as possible. It is a special case of blind source separation when there is no noise,

$$\mathbf{z} = \mathbf{Ky}, \tag{3.7}$$

with $\mathbf{z} = [z_m, m = 1, 2, \ldots, M]$ is the observable vector containing observation from m signal monitors, $\mathbf{K} = [k_{mc}, m = 1, 2, \ldots, M, c = 1, 2, \ldots, C]$ is the unknown mixing matrix, and $\mathbf{y} = [y_c, c = 1, 2, \ldots, C]$ is the source vector of C independent latent variables. Given the model and realizations of $\mathbf{z}$, ICA infers both the mixing matrix $\mathbf{K}$ and the source vector $\mathbf{y}$ by adaptively calculating the weight vector $\mathbf{w}$ and setting up a cost function that maximizes the non–Gaussianity of the calculated $\mathbf{s} = (\mathbf{w}^T\mathbf{z})$.

As signal dynamics are small, we can linearize the mapping between the measurements and the state vector as $\mathbf{z} = \mathbf{H}\boldsymbol{\theta}$. Due to the kirchhoff law, the state vector is typically highly correlated and varying the load on one bus, may change the value of states on the

[2]For other techniques such as Principal Component Analysis (PCA) [82], the uncorrelated random variables can still be dependent. With ICA we can add independent perturbations as shown later.

other buses. Thus, conceptually, we need to further project state vector $\boldsymbol{\theta}$ to a space where the resulting vector $\mathbf{y}$ is independent. In this case, let $\boldsymbol{\theta} = \mathbf{A}\mathbf{y}$, where $\mathbf{y}$ are independent random vectors, and $\mathbf{A}$ is the eigenvectors of $\boldsymbol{\theta}$. We have $\mathbf{z} = \mathbf{H}\mathbf{A}\mathbf{y} = \mathbf{K}\mathbf{y}$.

Now solutions for ICA can be applied to infer $\mathbf{HA}$ and $\mathbf{y}$. In the context of this research, we adopt FASTICA [83], one of the most widely used ICA algorithms. It is based on the optimization of a nonlinear contrast function measuring the non-Gaussianity of the sources. The algorithm is reported to converge quickly and does not depend on the user-defined parameters. In the following sections, we briefly describe secure and economical operation of power networks and then we will discuss a particular vulnerability in the monitoring of states for the power network.

3.3 Cyber Attack Against Electricity Prices

The real-time market uses state estimator results that reflect the run-time state of the network. In order to transfer data to the state estimator, the control center uses different communication channels. If an attacker can change the measurement values, the results of state estimation and consequently real-time market prices will be affected. Changing measurements' data without detection by Bad Data Detection (BDD) for financial gain, is the main goal of attackers in this chapter. In the previous subsection, we describe that congestion in lines will change the price of electricity in the network. In order to manipulate the congestion level in a specific line, the attacker needs to define the group of measurements that can increase or decrease the congestion, and then, knowing the mixing matrix $\mathbf{K}$, the attacker will insert an undetectable false data $\delta\mathbf{z} = \mathbf{K}\delta\mathbf{y}$ into the measurements as shown in (3.5) and (3.6).

Equation (1.4) shows that any change in voltage angle can change the transmitted power through the line. For example any increase/decrease in $\triangle\theta = (\theta_i - \theta_j)$ will increase/decrease the transmitted power in line L_{ij}. In online monitoring of power systems,

the transmitted power from bus i to bus j is estimated with $\hat{P_{ij}} = \frac{\hat{\theta}_i - \hat{\theta}_j}{X_{ij}}$, this equation together with (3.1) and (3.6) gives the following:

$$\hat{P_{ij}} = \frac{\hat{\theta}_i - \hat{\theta}_j}{X_{ij}} = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}\mathbf{z}, \tag{3.8}$$

$$= \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}\mathbf{K}\mathbf{y} = \mathbf{n^T}\mathbf{y} = \sum_{c=1}^{C} n_c y_c,$$

where $\frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}\mathbf{K} = \mathbf{n^T}$, $\mathbf{M_i}$ is the i^{th} row of matrix $\mathbf{M}$ and C is the number of independent components. Two important observations can be made from (3.8),

1) Increasing y_c, increases and decreases $\hat{P_{ij}}$ if and only if $n_c > 0$ and $n_c < 0$, respectively,

2) Varying the value of a component with a larger n_c results in bigger changes in the estimated power.

These observations are crucial to stage effective targeted attacks[3]. Because attackers have no access to $\mathbf{H}$ (consequently $\mathbf{n}$), they need to infer the signs of n_c's. Suppose the transmitted power through line L_{ij} (from bus i to bus j) is near the thermal limit (but is not congested yet), and the attacker wants to increase the estimated transmitted power (to create congestion in this line). In order to infer the sign of n_c, the attacker compromises each component of $\mathbf{y}$ separately, and determines the sign of each n_c based on the observed results on the real-time market. To do so, the attacker increases the c^{th} component of $\mathbf{y}$ and wait for the results of the real-time market. If the congestion is created, LMP_i will be greater than LMP_j, which implies $n_c > 0$. Otherwise, if congestion is not created, the attacker decreases the c^{th} component of $\mathbf{y}$ and if in this case congestion is increased, one can infer $n_c < 0$. This test should be repeated for all components of $\mathbf{y}$ to determine the sign of each n_c (for $c = 1, \cdots, C$) where C is the number of component of $\mathbf{y}$. As described before, launching successful attack depends not only on the sign of n_c's, but also

[3]Targeted attack means that attacker wants to change the congestion in the desired direction (increasing or decreasing the congestion).

their magnitudes too. Similar to the previous part, the attacker can infer the magnitudes of n_c by observing the changes induced to the real-time market. With the knowledge of the signs of n_c's, the attacker compromises the measurements for a number of times (say, Q) and observes the results. The component that has the highest success rate is the best candidate for attacks. Conceptually, for the c^{th} component of $\mathbf{y}$ the attacker solves the following optimization problem:

$$\max_{\mathbf{y_c}} . \quad Sign(n_c) \times \delta y_c, \tag{3.9}$$

$$\text{s.t.} \begin{cases} \mathbf{z}_{min} \leq \mathbf{K}\delta\mathbf{y} \leq \mathbf{z}_{max}, \\ y_d = 0, \quad \forall\, d \neq c. \end{cases}$$

The first constrain indicates that the maximum amount of stealth attack should be limited between $\mathbf{z}_{min}$ and $\mathbf{z}_{max}$. Otherwise large and unusual changes may be detectable by expert engineers in the control center.

Algorithm 1: Increasing congestion with stealth false data injection

input : $\mathbf{z}_0 =$ data matrix;

1 [$\mathbf{K}$ and $\mathbf{y}_0$] = `FastICA` ($\mathbf{z}_0$);
2 **for** $c = 1 : C$ **do**
  determine $\delta\mathbf{y}$ from (3.9) then,
  for $q = 1 : Q$ **do**
    $\mathbf{z}' = \mathbf{z}_0 + \mathbf{K}\delta\mathbf{y}$ and wait for market results
    if $LMP_{ij}^{EP} < LMP_{ij}^{EA}$ **then**
      $Counter = Counter + 1$ (counting successful att.)
    end if
  exit;
  exit;
3 Select $\delta\mathbf{y}^{opt}$ from the $max.$ number of successful att. ($Counter$)
4 $\mathbf{z}' = \mathbf{z}_0 + \mathbf{K}\delta\mathbf{y}^{opt}$;

output: compromised measurements $\mathbf{z}'$

The algorithm of attack is summarized in Algorithm 1. In step 1, the attacker runs the ICA program on the historical data and infers matrix $\mathbf{K}$ and $\mathbf{y}_0$. Step 1 verifies if $\mathbf{z}_0$ follows a linear model: if the linearity assumption holds then $\max(\mathbf{z}_0 - \mathbf{K}\mathbf{y}_0)$ should be small. In step 2, the attacker learns which sets of $\mathbf{y_0}$ increase and decrease the congestion

by repeatedly compromising the corresponding component and observing the market responses. In step 3, the attacker selects $\delta\mathbf{y}^{opt}$ that has the maximum number of successful attacks (according to the counters in step 2). And finally in step 4, the attacker inserts $\delta\mathbf{y}^{opt}$ to $\mathbf{y_0}$.

Algorithm 1 enables the attacker to create congestion in line L_{ij}; Following a similar process can also release the congestion level. Both creating and releasing congestion will change the electricity prices. In the following we describe how the attacker can make profits by doing so.

3.3.1 Decreasing congestion

In the day–ahead market, the attacker buys at a lower price LMP_i^{DA} and sells at higher price LMP_j^{DA} ($LMP_i^{DA} < LMP_j^{DA}$). The difference between two prices should be paid to the transmission company as the congestion prices. In the real–time market, because of decreased congestion, the congestion price paid by the attacker is less than the projected congestion price in the day–ahead market. Therefore, the profit of this trade in $\$/MWh$ is:

$$\begin{aligned} P_{Cng}^{Dec} &= Congestion_{Price}^{DA} - Congestion_{Price}^{RT} \\ &= (LMP_j^{DA} - LMP_i^{DA}) - (LMP_j^{RT} - LMP_i^{RT}). \end{aligned} \tag{3.10}$$

3.3.2 Increasing congestion

Increasing the transmitted power from bus i to bus j, can create congestion in line L_{ij}. This congestion increases/decreases the price of electricity in the receiving/sending end of the transmission line. The attacker purchases in the day-ahead market a Financial Transmission Right (FTR) from sending bus i to receiving bus j. FTR is a financial contract to hedge congestion charges. The FTR holder has access to a specific transmission line in a defined time and location to transmit a specific value of power. In the real–time market,

by creating congestion, an attacker can make profit by selling FTR (with higher price) to any Load Serving Entities (LSE's).

3.4 Numerical Results

In this section, we first evaluate the performance of the ICA methodology through extensive simulations using different network topologies. Then, we evaluate the financial implication of the stealth attack when the attacker only has the knowledge of measurement values over time. Attacker uses the ICA method to first infer the $\mathbf{K}$ matrix and then changes the transmission congestion. We use MATPOWER [74], a MATLAB simulation tool for solving power flow and optimal power flow problems. The presented results are experiment results conducted on the 4-Bus test system [68] (Fig. 3.2), IEEE 14-Bus (Fig. 3.1) and 30-bus [84] power grid models with different numbers of measurements. We have used the loads are uniform random variables in load buses, which gives rise to (correlated) variations in the state vector. We also evaluate the impacts of measurement noises on the detection probability.

3.4.1 Validation of linearity in ICA

In this subsection, we evaluate the validity of linearity assumptions in ICA and its performance with different levels of noises and different numbers of measurements.

Figure 3.3 shows the mean square error (MSE) $\Delta\mathbf{z}_0 = \mathbf{z}_0 - \mathbf{K}\hat{\mathbf{y}_0}$, where $\mathbf{K}$ and $\hat{\mathbf{y}_0}$ are the estimation by ICA under different topologies. In the experiments, we vary the level of measurement noises ($\mathbf{e}$ in (3.6)) indicated by the Signal Noise Ratio (SNR) of the true signal and the measurement noise. As shown in Figure 3.3, with increasing SNR, the mean square error (MSE) decreases linearly in the log-log scale. Furthermore, for different types of buses, the MSEs coincide even though the 14-bus has a more complex structure. When SNR is high (~ 40dB), the MSE is as low as 10^{-4}. This implies that the power flow

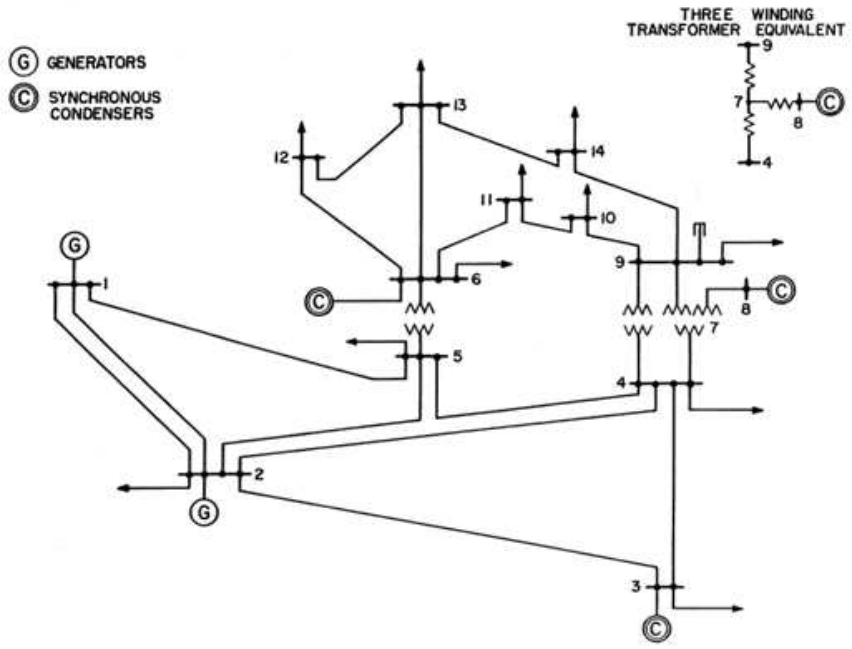


Figure 3.1 IEEE 14–Bus test system.

can indeed be characterized by a linear model, and the ICA can successfully identify the underlying structure for different topologies as long as the noise is not too significant.

Next, we evaluate the speed of convergence of ICA. Figure 3.4 gives the MSEs with different number of observations under different SNRs (5dB and 30dB) in the 14-bus topology. Similar results have been observed for other topologies and are thus omitted. As shown in Figure 3.4, as the number of measurements per bus increases from 10 to 30, the MSEs decrease drastically. However, when the number of measurements per bus increases beyond 30, there is little change in MSEs for both SNR levels. Therefore, we can conclude that the ICA algorithm can achieve high accuracy with a small number of observations. This implies that the attacks can be launched in almost real time.

In the third experiment, we study the independence of state vector θ_0. We compute the eigenvalues of the covariance and sort them in descending order. As shown in Figure 3.5, the state vector is clearly highly correlated. In fact, for the 14-bus and 30-bus, there are only 8 and 12 main components (with eigenvalues greater than 10^{-4}). Since ICA

Figure 3.2 4-Bus test power system.

gives independent components, the resulting $\mathbf{y}_0$ are naturally independent.

3.4.2 Performance of attacks

In the previous section, we demonstrate that the ICA algorithm can successfully identify the linear structure of the power flow measurements. Next, the strength of the ICA-based attack is evaluated. As a baseline, we consider a naive attack that randomly injects false data (following a Gaussian distribution with zero mean and the same variance, 10dB higher than the noise level) without knowledge on $\mathbf{H}$. We further compare the proposed attack to the case without any false data injection.

The null hypothesis (no attack) is accepted when (3.3) holds. The probability that the null hypothesis is determined to be true is an increasing function of the threshold. To compute the probability, we assume the residual error $\mathbf{r}$ follows the Gaussian distribution with the mean and variance in (3.2), respectively.

From Figure 3.6, we can see the proposed stealth attack has an almost identical probability as the no-attack case in the 14-bus topology. Thus it is indistinguishable for the

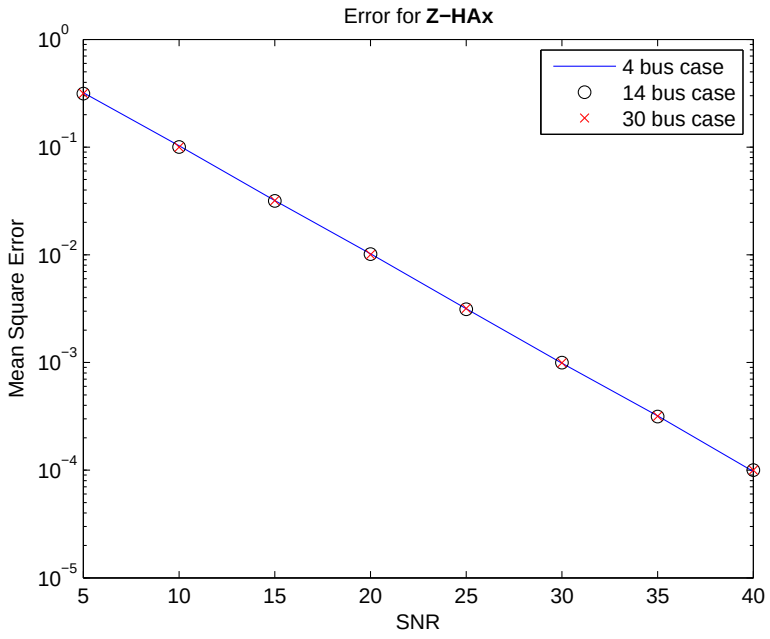


Figure 3.3 MSE of ICA inference ($\mathbf{z}_0 - \mathbf{K}\mathbf{y}_0$) vs. SNR.

Table 3.2 Line Reactance and thermal limit for 5–bus test system.

Line	L_{12}	L_{14}	L_{15}	L_{23}	L_{34}	L_{45}
X (%)	2.81	3.04	0.64	1.08	2.97	2.97
$F_k^{max}(MW)$	999	999	999	999	180	999

proposed attack using any probability based detection algorithm. On the other hand, the random attack has very different characteristics. Simulations on the other topologies show the similar results.

3.4.3 Attack against line congestion

In order to study the effect of the proposed attack on congestion and consequently the electricity prices, we use PJM 5-Bus Test System[4] with slight modifications. Transmission lines' parameters are given in Table 3.2 and Table 3.3. Generators' and loads' parameters (including G_i^{max}, C_i, and D_i) together with the location of measurements are shown in

[4]PJM 5-Bus Test System, is a small power network, which is often used for economical studies of power networks.

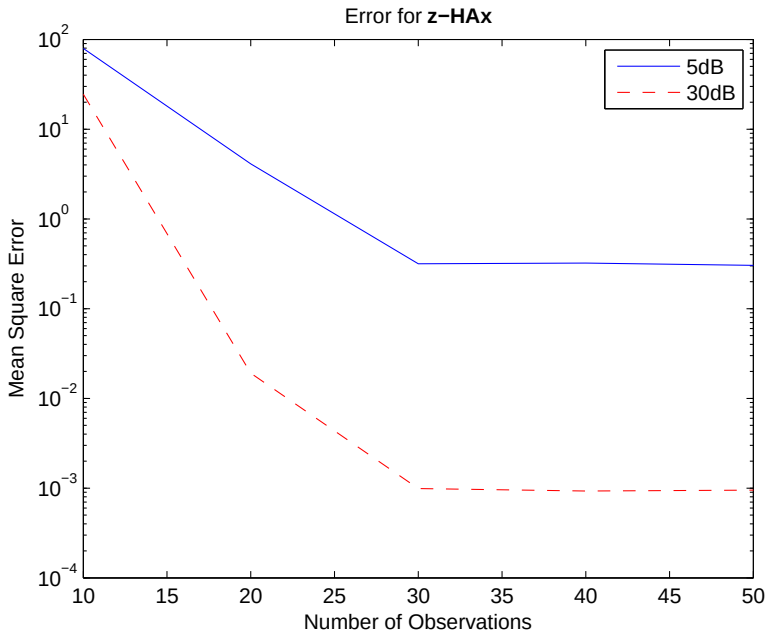


Figure 3.4 MSE of ICA inference ($\mathbf{z}_0 - \mathbf{K}\mathbf{y}_0$) vs. the number of Observations (14-bus case).

Figure 3.7. We use random loads with the specified mean and variance to simulate realistic conditions in the network. After solving (2.2) for the base case (without attack), results of the day-ahead market shows that there is no congestion on the lines and thus LMP will be the same in all buses (Figure 3.8) but the transmitted power in line L_{34} (from bus 3 to bus 4) is near its thermal limit. The attacker buys a specific amount of FTR (in line L_{34}), and decides to compromise measurements and create congestion in the real-time market. As previously described, this congestion will prevent dispatching of cheap generation and will increase the congestion price ($LMP_3 - LMP_4$) in line L_{34} (Figure 3.8 shows the the LMP's before and after a successful attack). The attacker follows the procedure in Algorithm 1. In the 1^{st} and 2^{nd} steps the attacker uses ICA and obtains mixing matrix $\mathbf{K}$. The simulation result shows that PJM 5–bus test system has 4 independent components so the dimension of $\mathbf{K}$ is 11×4. Notice that 11 is the number of measurements in the PJM 5-bus test system as shown in Figure 3.7.

To evaluate the effect of compromising each component of $\mathbf{y}$, the attacker injects

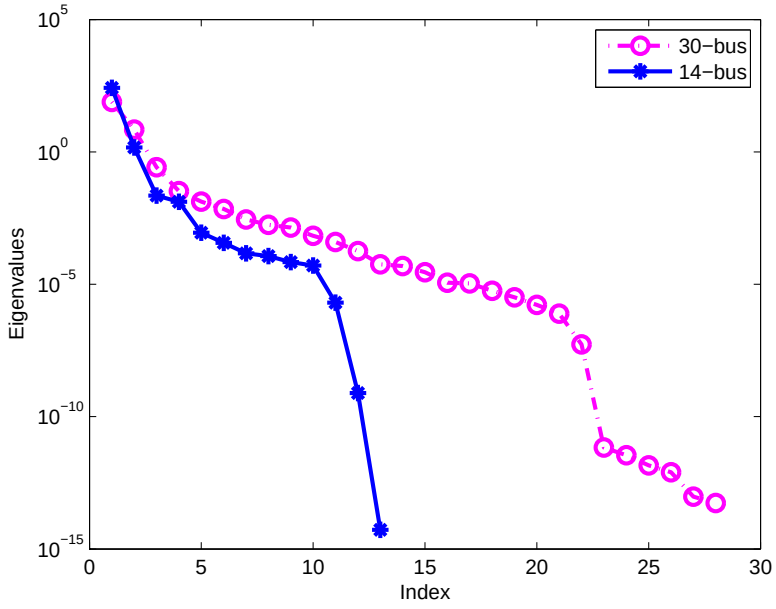


Figure 3.5 Eigenvalues of the state vector of different bus topologies.

false data to each element for a specific number of times ($Q = 1000$) and outputs the compromised $\mathbf{z}' = \mathbf{z_0} + \mathbf{K}\delta\mathbf{y}$. The percentage of successful attacks, defines the best component to attack (step 3). Figure 3.9 shows the attack vectors $\mathbf{K}\delta\mathbf{y}$, which are undetectable by the control center and will change the estimated voltage angle in the network (Figure 3.10). Any change in the estimated angle will change the estimated transmitted power in the transmission line (Figure 3.11). As previously described, the magnitude of such changes is not known to the attacker, instead it observes the changes in real time market prices, which is used to determine the optimal attack vector. Figure 3.12 shows that $\mathbf{y_4}$ have the most effect in creating congestion at line L_{34}. These results are consistent with the results in Figure 3.11, which assumes the knowledge of network topology and indicates $n_4 > n_3 > n_1 > n_2$. The attacker hereby inserts $\mathbf{K}\mathbf{y_4}$ to the measurements ($\mathbf{z}' = \mathbf{z_0} + \mathbf{K}\mathbf{y_4}$). This attack, after creating congestion in the real-time market, changes the LMP's in either end of the congested line. As a result, the attacker can sell $FTR_{34} = LMP_3 - LMP_4 = 30 - 8.64 = 21.36(\$/MWh)$ to any transmission costumer

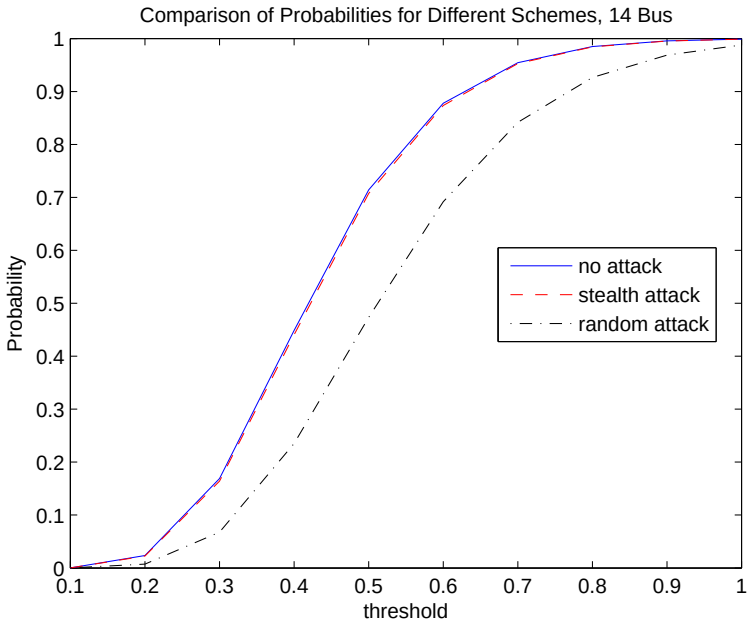


Figure 3.6 Probability for miss detection of attacks.

who needs to transfer power in this line[5].

Table 3.4 shows $\delta\mathbf{y}$ and the number of successes out of 1000 trials in creating congestion for each attack vector. Three different thresholds are used in the inequality constraints in (3.9) (it is assumed that $\epsilon = \mathbf{z_{max}} = -\mathbf{z_{min}}$). As Table 3.4 shows, the higher values of threshold gives rise to better chances of creating congestion but also increases the risk of detection by expert engineers in the control center. Similar to Figure 3.12, this table shows that $\delta\mathbf{y_4}$ has the most effect on changing congestion.

3.5 Conclusion

In this chapter, we proposed an inference algorithm in smart grid based on the linear independent component analysis. We showed that an attacker can estimate the system topology just by observing the power flow measurements using the ICA algorithm. Once

[5]It is assumed that the attacker already has bought $FTR_{34} = LMP_3 - LMP_4 = 30 - 30 = 0(\$/MWh)$ in the day-ahead market.

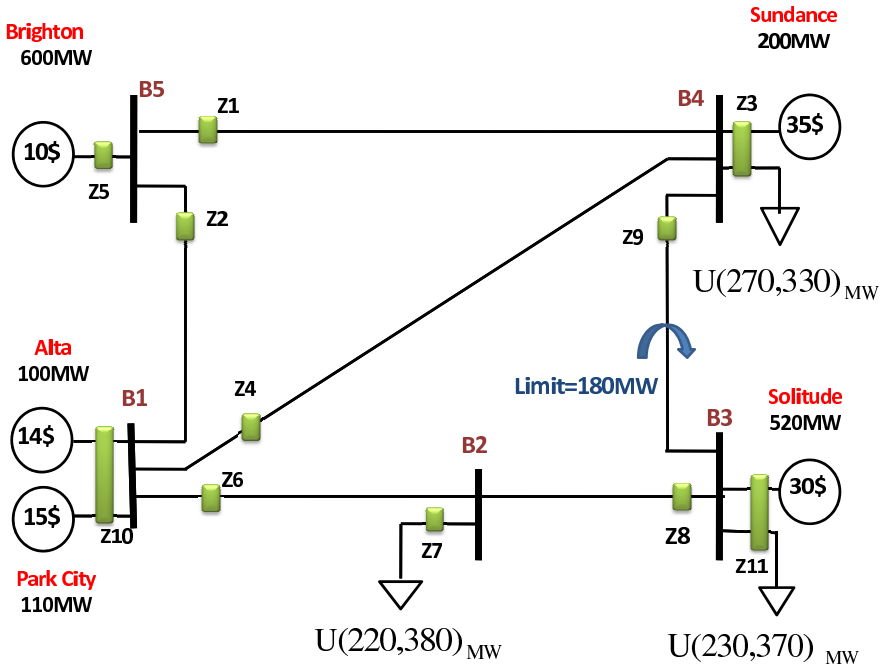


Figure 3.7 Measurement configuration in the PJM 5-bus test system.

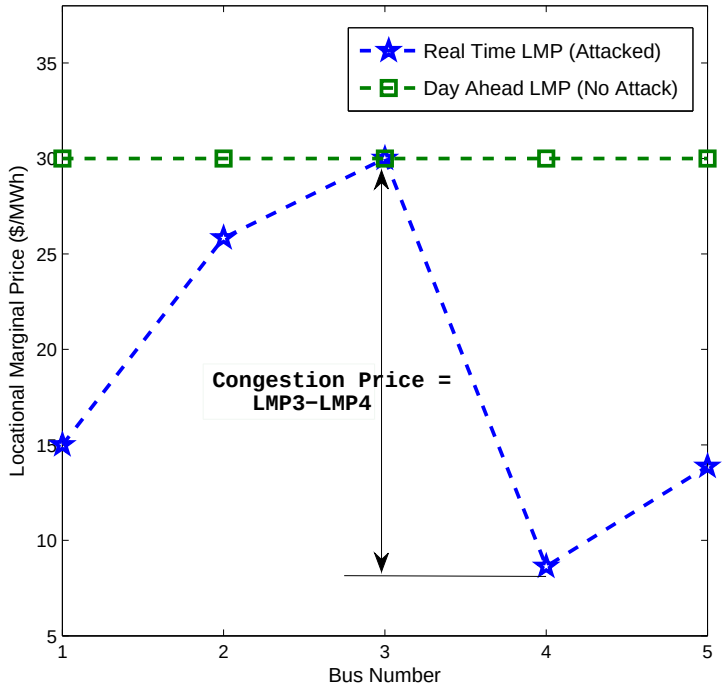


Figure 3.8 LMP's after and before successful attack ($\mathbf{K}y_4$).

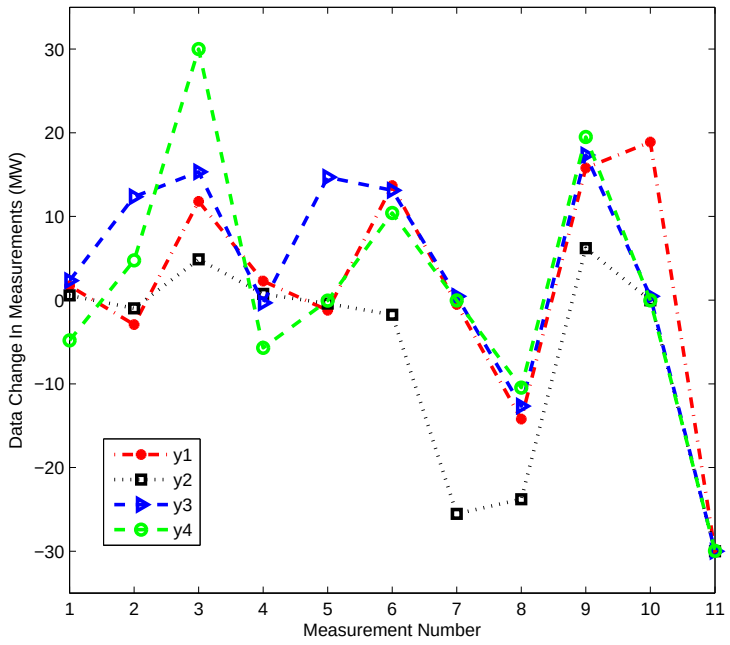


Figure 3.9 Injected false data to the measurements in order to change the estimated transmitted power $\mathbf{z}_a$.

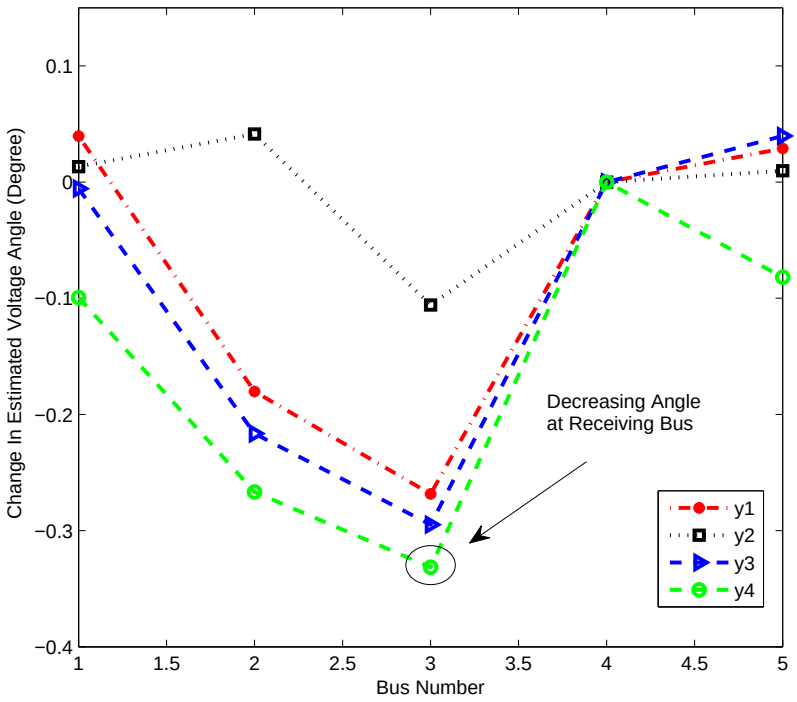


Figure 3.10 Change in estimated angle in each bus (by compromising individual components).

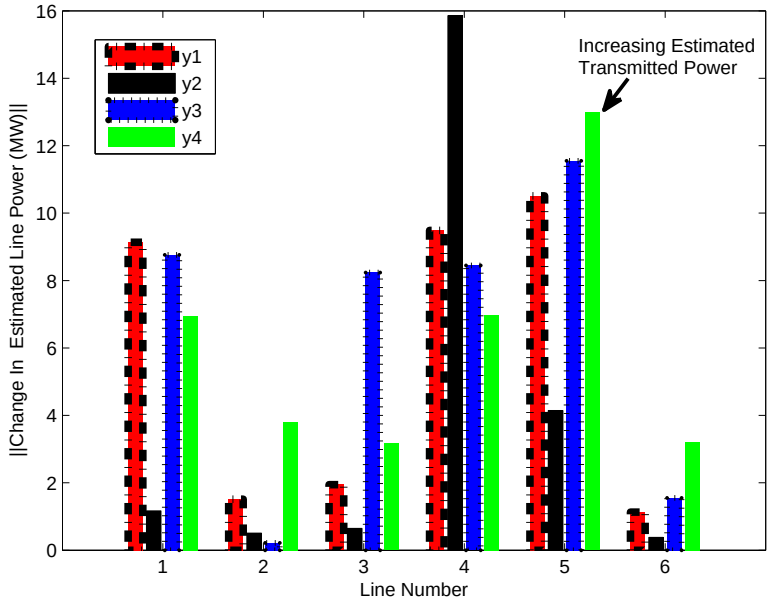


Figure 3.11 Change in the estimated transmitted power.

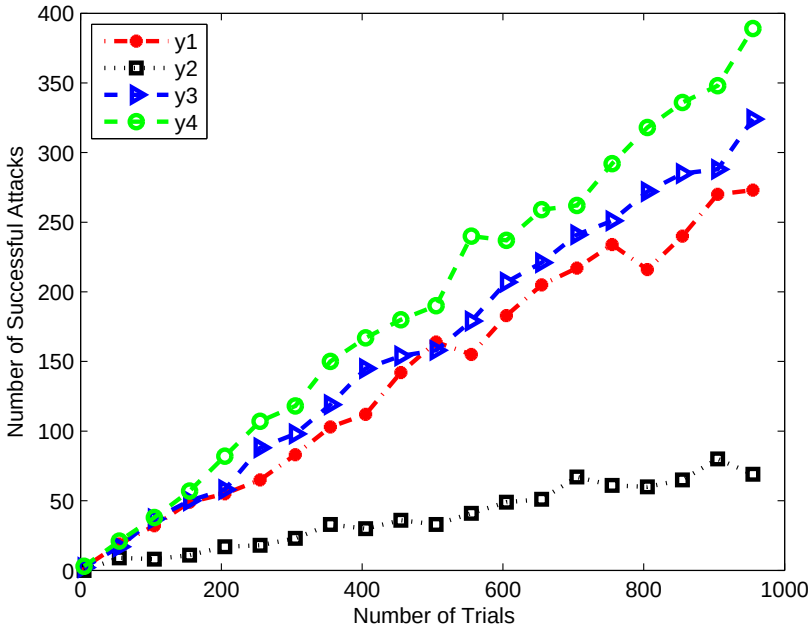


Figure 3.12 Effects of varying individual components on congestion.

Table 3.3 Generation shift factors of lines in 5–bus test system.

Line \ Bus	B_1	B_2	B_3	B_4	B_5
L_{1-2}	0.1939	-0.476	-0.349	0	0.1595
L_{1-4}	0.4376	0.258	0.1895	0	0.36
L_{1-5}	0.3685	0.2176	0.1595	0	-0.5195
L_{2-3}	0.1939	0.5241	-0.349	0	0.1595
L_{3-4}	0.1939	0.5241	0.6510	0	0.1595
L_{5-4}	0.3685	0.2176	0.1595	0	0.4805

Table 3.4 Attack vector $\delta\mathbf{y}$ and number of successful attacks (for $Q = 1000$ attack).

$\delta\mathbf{y}$	$\delta\mathbf{y_1} = \begin{bmatrix} 0.03 \\ 0 \\ 0 \\ 0 \end{bmatrix}$	$\delta\mathbf{y_2} = \begin{bmatrix} 0 \\ 0.01 \\ 0 \\ 0 \end{bmatrix}$	$\delta\mathbf{y_3} = \begin{bmatrix} 0 \\ 0 \\ 0.02 \\ 0 \end{bmatrix}$	$\delta\mathbf{y_4} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0.01 \end{bmatrix}$
$\epsilon_\mathbf{1} = 20_{MW}$	151	50	195	**216**
$\epsilon_\mathbf{2} = 30_{MW}$	294	81	335	**368**
$\epsilon_\mathbf{3} = 40_{MW}$	434	116	479	**572**

the information is in hand, malicious stealth attacks can be launched. The false data is inserted in such a way that it changes the congestion price of electricity. Using the simulated data from MATPOWER, we compare the proposed algorithm with a random attack scheme and showed that our attack methodology is undetectable and can indeed bring financial gains to the attacker.

Chapter 4

Bad Data Injection Attack and Defense in Electricity Market using Game Theory Study

4.1 Introduction

Power system is a very large and complex system that uses huge number of measurements to monitor the current state of the power grid. From cyber–security point of view, attacking and defending all of these measurements are impossible for attacker and defender respectively. This situation can be analyzed by the game theory. Game theory is a mathematical framework for studying complex interactions among the independent rational entities. Psychology, economics, politics, and communication systems are the examples that game theory have been used successfully [53, 54]. The proliferation of advanced technologies and services in smart grid systems implies that disciplines such as game theory will naturally have an outstanding role in the design and analysis of smart grids [55]. The heterogeneous nature of the smart grid[1] and the need for low-complexity distributed algorithms for distributed operation of the smart grid nodes, are the examples that elucidate the application of the game theory in the smart grid studies.

Some applications of game theory in smart grids have been studied in [56–59]. In [56], the authors present a method for evaluating a fully automated electric grid in real time and finding potential problem areas or weak points within the electric grid by using the game theory. In [57], the authors propose a consumption scheduling mechanism for home and neighborhood area load demand management in smart grid using integer linear programming (ILP) and game theory. [58] is a survey about some of game theory-based applications to solve different problems in smart grid. In [59] the authors model and analyze

[1] Smart grid typically composed of a variety of networks such as micro-grids, smart meters, appliances, and others. Each of these networks have different capabilities and may follow different objectives.

the interactions between the retailer and electricity customers as a four-stage Stackelberg game. In this chapter we use game theory to study the interactions between attacker and defender when they have limitations in attacking and defending all measurements. The game defines the proportion of times that the attacker and defender like to attack and defend different measurements, respectively.

The remainder of this chapter is organized as follows: The system model is given in Section 4.2, and the formulation of an undetectable attack in the electricity market is given in Section 4.3. Section 4.4 models the interactions between the attacker and defender as a zero–sum game. Numerical results are shown in Section 4.5, and the conclusion closes the chapter in Section 4.6.

4.2 System Model

As described in Section 1.3.2, the state-estimation problem is to estimate n phase angles θ_i's, by observing m real-time measurements. In Section 1.3.2 we showed that if phase difference is small, the relation between measurements and states can be approximated with $\mathbf{z} = \mathbf{P}(\boldsymbol{\theta}) + \mathbf{e}$, where $\mathbf{z} = [z_1, \cdots, z_m]^T$ is the vector of the measured active power in transmission lines. These measurements can be either transmitted active power from bus i to bus j (P_{ij}), or injected active power to bus i ($P_i = \sum_j P_{ij}$). $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n]^T$ is the state vector and $\mathbf{e} = [e_1, \ldots, e_n]^T$ is the measurements error vector. Note that $\mathbf{H}$ is unknown to the attackers but known to the ISO.

4.2.1 Bad data detection in linear state estimation

Given the power flow measurements $\mathbf{z}$, the least square estimated state $\hat{\boldsymbol{\theta}}$ can be computed as:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{z} = \mathbf{M}\mathbf{z}, \tag{4.1}$$

where $\mathbf{M} = \mathbf{H}(\mathbf{H}^T\mathbf{\Sigma}_e^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{\Sigma}_e^{-1}$. The difference between the measured quality and the calculated value from the estimated state is called the residue vector $\mathbf{r}$, and can be computed as the: $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}$. Therefore, the expected value and the covariance of the residual are:

$$E(\mathbf{r}) = 0 \text{ and } cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\mathbf{\Sigma}_e. \tag{4.2}$$

False data detection due to faulty sensors or topological errors can be performed using a threshold test [81]. The hypothesis of not being attacked is accepted if

$$\max_i |r_i| \leq \gamma, \tag{4.3}$$

where γ is the threshold and r_i is the i^{th} component of $\mathbf{r}$.

4.3 Cyber Attack Against Electricity Prices

Real-time market uses the state estimator results that shows the on-line state of the network. In order to transfer data to the state estimator, control center uses different communication channels such as power line communication channel. Using these channels, increases the risk of cyber attack. In other word, if an attacker can change the measurement values[2], the results of state estimation and consequently results of real-time market will be affected. Changing measurements' data without detection by BDD (which can bring financial benefits) is the main goal of the attacker in this chapter. In the previous section, we described that the congestion in lines will change the price of electricity in the network. Manipulating prices is a good incentive for the attacker to compromise the measurements. In order to manipulate the congestion level in a specific line, the attacker needs to define the group of measurements that can increase or decrease the congestion, then the attacker can insert false data into the measurements. Equation (1.4), shows that any change in

[2]Attacker can carry out stealth attacks by corrupting the power flow measurements through attacking the Remote Terminal Units (RTUs), tampering with the heterogeneous communication network or breaking into the Supervisory Control and Data Acquisition (SCADA) system through the control center office Local Area Network (LAN) [39, 85].

voltage angle can change the transmitted power through the line. For example, any increase/decrease in $\triangle\hat{\theta} = (\hat{\theta}_i - \hat{\theta}_j)$ will increase/decrease the transmitted power. In online monitoring of power systems, the transmitted power from bus i to bus j can be estimated with $\hat{P_{ij}} = \frac{\hat{\theta}_i - \hat{\theta}_j}{X_{ij}}$, and this equation together with equation (1.8) gives the following:

$$\begin{aligned} \hat{P_{ij}} = \frac{\hat{\theta}_i - \hat{\theta}_j}{X_{ij}} = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}\mathbf{z} \\ = \mathbf{Q}^T\mathbf{z} = \mathbf{Q}_+^T\mathbf{z}_+ + \mathbf{Q}_-^T\mathbf{z}_-, \end{aligned} \tag{4.4}$$

where $\mathbf{Q}^T = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}}$. The positive and negative arrays of this vector are shown with $\mathbf{Q}_+^T$ and $\mathbf{Q}_-^T$, respectively. These coefficient vectors divide the measurements into two groups $\mathbf{z}_+$ and $\mathbf{z}_-$, in which adding $z^a > 0$ to any array of $\mathbf{z}_+$ and $\mathbf{z}_-$ will increase and decrease the estimated transmitted power flow, respectively. In this chapter, the measurements in $\mathbf{z}_+$ and $\mathbf{z}_-$ are considered as group $\mathcal{M}$ and $\mathcal{N}$, respectively[3]. After defining these groups, the attacker tries to insert an undetectable bad data into the measurements. Assume $\mathbf{z} = \mathbf{z}_0$ is the measurement values without corruption (safe mode). From (1.10) residue for safe mode will be:

$$\mathbf{r}_0 = \mathbf{z} - \mathbf{H}\hat{\theta} = \mathbf{z}_0 - \mathbf{H}(\mathbf{M}\mathbf{z}_0). \tag{4.5}$$

In the case of attack, $\mathbf{z} = \mathbf{z}_0 + \mathbf{z}^a$ and the residue will be,

$$\begin{aligned} \mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\theta} = \mathbf{z}_0 + \mathbf{z}^a - \mathbf{H}(\mathbf{M}\mathbf{z}_0 + \mathbf{M}\mathbf{z}^a) \\ = \mathbf{z}_0 - \mathbf{H}\mathbf{M}\mathbf{z}_0 + \mathbf{z}^a - \mathbf{H}\mathbf{M}\mathbf{z}^a = \mathbf{r}_0 + \mathbf{r}^a, \end{aligned} \tag{4.6}$$

where $\mathbf{r}^a = (\mathbf{I} - \mathbf{H}\mathbf{M})z^a$. From triangular inequality,

$$\| \mathbf{r} \| \leq \| \mathbf{r}_0 \| + \| \mathbf{r}^a \|, \tag{4.7}$$

[3]It is assumed that attacker knows $\mathbf{H}$ (and consequently $\mathbf{M}$). Knowing the location of attack, from (4.4), attacker can distinguish the measurements in group $\mathcal{M}$ and $\mathcal{N}$.

this equation shows that if $\| \mathbf{r}^a \| = \| (\mathbf{I} - \mathbf{HM}) z^a \|$ is small, with large probability control center can not distinguish between $\| \mathbf{r} \|$ and $\| \mathbf{r}_0 \|$. So inserted attack will path the bad data detection if, $\|(\mathbf{I} - \mathbf{HM})\mathbf{z}^a\| \leq \xi$. In this constraint ξ is a design parameter for the attacker. Smaller values of ξ will be more likely to be undetected by the control center [29]. However, the ability to manipulate the state estimation, will be limited. we assume ξ is predetermined by the attacker. In order to change congestion, attacker will define the inserted false data using the following optimization,

$$\max_{\mathbf{z^a}} . \qquad \sum_{i \in \{\mathcal{M}\}} z^a(i) - \sum_{j \in \{\mathcal{N}\}} z^a(j), \tag{4.8}$$

$$\text{s.t.} \begin{cases} \|(\mathbf{I} - \mathbf{HM})\mathbf{z}^a\| \leq \xi, \\ z^a(k) = 0 \quad \forall\, k \in \{\mathcal{SM}\}, \end{cases}$$

where $z^a(i)$ is the i^{th} element of attack vector $\mathbf{z}^a$. Group $\mathcal{M}$ and $\mathcal{N}$ consist of measurements that increasing and decreasing their value will increase the congestion. Objective of the above optimization is to increase and decrease measurements value in group $\mathcal{M}$ and $\mathcal{N}$, respectively. First constraint is for avoiding detection of the attack by bad data detector in state estimator. Group $\mathcal{SM}$ shows the safe measurements that can not be compromised (such as those protected by Phasor Measurement Units). With inserting the resulted attack vector z^a to the actual values of measurements ($\mathbf{z} = \mathbf{z}_0 + \mathbf{z}^a$), the attacker will change the estimated transmitted power in the attacked line. From (4.4), this change will be

$$\Delta \hat{P}_{ij} = \frac{(\mathbf{M}_i - \mathbf{M}_j)^T}{X_{ij}} \mathbf{z}^a. \tag{4.9}$$

While the attacker tries to increase this change, the defender tries to decrease it by defending the measurements that have high risk of being attacked. Changing the estimated power flow in a specific line will increase the chance of changing prices in both sides of the attacked line[4]. Either increasing or decreasing congestion can bring financial benefits for attacker.

[4]The attacker doesn't have access to all data such as the submitted prices, generation limits, etc. So with changing the estimated transmitted power desired direction, the attacker increases the chance of creating or releasing congestion in the attacked line.

4.3.0.1 Decreasing the congestion

In day–ahead market the attacker buys at lower price LMP_i^{DA} and sells at higher price LMP_j^{DA} ($LMP_i^{DA} < LMP_j^{DA}$). The difference of two prices should be paid to the transmission company as the congestion prices. In the real–time market, because of decreasing congestion, the congestion price paid by the attacker is less than the supposed congestion price in the day–ahead market so the profit of this trade in $\$/MWh$ will be:

$$\begin{aligned} P_{Cng}^{Dec} &= Congestion_{Price}^{DA} - Congestion_{Price}^{RT} \\ &= (LMP_j^{DA} - LMP_i^{DA}) - (LMP_j^{RT} - LMP_i^{RT}). \end{aligned} \tag{4.10}$$

4.3.0.2 Increasing the congestion

Increasing transmitted power from bus i to bus j, can create congestion in line L_{ij}. This congestion increases/decreases the price of electricity in the receiving/sending end of the transmission line. So the attacker needs to buy a Financial Transmission Right (FTR) from sending bus i to ending bus j. FTR is a financial contract to hedge congestion charges. The FTR holder has access to a specific transmission line in a defined time and location to transmit a specific value of power. In real–time market with creating congestion, FTR can be sold (with higher price) to any Load Serving Entities (LSE's).

In the next section, we will analyze the behavior of both attacker and defender in the real–time market. Limitation in attack (to) and defend (from) different measurements makes a difficult situation for both parties. Mathematical modeling of this behavior in the next section, is an efficient answer to the question of *Where should I attack?* and *Where should I defend?* for the attacker and the defender, respectively.

4.4 Gaming Between Attacker and Defender

In order to protect line L, the defender needs to protect group $\mathcal{M}$ and group $\mathcal{N}$. Because the inserted attack will pass the BDD in state estimation (first constraint in (4.8)), the control center should use some other detection methods. For example, the defender can put some secure measurements into random locations in the network. The main problem in this procedure is that defending all measurements is not possible. On the other hand, it is impossible for the attacker to attack all measurements. Instead it tries to attack measurements that have the most effect on the state estimator without being detected by the control center. This behavior can be modeled with a zero–sum strategic game between the attacker and the defender[5].

4.4.1 Two-person zero-sum game between attacker and defender

Define $A = (\mathcal{N}, (\mathcal{S}_i)_{i\epsilon\mathcal{R}}, (\mathcal{U}_i)_{i\epsilon\mathcal{N}})$ as a game, in which the defender and the attacker compete to increase and decrease the change of the estimated transmitted power ($\Delta\hat{P}_{ij}$), respectively. In this game, $\mathcal{R}$ is the set of players (the defender and the attacker), and the game can be defined as:

- Players set: $\mathcal{R} = \{1, 2\}$ (the defender and the attacker).

- Attacker's strategy: to choose measurements to attack.

- Strategy set $\mathcal{S}_i$: The set of available strategies for player i, $\mathcal{S}_1 = \{_\alpha C_{N_a}\}$, $\mathcal{S}_2 = \{_\alpha C_{N_d}\}$, where N_a and N_d are the maximum number of measurements that the at-

[5]In the case that there are different non-cooperative attackers, they will have the worst performance. But if the attackers are cooperative, it is the worst case for the defender. In this chapter, we consider the worst case by assuming all attackers are together as one party. So we formulate the problem as the two-user zero sum game. If the attackers are non-cooperative, some games such as the Stackelberg game can be employed. These games are interesting topics which needs future investigations.

tacker can attack and the defender can defend and ${}_{\alpha}C_{N_a}$ is the combination of N_a measurement out of α measurement.

- Utility: $U_1 = \Delta\hat{P}_{ij}$ and $U_2 = -\Delta\hat{P}_{ij}$ for the attacker and the defender, respectively.

4.4.2 Noncooperative finite games: two–person zero–sum

A strategic game is a model of interactive decision-making, in which each decision-maker chooses its plan of action once and for all, and these choices are made simultaneously. For a given $(m \times n)$ matrix game $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m; j = 1, \ldots, n\}$, let $\{row\ i^*, column\ j^*\}$ be a pair of strategies adopted by the players. Then, if the pair of inequalities

$$a_{i^*j} \leq a_{i^*j^*} \leq a_{ij^*}, \tag{4.11}$$

is satisfied $\forall i, j$. The two–person zero–sum game is said to have a saddle point in pure strategies. The strategies {row i^*, column j^*} are said to constitute a saddle–point equilibrium. Or simply, they are said to be the saddle–point strategies. The corresponding outcome $a_{i^*j^*}$ of the game is called the saddle–point value. If a two–person zero–sun game possesses a single saddle point, the value of the game is uniquely given by the value of saddle point. However, the mixed strategies are used to obtain an equilibrium solution in the matrix games that do not possess a saddle point in pure strategies. A mixed strategy for a player is a probability distribution on the space of its pure strategies. Given an $(m \times n)$ matrix game $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m; j = 1, \ldots, n\}$, the frequencies with which different rows and columns of the matrix are chosen by the defender and the attacker will converge to their respective probability distributions that characterize the strategies. In this way, the average value of the outcome of the game is equal to

$$J(\mathbf{y}, \mathbf{w}) = \sum_{i=1}^{m} \sum_{j=1}^{n} y_i a_{ij} w_j = \mathbf{y}' \mathbf{A} \mathbf{w}, \tag{4.12}$$

where $\mathbf{y}$ and $\mathbf{w}$ are the probability distribution vectors defined by

$$\mathbf{y} = (y_1, \cdots, y_m)', \quad \mathbf{w} = (w_1, \cdots, w_n)'. \tag{4.13}$$

The defender wants to minimize $J(\mathbf{y}, \mathbf{w})$ by an optimum choice of a probability distribution vector $\mathbf{y} \in Y$, while the attacker wants to maximize the same quantity by choosing an appropriate $\mathbf{w} \in W$. The sets Y and W are

$$Y = \{\mathbf{y} \in R^m : \mathbf{y} \geq \mathbf{0}, \quad \sum_{i=1}^{m} y_i = 1\}, \tag{4.14}$$

$$W = \{\mathbf{w} \in R^n : \mathbf{w} \geq \mathbf{0}, \quad \sum_{j=1}^{n} w_j = 1\}. \tag{4.15}$$

Given an $(m \times n)$ matrix game $\mathbf{A}$, a vector $\mathbf{y}^*$ is known as a mixed security strategy for the defender if the following inequality holds $\forall \mathbf{y} \in Y$:

$$\overline{V}_m(\mathbf{A}) \triangleq \max_{\mathbf{w} \in W} \mathbf{y}^{*\prime} \mathbf{A} \mathbf{w} \leq \max_{\mathbf{w} \in W} \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \mathbf{y} \in Y. \tag{4.16}$$

And the quantity $\overline{V}_m(\mathbf{A})$ is known as the average security level of the defender. We can also define the average security level of the attacker as $\underline{V}_m(\mathbf{A})$ if the following inequality holds for all $\mathbf{w} \in W$:

$$\underline{V}_m(\mathbf{A}) \triangleq \min_{\mathbf{y} \in Y} \mathbf{y}' \mathbf{A} \mathbf{w}^* \geq \min_{\mathbf{y} \in Y} \mathbf{y}' \mathbf{A} \mathbf{w}, \quad \mathbf{w} \in W. \tag{4.17}$$

The two inequalities can also be given as:

$$\overline{V}_m(\mathbf{A}) = \min_{Y} \max_{W} \mathbf{y}' \mathbf{A} \mathbf{w}, \tag{4.18}$$

$$\underline{V}_m(\mathbf{A}) = \max_{W} \min_{Y} \mathbf{y}' \mathbf{A} \mathbf{w}. \tag{4.19}$$

However, it always holds true that $\underline{V}_m(\mathbf{A}) = \overline{V}_m(\mathbf{A})$ for a two-person zero-sum game in the mixed strategies. In this way, for an $(m \times n)$ matrix game $\mathbf{A}$, $\mathbf{A}$ has a saddle point in the mixed strategies, and $V_m(\mathbf{A})$ is uniquely given by

$$V_m(\mathbf{A}) = \overline{V}_m(\mathbf{A}) = \underline{V}_m(\mathbf{A}). \tag{4.20}$$

We can see that if the players are able to use mixed strategies, the matrix games always have a saddle-point solution $V_m(\mathbf{A})$ as the only solution in the zero-sum two-person game.

4.4.3 Computation of a two-Person zero-sum game

One way to get the saddle point in the mixed strategies is to convert the original matrix game into a linear programming (LP) problem. Given $\mathbf{A} = \{a_{ij} : i = 1, \ldots, m; j = 1, \ldots, n\}$ with all entries positive $(i.e., a_{ij} > 0)$, the average value of the game in mixed strategies is given by

$$V_m(\mathbf{A}) = \min_Y \max_W \mathbf{y}'\mathbf{A}\mathbf{w} = \max_W \min_Y \mathbf{y}'\mathbf{A}\mathbf{w}. \tag{4.21}$$

Obviously, $V_m(\mathbf{A})$ must be a positive quantity on $\mathbf{A}$. Furthermore, the expression can also be written as

$$\min_{\mathbf{y}\in Y} v_1(\mathbf{y}), \tag{4.22}$$

where $v_1(\mathbf{y})$ is defined as

$$v_1(\mathbf{y}) = \max_W \mathbf{y}'\mathbf{A}\mathbf{w} \geq \mathbf{y}'\mathbf{A}\mathbf{w}, \quad \forall \mathbf{w} \in W. \tag{4.23}$$

In addition, it can also be written as

$$\mathbf{A}'\mathbf{y} \leq \mathbf{1_n} v_1(\mathbf{y}), \quad \mathbf{1_n} \triangleq (1, \ldots, 1)' \in R^n. \tag{4.24}$$

Now the mixed security strategy for the defender is to

$$\min \ v_1(\mathbf{y}) \tag{4.25}$$

$$\text{s.t.} \begin{cases} A'\tilde{\mathbf{y}} \leq \mathbf{1_n}, \\ \tilde{\mathbf{y}}'\mathbf{1_m} = [v_1(\mathbf{y})]^{-1}, \\ \mathbf{y} = \tilde{\mathbf{y}} v_1(\mathbf{y}) \\ \tilde{\mathbf{y}} \geq 0, \end{cases}$$

where $\tilde{\mathbf{y}}$ is defined as $\mathbf{y}/v_1(\mathbf{y})$. This is further equivalent to the maximization problem

$$\max_{\tilde{\mathbf{y}}} \ \tilde{\mathbf{y}}'\mathbf{1_m}, \tag{4.26}$$

$$\text{s.t.} \begin{cases} \mathbf{A}'\tilde{\mathbf{y}} \leq \mathbf{1_n}, \\ \tilde{\mathbf{y}} \geq 0, \end{cases}$$

which is a standard LP problem.

Similarly, we can get the standard LP problem for the attacker

$$\min_{\tilde{\mathbf{w}}} \ \tilde{\mathbf{w}}'\mathbf{1_n}, \tag{4.27}$$

$$\text{s.t.} \begin{cases} \mathbf{A}\tilde{\mathbf{w}} \geq \mathbf{1_m}, \\ \tilde{\mathbf{w}} \geq 0, \end{cases}$$

where $\tilde{\mathbf{w}}$ is defined as $\mathbf{w}/v_2(\mathbf{w})$ and

$$v_2 \triangleq \min_{Y} \mathbf{y}'\mathbf{A}\mathbf{w} \leq \mathbf{y}'\mathbf{A}\mathbf{w}, \quad \forall \mathbf{y} \in Y. \tag{4.28}$$

4.5 Numerical Results

In this section, we analyze the effect of attack on the PJM 5-bus test system in [86] with a slightly modifications. Transmission lines' parameters are given in Table 3.2 and 3.3. Generators' and loads' parameters (including G_i^{max}, C_i, and D_i) together with the location of measurements are shown in Figure 4.1. Solving (2.2) for the day–ahead market shows that L_{54} (line from B_5 to B_4) is congested. Here attacker chooses L_{54} to attack. Knowing H, from (4.4) the attacker obtains $\mathbf{Q} = [0.2\ 0.05\ 0\ 0.19\ 0.25\ 0.04\ -0.04\ -0.08\ -0.13\ 0.18\ 0.05]$. Positive and negative arrays of this vector correspond to z_+ and z_- vectors, respectively, i.e., $z_+^T = [z_1, z_2, z_4, z_5, z_6, z_{10}]$ and $z_-^T = [z_7, z_8, z_9]$. The greater values of $Q(i)$ correspond to measurements that have more effect on $\hat{P}_{ij}$. Suppose there are 4 insecure measurements $\{z_1, z_4, z_5, z_{10}\}$ and the attacker can compromise 2 of them, also the defender can defend 2 measurements simultaneously. So the attacker should choose 2 measurements among these measurements that have more effect on $\hat{P}_{ij}$ and a sufficiently low probability of detection by the defender. In this example, the attacker can choose from strategy set $\mathcal{S}_1 = \{z_1z_4, z_1z_5, z_1z_3, z_4z_5, z_4z_3, z_5z_3\}$, and the defender can choose

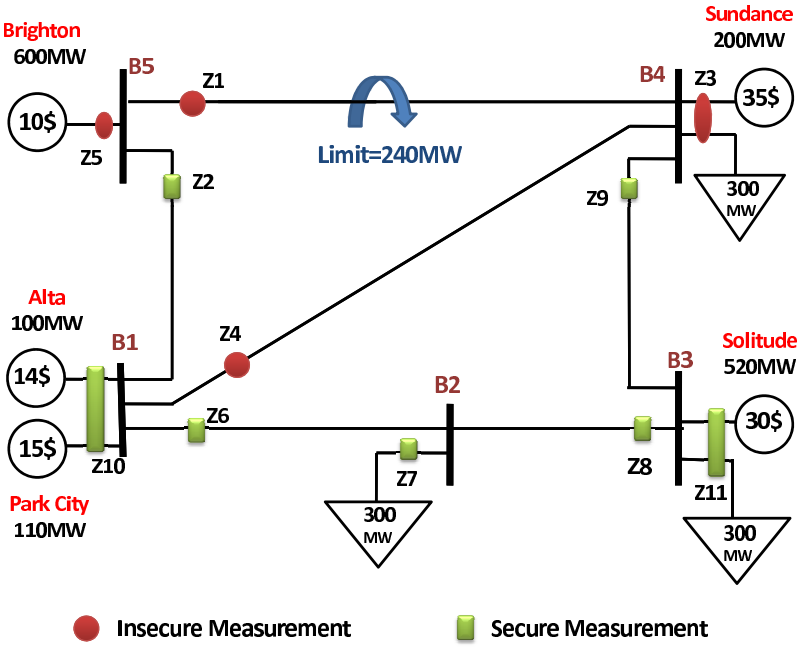


Figure 4.1 Measurement configuration in PJM 5-bus test system.

from strategy set $\mathcal{S}_2 = \{z_1z_5, z_1z_3, z_4z_5, z_4z_3, z_5z_3\}$. It is assumed that if the attacker for example chooses $\{z_iz_j\}$ (to attack measurement i and j, $i \neq j$) and the defender chooses $\{z_iz_k\}$ (to defend measurement i and k, $i \neq k$), compromising $\{z_j\}$ will be successful, and the change in $\hat{P}_{ij}$ is only because of compromising $\{z_j\}$. If $\xi = [5_{MW}, \cdots, 5_{MW}]'_{(12\times1)}$, solving (4.8) and (4.9) gives $\Delta\hat{P}_{54} = U_1 = -U_2$. As Figure 4.2 shows, these payoffs are the results of different attack and defend strategies (which both players take). The attacker and defender in this game are not aware of the sequence of play. Also one player has no idea about the other player's action. These situations are described by a normal form zero–sum game in Table 4.1.

Table 4.1 shows that $\min(\max_{row}) = 3.21$, which is not equal to $\max(\min_{column}) = 0$. So there is no $a_{i^*j^*}$ that satisfies (4.11). Therefore, the game doesn't have a single saddle point and the problem shifts to finding the proportion of times that the attacker and the defender, play their own strategies. Solving such a game (which does not have a single saddle point)

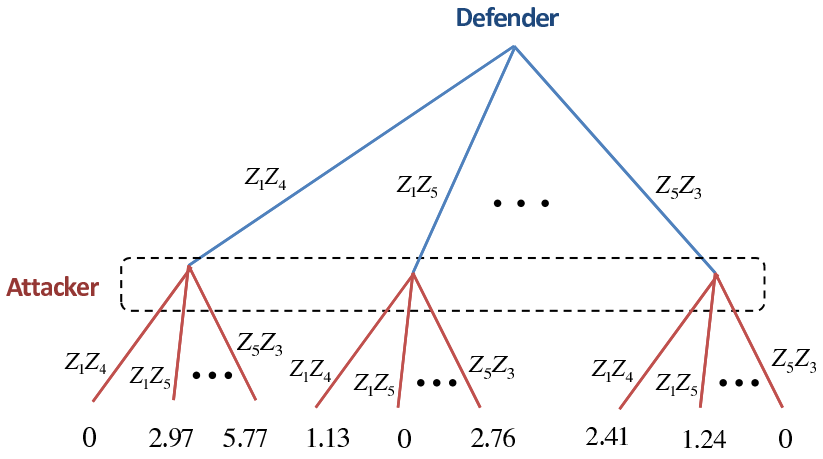


Figure 4.2 Extensive form of single–act game.

Table 4.1 Zero–sum game between the Attacker and the Defender

		w_1	w_2	w_3	w_4	w_5	w_6
	Att. / Def.	z_1z_4	z_1z_5	z_1z_{10}	z_4z_5	z_4z_{10}	z_5z_{10}
y_1	z_1z_4	0	3.14	2.81	3.14	2.81	4.84
y_2	z_1z_5	1.17	0	2.81	1.17	5	2.81
y_3	z_1z_{10}	1.17	3.14	0	5	1.17	3.14
y_4	z_4z_5	1.28	1.28	4.43	0	2.81	2.81
y_5	z_4z_{10}	1.28	5.35	1.28	3.14	0	3.14
y_6	z_5z_{10}	3.21	1.28	1.28	1.17	1.17	0

is a linear programming. From (4.26) defender defines $\tilde{\mathbf{y}}$, we have

$$\max \quad \tilde{\mathbf{y}}'\mathbf{1_m}, \tag{4.29}$$

$$\text{s.t.} \begin{cases} 1.17\tilde{y}_2 + 1.17\tilde{y}_3 + 1.28\tilde{y}_4 + 1.28\tilde{y}_5 + 3.2\tilde{y}_6 \le 1, \\ 3.14\tilde{y}_1 + 3.14\tilde{y}_3 + 1.28\tilde{y}_4 + 5.35\tilde{y}_5 + 1.28\tilde{y}_6 \le 1, \\ 2.81\tilde{y}_1 + 2.81\tilde{y}_2 + 4.43\tilde{y}_4 + 1.28\tilde{y}_5 + 1.28\tilde{y}_6 \le 1, \\ 3.14\tilde{y}_1 + 1.17\tilde{y}_2 + 5\tilde{y}_3 + 3.14\tilde{y}_5 + 1.17\tilde{y}_6 \le 1, \\ 2.81\tilde{y}_1 + 5\tilde{y}_2 + 1.17\tilde{y}_3 + 2.81\tilde{y}_4 + 1.17\tilde{y}_6 \le 1, \\ 4.84\tilde{y}_1 + 2.81\tilde{y}_2 + 3.14\tilde{y}_3 + 2.81\tilde{y}_4 + 3.14\tilde{y}_5 \le 1, \\ \tilde{y}_1, \tilde{y}_2, \tilde{y}_3, \tilde{y}_4, \tilde{y}_5, \tilde{y}_6 \ge 0, \end{cases}$$

which gives $\tilde{\mathbf{y}} = [0\, 0.049\, 0.134\, 0.136\, 0.018\, 0.183]$. Therefore, $\mathbf{y} = \tilde{\mathbf{y}} v_1(\mathbf{y}) = \tilde{\mathbf{y}}(\tilde{\mathbf{y}}'\mathbf{1_m})^{-1} = [0\ 0.094\ 0.26\ 0.262\ 0.0347\ 0.35]$. Similarly, solving (4.27) for the attacker gives $\tilde{\mathbf{w}} =$

$[0.29\ 0\ 0.02\ 0.019\ 0.019\ 0.174]$, and therefore, $\mathbf{w} = \tilde{\mathbf{w}} v_1(\mathbf{w}) = \tilde{\mathbf{w}}(\tilde{\mathbf{w}}'\mathbf{1_m})^{-1}$
$= [0.556\ 0\ 0.038\ 0.036\ 0.037\ 0.333]$.

Figure 4.4 shows the proportion of times that the defender and the attacker should defend and attack different measurements, respectively. As discussed in Section 4.3, changing the estimated transmitted power in line L_{54} can change the prices in either bus 5 or bus 4. In real–time market the control center estimates transmitted power and then knowing dispatch schedule (which is defined in day–ahead market) load level in different buses is estimated. This estimated load together with the current state of the network is applied to a DCOPF, and this program defines the real–time prices. If the operating condition (such as the load level) has not changed and there is no error in the measurements, the real–time prices should be the same as the day–ahead prices. Here without loss of generality, we assume that the actual load level doesn't change and any change in the estimated load level is because of bad data injection to the state estimator.

The following example shows how attacker is able to change the prices in real–time market. Suppose attacker compromise $z_1 z_4$ and the defender defends $z_5 z_{10}$ so, attack against $z_1 z_4$ is successful. In this case solving (4.8) gives $\mathbf{z^a} = [8.21\ 0\ 0\ 8.09\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]_{(MW)}$. So from (1.8), estimated states for all buses will be $\hat{\theta} = [50\ 56\ 65\ 01\ 71.6] \times 10^{-3}_{(rad)}$. Using (4.4), estimated transmitted power can be obtained[6] $\hat{P_{54}} = 236.59_{(MW)}$. This power is less than thermal limit of transmission line that shows, congestion in this line is released. In this case solving (2.10) and (2.15) gives the real time prices (here it is assumed that $\Delta G_i^{max} = -\Delta G_i^{min} = 0.1_{MW}$ and $\Delta D_i^{max} = -\Delta D_i^{min} = 0_{MW}$).

Figure 4.3 shows the prices for attacked and without–attack cases. Change of estimated transmitted power in transmission line is shown in Figure 4.5. Now, assume that in day–ahead market, the attacker buys 100_{MW} power in bus 5 and sells it in bus 4. From

[6]This value is considered as the real–time transmitted power in L_{54}.

(4.10), the profit of this contract will be:

$$Profit = [(35 - 20) - (30 - 30)] \times 100 = 1500_{(\$/h)}. \tag{4.30}$$

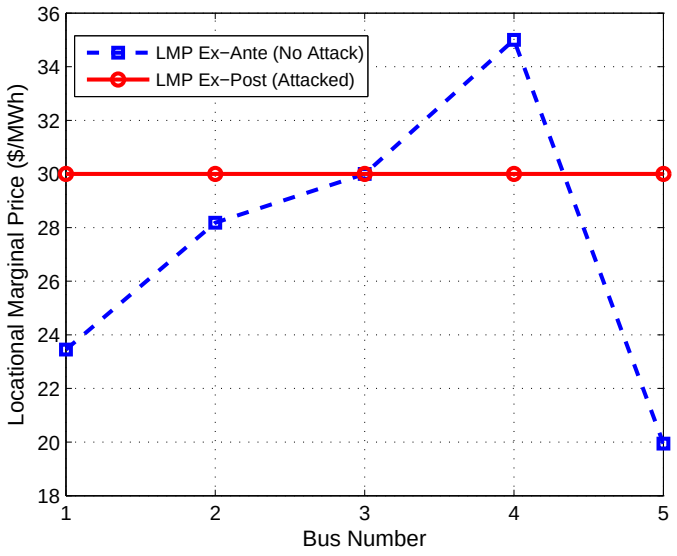
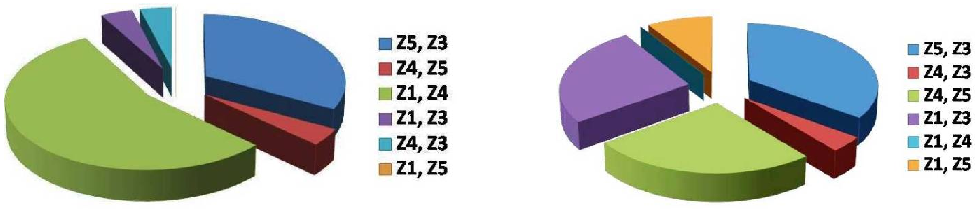


Figure 4.3 Locational marginal prices for PJM 5-Bus test system for both with attack and without attack.

4.6 Conclusion

In this chapter, first we analyzed the effect of compromising each measurement on the state estimator results. Compromising these measurements can change the congestion and consequently the price of electricity, and thus, the attacker has an intensive to change



(a) Probability of attack (b) Probability of defend

Figure 4.4 Proportion of times that attacker and defender, attack and defend to measurements respectively.

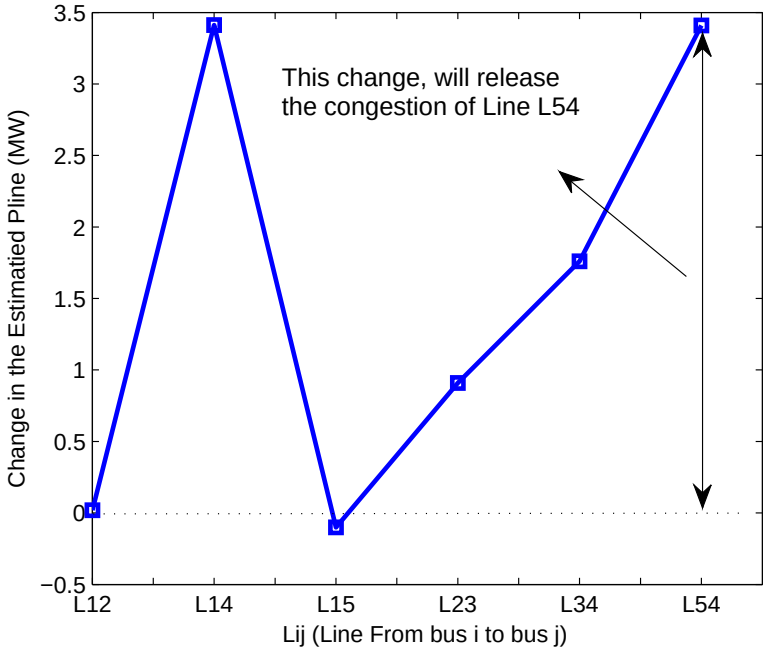


Figure 4.5 Change in the estimated transmitted power of lines because of attack to Z_1 and Z_4.

the congestion in the desired direction. Since a typical power system has a huge number of measurements, attacking or defending all of those becomes impossible for attacker and defender, respectively. To this end, this behavior is modeled and analyzed in the framework of game theory. The simulation results on PJM 5–Bus test system indicate that, in the specified load level, how attacker can change the prices in the desired direction (decreasing in this example).

Chapter 5

Detecting Stealthy False Data Injection using Machine Learning in Smart Grid

5.1 Introduction

For many engineering and science problems, there is no direct mathematical solution. Learning techniques have been used extensively to overcome this problem. Researchers in different fields try to develop algorithms that learn the behavior of the given problem using historical data [87], [88], [89]. Machine learning usually is used to establish relationships between multiple features of the data sets and can be used in different applications such as prediction, clustering and detection of anomaly behavior in the data set. Learning methods are divided into two groups, supervised on unsupervised. In supervised learning each observation (time samples of data set) has an output label that is used to learn the relation between features [90, 91]. In unsupervised learning, only time instances (observations) of different features are available. Having only observations, unsupervised techniques try to discover new properties and classes in the data set [92, 93].

In this chapter, we use both supervised and unsupervised[1] learning methods to distinguish the attacked and the safe operating modes in state estimation. To do so, in Section 5.2 we first discuss state estimation and bad data detection problem. In Section 5.3 we illustrate two different machine learning algorithms and the way that they can be utilized to detect the bad data will be described. Numerical result in Section 5.4 shows the effectiveness of our learning techniques. Conclusion in Section 5.5 closes this chapter. For the sake of clarity, some important notations are listed in Table 5.1.

[1]In order to compare the performance with supervised learning technique, we are indeed using semi-supervised method in this chapter. Output labels are used to learn the best performance in the unsupervised learning method, but in the case that the output labels are not available, (losing some performance) unsupervised technique can be used instead.

Table 5.1 Machine learning notations

P_{ij}	Transmitted power from bus i to bus j
$\boldsymbol{\theta}$	$n \times 1$ vector of voltage angles
X_{ij}	Line reactance between bus i and bus j
$\mathbf{H}$	$m \times n$ Jacobian matrix
m	Number of measurements
n	Number of states (number of buses here)
$\mathbf{r}$	$m \times 1$ residue vector for BDD
γ	Residue threshold in BDD
$\mathbf{\Sigma}_e$	$m \times n$ covariance matrix of measurements' errors
$\mathbf{z}'$	$m \times 1$ attacked measurement vector
$\mathbf{Z_t}$	Measurement sets over m different time steps
$\mathbf{Z_{tr}}$	$m \times k$ reduced measurement matrix
$\boldsymbol{\varphi}$	SVM optimization parameter
$\mathbf{f^{(i)}}$	Similarity function for i^{th} sample
F_1	Metric for evaluating the performance of clustering algorithms
ξ	Threshold for Anomaly Detection algorithm

5.2 System Model

As described in Section 1.3.2, the state-estimation problem is to estimate n phase angles θ_i's, by observing m real-time measurements. In Section 1.3.2 we showed that if phase difference is small, the relation between measurements and states can be approximated with $\mathbf{z} = \mathbf{P}(\boldsymbol{\theta}) + \mathbf{e}$, where $\mathbf{z} = [z_1, \cdots, z_m]^T$ is the vector of the measured active power in transmission lines. These measurements can be either transmitted active power from bus i to bus j (P_{ij}), or injected active power to bus i ($P_i = \sum_j P_{ij}$). $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n]^T$ is the state vector and $\mathbf{e} = [e_1, \ldots, e_n]^T$ is the measurements error vector. Note that $\mathbf{H}$ is unknown to the attackers but known to the ISO.

5.2.1 Bad data detection in linear state estimation

Given the power flow measurements $\mathbf{z}$, the least square estimated state $\hat{\boldsymbol{\theta}}$ can be computed as:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{z} = \mathbf{M}\mathbf{z}, \tag{5.1}$$

where $\mathbf{M} = \mathbf{H}(\mathbf{H}^T\mathbf{\Sigma}_e^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{\Sigma}_e^{-1}$. The difference between the measured quality and the calculated value from the estimated state is called the residue vector $\mathbf{r}$, and can be computed as the: $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}$. Therefore, the expected value and the covariance of the residual are:

$$E(\mathbf{r}) = 0 \text{ and } cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\mathbf{\Sigma}_e. \tag{5.2}$$

False data detection due to faulty sensors or topological errors can be performed using a threshold test [81]. The hypothesis of not being attacked is accepted if

$$\max_i |r_i| \leq \gamma, \tag{5.3}$$

where γ is the threshold and r_i is the i^{th} component of $\mathbf{r}$.

5.3 Machine Learning Based Bad Data Detection

In the previous section, we have showed that stealth bad data can pass the traditional BDD. In this section, we devise two machine learning based techniques to detect stealthy attacks. The key observation that motivates our solution approach is that normal data and tampered data (due to attacks) tend to be separated in certain projected space. When the class labels (normal vs tampered) are given in the historical data, we can train a classifier to identify attacks. On the other hand, when labels are not given, we will apply anomaly detection to identify the outliers as potential attacks. In both schemes, one main challenge is the curse of dimensionally, namely, as the size of the power grid grows, the dimension of the measurement data grows rendering high computation complexity. We use principle component analysis (PCA) to first reduce the dimension of measurements and then apply the proposed classification/detection techniques. PCA maps the data from the original domain to a new domain. Attacked data in the new domain are more handleable than the original domain because the data are not correlated anymore.

5.3.1 Principle component analysis

Most of the practical systems such as power networks have complex structure, thus understanding their dynamics is very challenging in some cases. One interesting way of analyzing these dynamics is to first use redundant measurements in the network, and then use PCA to extract the interest dynamics of the system. PCA is a well known method, so we just briefly bring the concept and formulation here. Mathematically, PCA maps the data from n dimensional space to r dimensional space (5.6) where $r \leqslant n$. The data in the new domain have two important properties: 1) different dimensions of the data have no correlation anymore 2) the dimensions are ordered based on the importance of their information. The following equations are used to map the $m \times n$ measurement matrix $\mathbf{Z_t}$ to an $m \times r$ dimension matrix $\mathbf{Z_{tr}}$ [94],

$$\beth = \frac{1}{m} \times \mathbf{Z_t^T} \times \mathbf{Z_t}, \tag{5.4}$$

$$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = svd(\beth), \tag{5.5}$$

$$\mathbf{Z_{tr}} = \mathbf{U}(:, 1:r)^T \times \mathbf{Z_t}, \tag{5.6}$$

where $\mathbf{Z_t} = [\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(m)}]^T$ is the matrix containing measurement sets over m different time steps. $\mathbf{S}$ is a diagonal matrix with nonnegative diagonal elements in a decreasing order. Matrices $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices that satisfy $\beth = \mathbf{USV}^T$. svd is a function for computing singular value decomposition. S_{ii} is the eigenvalue of i^{th} feature where the bigger S_{ii} is, the more information i^{th} feature has[2]. Indeed in many correlated systems (such as power grids), only first few components of S are significant. It is common to select the smallest value of r such that the following condition holds,

$$\frac{\sum_{i=1}^{r} S_{ii}}{\sum_{i=1}^{m} S_{ii}} \times 100 \geq \varepsilon, \tag{5.7}$$

[2]Statistically, direction with the highest variation is the most important direction because it can represent the best approximation of the data in lower dimensions (direction with highest variation, has the most important information among other directions inside the data).

namely $\varepsilon\%$ of variance is retained. After mapping the features to the low dimensional space in (5.6), the control center can use efficient machine learning techniques to determine the boundary between normal and tampered data (in the sequel).

5.3.2 Support vector machines

To classify the measurements as under either "safe" or "under-attack", we propose to utilize the Support Vector Machine (SVM) [95]. SVM is a solution to find a hyperplane that serves as a decision boundary to separate two sets of observations. A non–linear decision boundary can be defined by solving the following optimization problem,

$$\min_{\boldsymbol{\varphi}} \; C\sum_{i=1}^{m}[y^{(i)}cost_1(\boldsymbol{\varphi}^T\mathbf{f}^{(i)}) + (1-y^{(i)})cost_0(\boldsymbol{\varphi}^T\mathbf{f}^{(i)})]$$

$$+ 1/2\sum_{j=1}^{n}\varphi_j^2, \tag{5.8}$$

where C is a weighting parameter that controls the complexity of the fitted decision boundary[3]. $y^{(i)}$ is a binary variable and indicates the label of the i^{th} operating points in the historical data with $y_i = 0$ for non-attack and $y^{(i)}$=1 for safe mode. $cost_1$ and $cost_0$ are cost functions defined respectively,

(5.9)

$$cost_1\text{=} \begin{cases} 0 & \boldsymbol{\varphi}^T\mathbf{f}^{(i)} \geq 1, \\ 1-\boldsymbol{\varphi}^T\mathbf{f}^{(i)} & \boldsymbol{\varphi}^T\mathbf{f}^{(i)} < 1, \end{cases}$$

(5.10)

$$cost_0\text{=} \begin{cases} 0 & \boldsymbol{\varphi}^T\mathbf{f}^{(i)} \leq -1, \\ \boldsymbol{\varphi}^T\mathbf{f}^{(i)}+1 & \boldsymbol{\varphi}^T\mathbf{f}^{(i)} > -1. \end{cases}$$

[3]A large value of C decreases the effect of the regularizing term in (5.8) ($1/2\sum_{i=1}^{n}\varphi_j^2$) and the optimization problem fits a complex boundary to the learning data sets. This complex boundary fails to generalize the clustering of new data sets which are not in the training data set (high variance problem). A small value of C increases the effect of regularizing term and fits a simple decision boundary that can not efficiently separate the positive and negative hypothesis (High bias).

$\boldsymbol{\varphi}^T = [\varphi_0, \varphi_1, \cdots, \varphi_m]$ is the optimization parameter and defines the decision boundary. $\mathbf{f^{(i)}} = [1, f_1^{(i)}, \cdots, f_m^{(i)}]$ is a vector containing similarity functions for the i^{th} sample point. In this chapter, we use the Gaussian kernel for the similarity function,

$$f_m^{(i)} = exp(-\frac{\|\mathbf{z}_{tr}^{(i)} - \mathbf{l}^{(m)}\|^2}{2\sigma^2}), \tag{5.11}$$

where $\mathbf{l}^{(m)}$ is the m^{th} landmark. The landmarks can be placed randomly in the historical data set space. σ is another parameter that can be used for changing the complexity of the decision boundary. Optimal choice for σ and C can improve the efficiency of SVM in detecting the attacked mode for cross validation set[4]. In order to define the optimal choice for σ and C, we vary both and choose the best σ and C, which correspond to the largest accuracy. In this chapter, we use F_1 score as the measure of accuracy, i.e.,

$$F_1 = 2\frac{P_r \times R_e}{P_r + R_e}, \tag{5.12}$$

where P_r and R_e are called precision and recall, respectively, and they are calculated using the following equations,

$$P_r = \frac{True\ Positive}{Predicted\ Positive},\ R_e = \frac{True\ Positive}{Actual\ Positive}, \tag{5.13}$$

where true positive corresponds to the points that the algorithm detects as positive samples and they are indeed positive ones. Predictive positives are the points that algorithm detects as positive points but it may have errors. Actual positive are all positive points in the data sets. $F1$ score is no greater than 1, and the bigger the value of $F1$, the more accurate the classifier in general. Algorithm 2 describes the procedure to detect stealth false data injection using the SVM method.

[4]In this chapter we have used 70% of the historical data as learning data set and we have tested the accuracy of the fitted decision boundary on the 30% of the remaining data sets called cross validation data sets.

Algorithm 2: Stealth false data detection using SVM

1 Collect historical data from state estimator
$\mathbf{Z_t} = [\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(m)}]^T$;

2 Use PCA:
$\beth = \frac{1}{m} \times \mathbf{Z_t^T} \times \mathbf{Z_t}$;
$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = svd(\beth)$;
$\mathbf{Z_{tr}} = \mathbf{U}(:, 1:k)^T \times \mathbf{Z_t}$;

3 Choose the best C and σ
for $w = 1, \ldots, W$ **do**
  $C = C + \triangle C$;
  for $b = 1, \ldots, B$ **do**
    $\sigma = \sigma + \triangle \sigma$;
    Define $\boldsymbol{\varphi}$ from (5.8) for the learning data set
    Define F_1 from (5.12) for the validation data set
    if $F_1 > F_1^{best}$ **then**
      $F_1^{best} \leftarrow F_1$;
      $\boldsymbol{\varphi}_{best} \leftarrow \boldsymbol{\varphi}$;
      exit
    end
  end

4 For the new operating point $\mathbf{Z^{new}}$

$$y^{(new)} = \begin{cases} 1 & \boldsymbol{\varphi}_{best}^T \mathbf{f}^{(i)} \geq 0, \quad (\mathbf{Z^{new}} \text{ is corrupted}) \\ 0 & \boldsymbol{\varphi}_{best}^T \mathbf{f}^{(i)} < 0. \quad (\mathbf{Z^{new}} \text{ is normal}) \end{cases}$$

.

5.3.3 Anomaly detection

In data mining, the data sets considerably different from the remainder of data are called outliers or anomalies. Different types of anomaly detection methods have been proposed such as the distance-based, model based, and statistical methods [96]. In this chapter, we use the statistical based methods. We use metric $P(\mathbf{z})$ and a threshold ξ, where $P(\mathbf{z})$ represents the statistical characteristics of the historical data. If $P(\mathbf{z}) \leq \xi$, then $\mathbf{z}$ statistically has low similarity to the remaining data. In this method, the hypothesis of anomaly is confirmed if $P(\mathbf{z}) \leq \xi$ and it is rejected if $P(\mathbf{z}) > \xi$. Threshold ξ will be learnt by the historical data[5] (Step 3. in Algorithm 3). We use the multivariate Gaussian distribution probability density function as the metric $P(\mathbf{z})$,

$$\mathbf{P}(\mathbf{Z}; \boldsymbol{\mu}, \boldsymbol{\Sigma}) = \frac{1}{(2\pi)^{\frac{n}{2}} |\boldsymbol{\Sigma}|^{0.5}} exp\left[-\frac{1}{2}(\mathbf{Z} - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1} (\mathbf{Z} - \boldsymbol{\mu})\right], \tag{5.14}$$

$$\boldsymbol{\mu} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{Z}^{(i)}, \quad \boldsymbol{\Sigma} = \frac{1}{m}\sum_{i=1}^{m} (\mathbf{Z}^{(i)} - \boldsymbol{\mu})(\mathbf{Z}^{(i)} - \boldsymbol{\mu})^T,$$

where n is the number of features, m is the number of samples and $P_i(z_i)$ is the probability density function (PDF) of feature i. Each feature z_i follows a certain distribution that should be fitted based on the historical data. It is worth mentioning that the assumption of independency for Z's holds for Gaussian distributed features because of using PCA[6]. Algorithm 3 shows the basic procedure of the anomaly detection method.

5.4 Numerical Results

In this section, we evaluate the effect of machine learning based techniques for detecting stealth attack in the state estimator. We use the IEEE 118–bus test system (Fig. 5.2). In order to simulate more realistic operation of the power system, we will use the stochastic loads in the network. Without loss of generality, these loads are considered to follow a

[5]Because of using labeled historical data to learn ξ_{Best}, this method in some literature is called semi–supervised learning method.

[6]PCA transforms a set of (possibly) correlated data into the linearly uncorrelated data.

Algorithm 3: Stealth false data detection using anomaly detection

1 Collect historical data from state estimator
$\mathbf{Z_t} = [\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(m)}]^T$;

2 Use PCA:
$\beth = \frac{1}{m} \times \mathbf{Z_t^T} \times \mathbf{Z_t}$;
$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = svd(\beth)$;
$\mathbf{Z_{tr}} = \mathbf{U}(:, 1:k)^T \times \mathbf{Z_t}$;

3 Fit density function $\mathbf{P}(\mathbf{Z}; \boldsymbol{\mu}, \boldsymbol{\Sigma})$ to the historical data $\mathbf{Z_t}$ using (5.14);

4 Choose the best ξ;
$\xi^{best} = 0,\ F_1^{best} = 0,$
for $\xi = min\mathbf{P}(\mathbf{Z_{val}}) : St : max\mathbf{P}(\mathbf{Z_{val}})$ **do**

$$\mathbf{Y_{pred}} = \begin{cases} \mathbf{Y_{pred}}(i) = 1, & \forall i, \quad P(Z_{val})(i) \leq \xi, \\ \mathbf{Y_{pred}}(i) = 0, & \forall i, \quad P(Z_{val})(i) > \xi, \end{cases}$$

$f_p = sum(\mathbf{Y_{pred}} == 1\ \&\ \mathbf{Y} == 0),$
$t_p = sum(\mathbf{Y_{pred}} == 1\ \&\ \mathbf{Y} == 1),$
$f_n = sum(\mathbf{Y_{pred}} == 0\ \&\ \mathbf{Y} == 1),$
$t_n = sum(\mathbf{Y_{pred}} == 0\ \&\ \mathbf{Y} == 0),$

$$F_1 = 2\frac{P_r \times R_e}{P_r + R_e}, \text{ where } \begin{cases} P_r = t_p/(t_p + f_p), \\ R_e = t_p/(t_p + f_n), \end{cases}$$

if $F_1 > F_1^{best}$ **then**
$F_1^{best} \leftarrow F_1\ \xi^{best} \leftarrow \xi$ exit
end

5 For the new operating point $\mathbf{Z^{new}}$

$$\text{If } P(\mathbf{Z^{new}}; \mu, \boldsymbol{\Sigma}) = \begin{cases} \leq \xi^{best} \dashrightarrow \mathbf{Z^{new}} \text{ is corrupted,} \\ > \xi^{best} \dashrightarrow \mathbf{Z^{new}} \text{ is normal.} \end{cases}$$

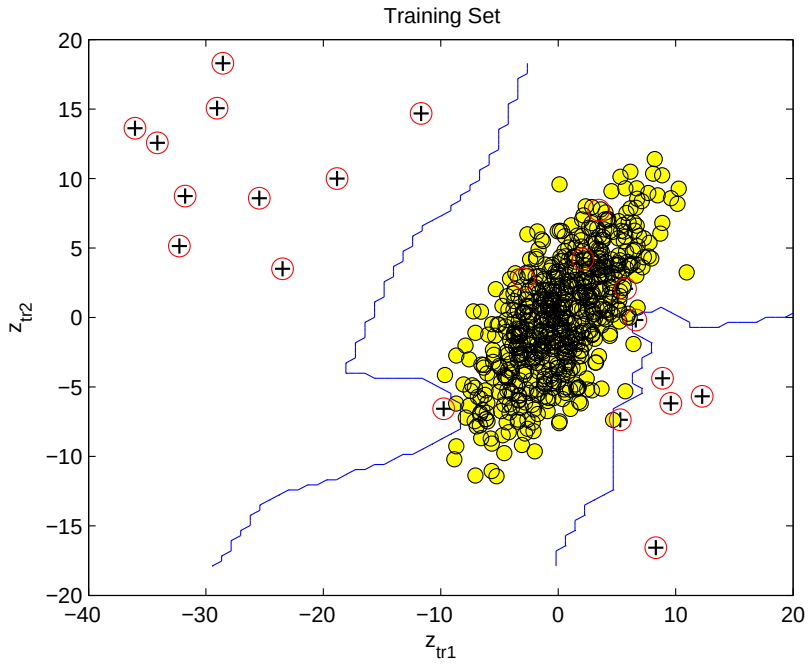


Figure 5.1 Attacked and safe operating modes in $\mathbb{R}^2$ space

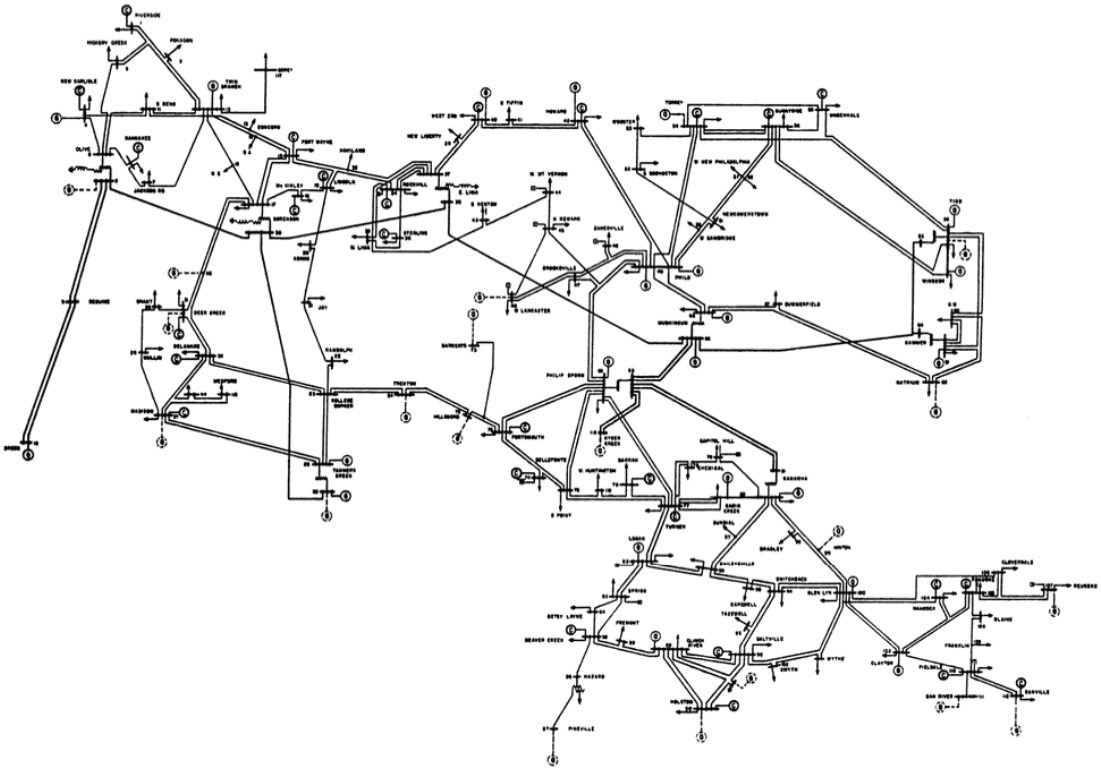


Figure 5.2 IEEE 118–Bus test system

uniform distribution in the range of $[0.9 \times L_0 - 1.1 \times L_0]$, where L_0 is the base load[7]. Here, we use matpower[8] to simulate the operation of the power network. In these simulations, active power measurements are collected from each transmission line. Thus, in the 118-bus case study there are 304 measurement features (one feature per transmission line). These measurements will be considered as inputs to the proposed algorithms. Due to the random nature of the load, the measurement vector varies over the time. Using the Monte-Carlo simulation we have recorded measurement vector in 1000 different instances[9]. As previously discussed, the measurements data are highly correlated and thus PCA is applied for dimension reduction. In the simulated data set, with only 2 principal components ($k = 2$), 99% of variance will be retained. Figure 5.1 shows a 2–dimensional plot of the principal components. This figure demonstrates that stealth attack is separable in the control center.

5.4.1 Support vector machine

To define the attacked and safe mode's boundary, we use a non-linear classifier with a Gaussian–kernel. Different values of C and σ have different effects on the clustering efficiency, so we train SVM with different C and σ and compute $F1$ for the cross validation set. Following Algorithm 2, we define the best choice for C and σ. Figure 5.3 shows F_1 score for different values of C and σ. Efficiency of the learning algorithm can be improved by increasing the number of learning data. In order to analyze the effect of increasing the number of learning data on detection performances, it is often useful to plot a learning curve. Figure 5.4 shows $F1$ values in both training and cross validation sets. This figure shows that, using enough training data, SVM is able to detect the stealth attack efficiently.

[7]The mean value of load in a specific period of time is often considered as L_0.

[8]matpower is a package of MATLAB M-files for solving power flow and optimal power flow problems [74].

[9]In the PJM (Pennsylvania, New Jersey, and Maryland) market, the control center collects the measured data in 1-minute time intervals and runs siemens state estimation program [72].

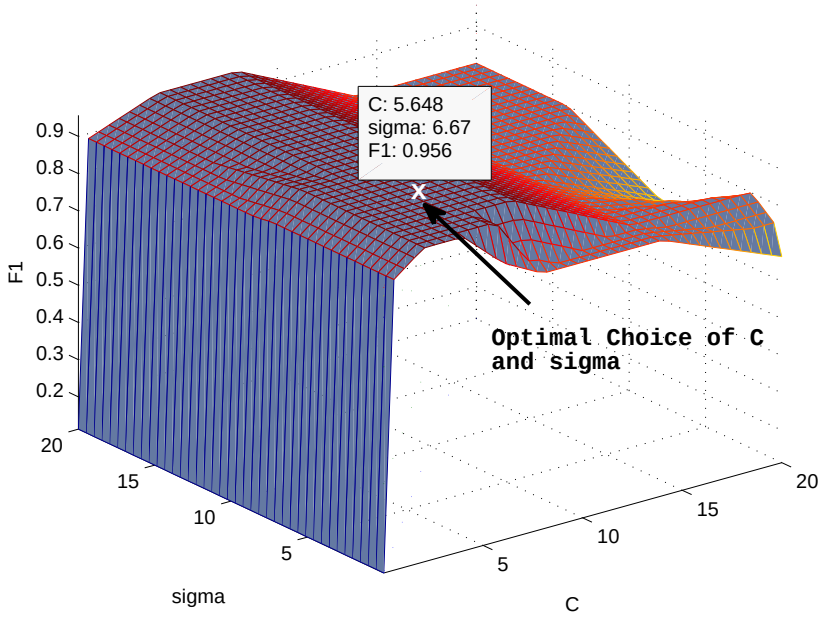


Figure 5.3 Optimal choice for C and sigma

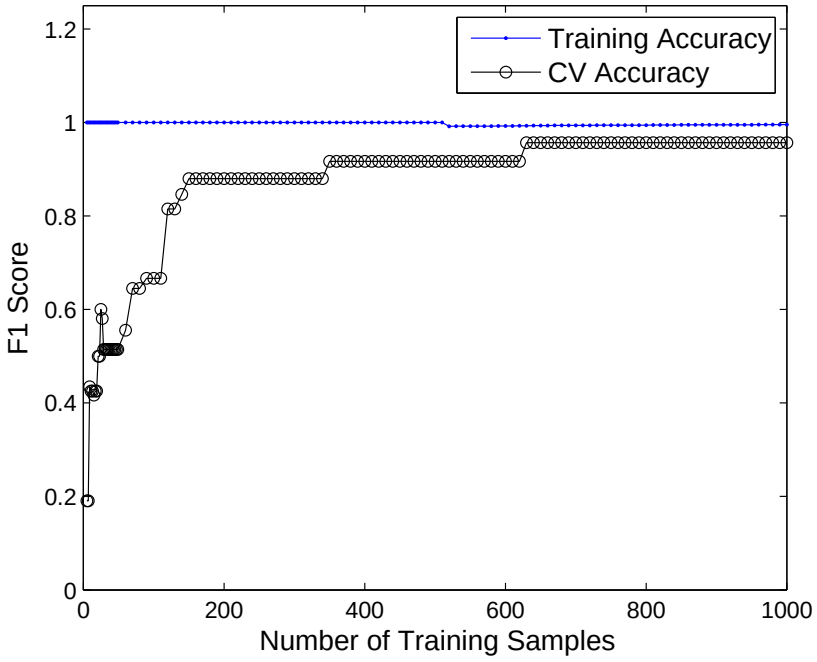


Figure 5.4 Learning curve of SVM

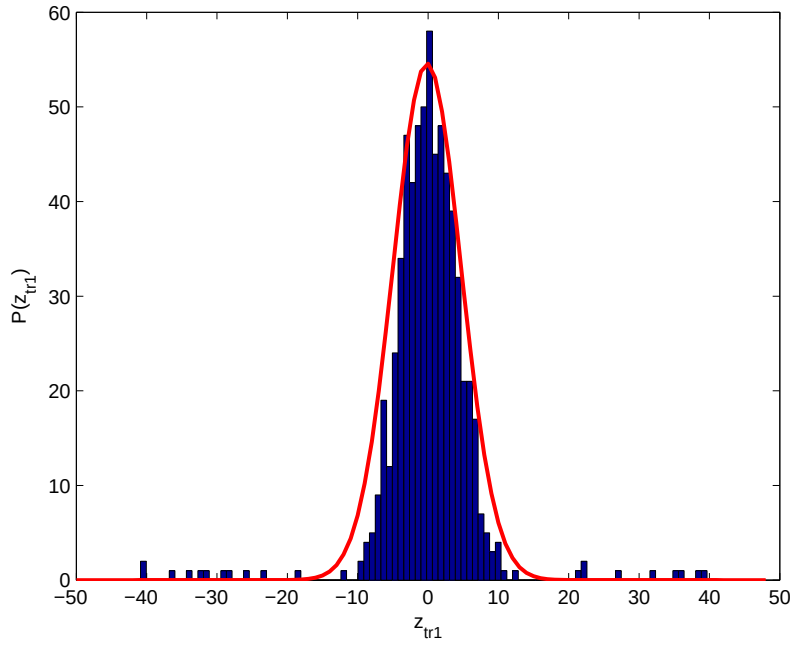


Figure 5.5 Histogram representation of $\mathbf{z_{tr1}}$

5.4.2 Anomaly detection

After applying PCA, the measurement data are mapped to points in $2D$. Figure 5.5 shows the histogram of the first feature. We fit a Gaussian probability density function to the features[10]. Following the procedure given in Algorithm 3, the anomaly points can be detected by applying a threshold ϵ. The sensitivity of detecting a point as anomaly, depends on the magnitude of threshold ξ. Figures 5.6, 5.7, and 5.8 show the detection sensitivity to different thresholds.

5.5 Conclusion

In this chapter, we first collect the normal and stealthily attacked operating points in the state estimator. We use collected data from active power flow measurements in the net-

[10]Results of anomaly detection on practical problems show that fitting the Gaussian density function for other data sets (which does not follow the Gaussian distribution) does not change the clustering efficiency drastically.

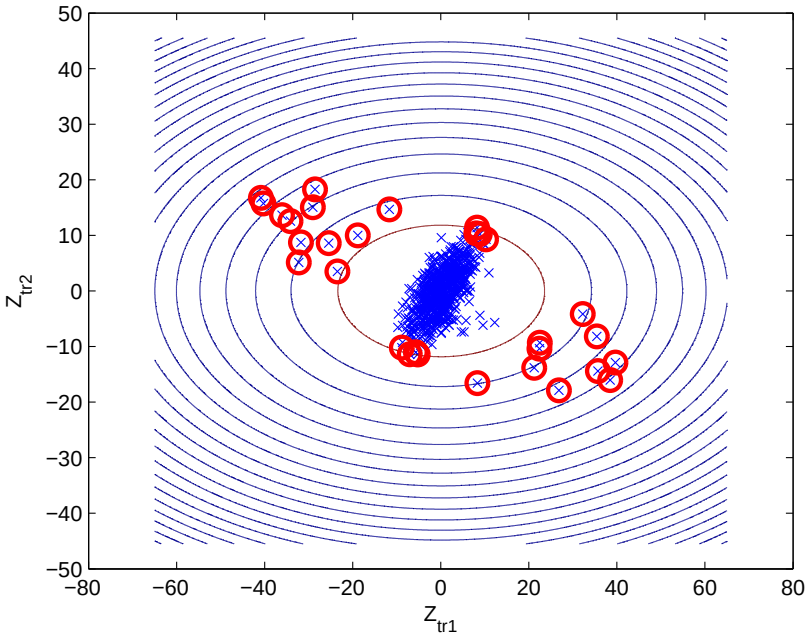


Figure 5.6 Anomaly detection with $P(\mathbf{z}) < 2e-4$

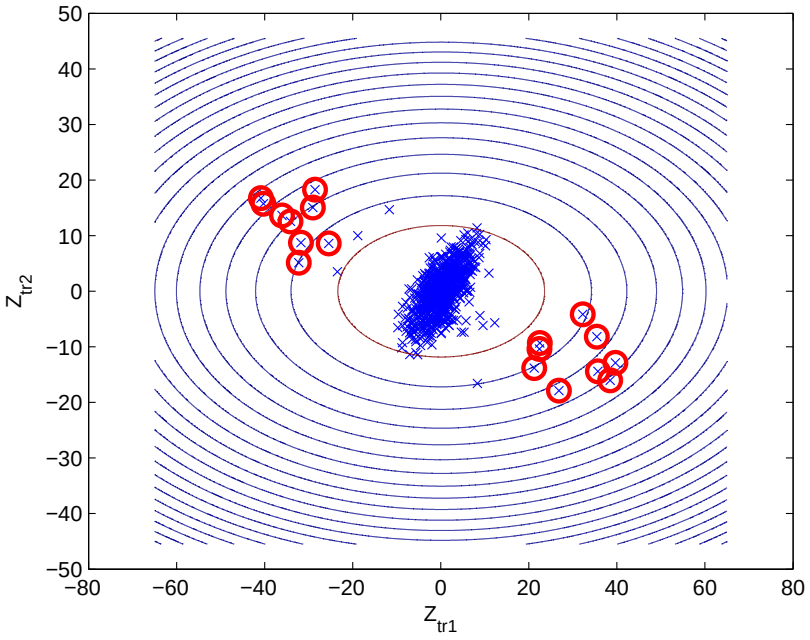


Figure 5.7 Anomaly detection with $P(\mathbf{z}) < 2.98e-5$

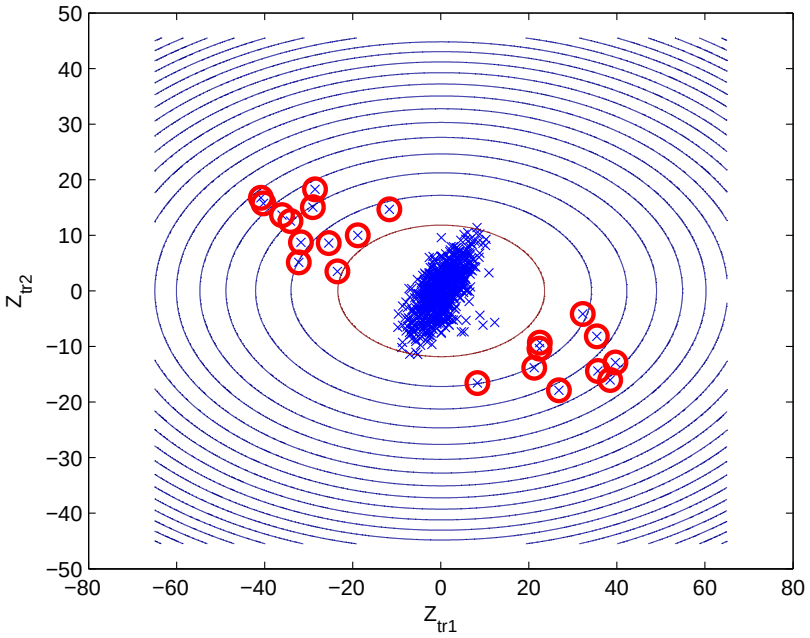


Figure 5.8 Anomaly detection with best choice of ξ

work as the learning (historical) data. Projecting the historical data into a low dimensional space shows that normal measurement data are well separated from data under attack. This fact shows that the machine learning algorithms can be applied to detect the stealth false data injection in the state estimator. We use both supervised and unsupervised[11] learning methods to distinguish the attacked and the safe operating modes. Numerical results shows the effectiveness of the proposed algorithms in detecting the stealth false data injection.

[11] In order to compare the performance with supervised learning technique, we are indeed using semi-supervised method in this chapter. Output labels are used to learn the best performance in the unsupervised learning method, but in the case that the output labels are not available, (losing some performance) unsupervised technique can be used instead.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this thesis, we analyzed the cyber attack against state estimation, from both attacker and defender points of views. We first reviewed the structure of electricity market, and then we presented the way that attacker alters the congestion in the ex–post market (in the desired direction) and makes financial profits. We investigated the case that the attackers without prior knowledge of the power grid topology, made inferences through phasor observations. The inferred structural information then used to launch stealth attacks. Attack formulated to change the price of electricity in the real-time market and the simulation results showed the effectiveness of attack in creating congestion and consequently changing the prices.

Then, we looked at the false data injection from defender point of view. Because of a huge number of measurements in the network, attacking and defending all measurements are impossible for the attacker and defender, respectively. This situation modeled as a zero-sum game between the attacker and defender, and we described how the interest of one party (attacker or defender) can influence the other's interest. The results of this game defined the proportion of times that the attacker and defender will attack and defend different measurements, respectively.

Finally, we illustrated how the normal operations of power networks can be statistically distinguished from the case under stealthy attacks. We first proposed two machine learning based techniques for stealthy attack detection. The first method utilized the supervised learning over labeled data and trained a support vector machine. The second method requires no labeled outputs for training data and detects deviation in the measurements. In

both methods, principle component analysis reduced the dimensionality of the data to be processed, which leads to lower computational complexities.

6.2 Future Work

Security issues remain challenging in the generation, Transmission, and Distribution of the power networks. This is mainly because of the large scale that power systems have and also their interionic differences with other networks such as Internet[1]. Current power systems use internet security mechanisms for data communication. Considering principal differences between internet and power networks, developing proper security mechanisms for power systems would be promising. Physical security of power grid should be analyzed beside the cyber security issues. Research in [97] is an example of case in which authors present an impact analysis framework and focus on the model synthesis stage in which both cyber and physical grid entity relationships are modeled as directed graphs.

In order to make the smart grid more secure, different aspects should be considered such as integrity and privacy of the transmitted data. For example in state estimation it is extremely important to assure the accuracy and consistency of the data (integrity of the data) [39, 43, 49, 98]. Privacy of the data is important for both utility companies and customers. For example having access to customers data can expose their habits and behavior so public acceptance of the smart meters needs solid security investigations in this regard. Research in this area is ongoing and several researchers try to improve the security of data communication from smart meters to the control centers [99–102].

Using the load as a corrective action in the peak time is an important tool for utilizing the power network efficiently. Affordable global communication infrastructure and embedded systems make it now relatively easy to give incentives to the loads and change

[1] An important difference is the stability problems in which any demand and supply mismatch can cause instability in the power network in portion of seconds. This problem becomes challenging when we consider the fact that electrical energy is not storable in the large scales.

their behaviors (demand side management). Demand side management relatively well researched in the potential and operations of the physical parts [103, 104]. Currently the inter–operability, algorithm stability, information security, and (information) network management in the ICT side shows the highest levels of activities [105, 106]. In other perspective, control center can use the collected data from smart meters in order to monitor the distribution system. The major ongoing challenge here is the large amount of data that should be processed. Indeed data analysis should extract information from the smart meters' large data set and transform it into an understandable structure that control center can use for different purposes such as quick fault detection in distribution systems.

Exploiting communication infrastructure in smart grid makes it more flexible confronting with different faults and load changes in the network. On the other hand integrating renewable resources will decrease this flexibility. This is because of intermittency of the renewable resources which is ongoing research mainly in two directions, one group of researchers are trying to improve the prediction of intermittency in renewable resources by developing precise models [16–19]. Other group of researchers try to find the optimal way of integrating renewable recourses. The common goal of these studies is to maximize the integration of renewable resources without violating security constraints[2] [20–22].

Microgrids are small-scale and low voltage supply networks that are designed to supply electrical and heat loads for small consumers, such as academic or public communities, and manufacturing companies [66]. These units can be separated from the main grid in contingencies and they can provide electricity for their consumers with acceptable quality. Although microgrid shows great promises in integrating renewable resources and peak shaving of smart grids, it faces several challenges in real-time power management and control systems. Some of these challenges can be addressed by the optimization problems with different objectives such as, power demands, fuel consumption, environmental emissions, costs, dispatchable loads, etc. [67]. Developing a model to consider these objectives is an

[2]In other words, flexibility of power network should meet the intermittency of renewable recourses.

ongoing research which can be further investigated.

Bibliography

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC, 2004, vol. 24.

[2] "Transmission access policy study group v. ferc," p. 667, 2000.

[3] T. Ackermann, G. Andersson, and L. Söder, "Distributed generation: a definition," *Electric Power Systems Research*, vol. 57, no. 3, pp. 195–204, 2001.

[4] P. P. Barker and R. De Mello, "Determining the impact of distributed generation on power systems. i. radial distribution systems," in *Power Engineering Society Summer Meeting, 2000. IEEE*, vol. 3. IEEE, 2000, pp. 1645–1656.

[5] T. F. Garrity, "Getting smart," *Power and Energy Magazine, IEEE*, vol. 6, no. 2, pp. 38–45, Apr. 2008.

[6] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Computer Networks*, vol. 50, no. 7, pp. 877–897, May. 2006.

[7] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, Jul. 2011.

[8] T.-I. Choi, K. Y. Lee, D. R. Lee, and J. K. Ahn, "Communication system for distribution automation using cdma," *Power Delivery, IEEE Transactions on*, vol. 23, no. 2, pp. 650–656, Apr. 2008.

[9] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES, Seatle, WA*. IEEE, Mar. 2009, pp. 1–9.

[10] H. Zhou, C. Guo, and J. Qin, "Efficient application of gprs and cdma networks in scada system," in *Power and Energy Society General Meeting, 2010 IEEE, Minneapolis, MN*. IEEE, Jul. 2010, pp. 1–6.

[11] C. W. Potter, A. Archambault, and K. Westrick, "Building a smarter smart grid through better renewable energy information," in *Power Systems Conference and Exposition (PSCE'09),Seatle, WA*. IEEE, Mar. 2009, pp. 1–5.

[12] M. Liserre, T. Sauter, and J. Y. Hung, "Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics," *Industrial Electronics Magazine, IEEE*, vol. 4, no. 1, pp. 18–37, 2010.

[13] T. Hammons, "Integrating renewable energy sources into european grids," *International Journal of Electrical Power & Energy Systems*, vol. 30, no. 8, pp. 462–475, 2008.

[14] A. Ipakchi and F. Albuyeh, "Grid of the future," *Power and Energy Magazine, IEEE*, vol. 7, no. 2, pp. 52–62, 2009.

[15] H. Farhangi, "The path of the smart grid," *Power and Energy Magazine, IEEE*, vol. 8, no. 1, pp. 18–28, 2010.

[16] B. Ernst, "Wind power prediction," *Wind Power in Power Systems, Second Edition*, pp. 753–766, 2012.

[17] A. Costa, A. Crespo, J. Navarro, G. Lizcano, H. Madsen, and E. Feitosa, "A review on the young history of the wind power short-term prediction," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 6, pp. 1725–1744, 2008.

[18] M. G. De Giorgi, A. Ficarella, and M. Tarantino, "Assessment of the benefits of numerical weather predictions in wind power forecasting based on statistical methods," *Energy*, vol. 36, no. 7, pp. 3968–3978, 2011.

[19] Y. Atwa and E. El-Saadany, "Annual wind speed estimation utilizing constrained grey predictor," *Energy Conversion, IEEE Transactions on*, vol. 24, no. 2, pp. 548–550, 2009.

[20] C. W. Potter, H. A. Gil, and J. McCaa, "Wind power data for grid integration studies," in *Power Engineering Society General Meeting, 2007. IEEE*. IEEE, 2007, pp. 1–6.

[21] C. W. Potter, D. Lew, J. McCaa, S. Cheng, S. Eichelberger, and E. Grimit, "Creating the dataset for the western wind and solar integration study (usa)," *Wind Engineering*, vol. 32, no. 4, pp. 325–338, 2008.

[22] J. C. Smith, M. R. Milligan, E. A. DeMeo, and B. Parsons, "Utility wind integration and operating impact state of the art," *Power Systems, IEEE Transactions on*, vol. 22, no. 3, pp. 900–908, 2007.

[23] S. Darby, "Smart metering: what potential for householder engagement?" *Building Research & Information*, vol. 38, no. 5, pp. 442–457, 2010.

[24] B. Neenan and R. C. Hemphill, "Societal benefits of smart metering investments," *The electricity journal*, vol. 21, no. 8, pp. 32–45, 2008.

[25] A. B. Haney, T. Jamasb, and M. G. Pollitt, "Smart metering and electricity demand: Technology, economics and international experience," 2009.

[26] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[27] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN. com*, vol. 26, 2007.

[28] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*. IEEE, 2012, pp. 2468–2472.

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

[30] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid-the new and improved power grid: A survey," 2011.

[31] H. Brown and S. Suryanarayanan, "A survey seeking a definition of a smart distribution system," in *North American Power Symposium (NAPS), 2009*. IEEE, 2009, pp. 1–7.

[32] S. Rohjans, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, and T. Weidelt, "Survey of smart grid standardization studies and recommendations," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 583–588.

[33] N. Framework, "Roadmap for smart grid interoperability standards," *National Institute of Standards and Technology*, 2010.

[34] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010*. IEEE, 2010, pp. 1830–1835.

[35] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in dnp3 controlled scada systems," in *Simulation Conference (WSC), Proceedings of the 2011 Winter*. IEEE, 2011, pp. 2614–2626.

[36] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for iec61850 automated substations," *Power Delivery, IEEE Transactions on*, vol. 25, no. 4, pp. 2376–2383, 2010.

[37] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against ddos attacks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 93–107.

[38] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, 2013.

[39] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[40] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Innovative Smart Grid Technologies (ISGT), 2010*. IEEE, 2010, pp. 1–7.

[41] H. Li, L. Lai, and R. C. Qiu, "Communication capacity requirement for reliable and secure state estimation in smart grid," *IEEE SmartGrid-Comm10*, pp. 191–196, 2010.

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

[43] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 226–231.

[44] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 244–248.

[45] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 220–225.

[46] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 214–219.

[47] L. Lanchao, M. Esmalifalak, and Z. Han, "Detection of false data injection in power grid exploiting low rank and sparsity," in *IEEE International Conference on communications, Budapest, Hungary, June 2013*.

[48] L. Lanchao, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Protection against false data injection attacks in power grids via sparsity and low rank," *to appear, Smart Grid, IEEE Transactions on*.

[49] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *to appear, Smart Grid, IEEE Transactions on*, 2012.

[50] K. Jain, "Security based on network topology against the wiretapping attack," *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 68–71, 2004.

[51] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 3, pp. 476–486, 2011.

[52] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 220–225.

[53] T. Basar, G. J. Olsder, G. Clsder, T. Basar, T. Baser, and G. J. Olsder, *Dynamic noncooperative game theory*. SIAM, 1995, vol. 200.

[54] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2011.

[55] W. Saad, Z. Han, H. V. Poor, and T. Basar, "Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications," *Signal Processing Magazine, IEEE*, vol. 29, no. 5, pp. 86–105, 2012.

[56] M. Swearingen, "Real time evaluation and operation of the smart grid using game theory," in *Rural Electric Power Conference (REPC), 2011 IEEE*. IEEE, 2011, pp. B3–1.

[57] Z. Zhu, J. Tang, S. Lambotharan, W. Chin, and Z. Fan, "An integer linear programming and game theory based optimization for demand-side management in smart grid," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011, pp. 1205–1210.

[58] Z. M. Fadlullah, Y. Nozaki, A. Takeuchi, and N. Kato, "A survey of game theoretic approaches in smart grid," in *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*. IEEE, 2011, pp. 1–4.

[59] S. Bu, F. R. Yu, and P. X. Liu, "A game-theoretical decision-making scheme for electricity retailers in the smart grid with demand-side management," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 387–391.

[60] Z. Xudong, L. Jianming, S. Hao, and M. Xiangchun, "Orderly consumption and intelligent demand-side response management system under smart grid," in *Power*

and Energy Engineering Conference (APPEEC), 2010 Asia-Pacific. IEEE, 2010, pp. 1–4.

[61] P. Wang, J. Huang, Y. Ding, P. Loh, and L. Goel, "Demand side load management of smart grids using intelligent trading/metering/billing system," in *PowerTech, 2011 IEEE Trondheim*. IEEE, 2011, pp. 1–6.

[62] A. Mohsenian-Rad, V. W. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 3, pp. 320–331, 2010.

[63] P. Xu, P. Haves, M. A. Piette, and L. Zagreus, "Demand shifting with thermal mass in large commercial buildings: Field tests, simulation and audits," Ernest Orlando Lawrence Berkeley NationalLaboratory, Berkeley, CA (US), Tech. Rep., 2005.

[64] J. E. Braun, "Load control using building thermal mass," *Journal of solar energy engineering*, vol. 125, p. 292, 2003.

[65] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug-in hybrid electric vehicles on a residential distribution grid," *Power Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 371–380, 2010.

[66] S. Chowdhury, S. Chowdhury, and P. Crossley, *Microgrids and active distribution networks*. Institution of Engineering and Technology, 2009.

[67] C. Colson and M. Nehrir, "A review of challenges to real-time power management of microgrids," in *Power & Energy Society General Meeting, 2009. PES'09. IEEE*. IEEE, 2009, pp. 1–8.

[68] J. J. Grainger and W. D. Stevenson, *Power systems analysis*. McGraw-Hill, 1994.

[69] A. J. Wood and B. Wollenberg, *POWER GENERATION OPERATION & CONTROL, (With CD)*. John Wiley & Sons, 2006.

[70] D. White, A. Roschelle, P. Peterson, D. Schlissel, B. Biewald, and W. Steinhurst, "The 2003 blackout: solutions that wont cost a fortune," *The Electricity Journal*, vol. 16, no. 9, pp. 43–53, 2003.

[71] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, "Marginal loss modeling in lmp calculation," *Power Systems, IEEE Transactions on*, vol. 19, no. 2, pp. 880–888, 2004.

[72] A. L. Ott, "Experience with pjm market operation, system design, and implementation," *Power Systems, IEEE Transactions on*, vol. 18, no. 2, pp. 528–534, 2003.

[73] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *Power Systems, IEEE Transactions on*, vol. 21, no. 4, pp. 1528–1538, 2006.

[74] 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," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, 2011.

[75] A. Bose and K. A. Clements, "Real-time modeling of power networks," *Proceedings of the IEEE*, vol. 75, no. 12, pp. 1607–1622, 1987.

[76] F. F. Wu, "Power system state estimation: a survey," *International Journal of Electrical Power & Energy Systems*, vol. 12, no. 2, pp. 80–87, 1990.

[77] L. Holten, A. Gjelsvik, S. Aam, F. F. Wu, and W.-H. Liu, "Comparison of different methods for state estimation," *Power Systems, IEEE Transactions on*, vol. 3, no. 4, pp. 1798–1806, 1988.

[78] Z. Alaywan and J. Allen, "California electric restructuring; a broad description of the development of the california iso," *Power Systems, IEEE Transactions on*, vol. 13, no. 4, pp. 1445–1452, 1998.

[79] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 5991–5998.

[80] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*, 2010.

[81] F. F. Wu and W.-H. Liu, "Detection of topology errors by state estimation [power systems]," *Power Systems, IEEE Transactions on*, vol. 4, no. 1, pp. 176–183, 1989.

[82] I. Jolliffe, *Principal component analysis*. Wiley Online Library, 2005.

[83] J. Himberg and A. Hyvärinen, "Independent component analysis for binary data: An experimental study," in *Proc. ICA2001*, 2001, pp. 552–556.

[84] "Power systems test case archives," *University of Washington, Department of Electrical Engineering,[Online], Available: http://www.ee.washington.edu/research/pstca/*, 1993.

[85] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 5991–5998.

[86] F. Li and R. Bo, "Small test systems for power system economic studies," in *Power and Energy Society General Meeting, 2010 IEEE*, July, pp. 1–4.

[87] V. Vapnik, "An overview of statistical learning theory," *Neural Networks, IEEE Transactions on*, vol. 10, no. 5, 1999.

[88] S. Marsland, *Machine learning: an algorithmic perspective*. Chapman & Hall/CRC, 2009.

[89] R. Sutton and A. Barto, *Reinforcement learning: An introduction*. Cambridge Univ Press, 1998, vol. 1, no. 1.

[90] S. Kotsiantis, I. Zaharakis, and P. Pintelas, "Supervised machine learning: A review of classification techniques," *Frontiers in Artificial Intelligence and Applications*, vol. 160, p. 3, 2007.

[91] E. Alpaydin, *Introduction to machine learning*. MIT press, 2004.

[92] K. Yamanishi, J.-I. Takeuchi, G. Williams, and P. Milne, "On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms," in *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2000, pp. 320–324.

[93] S. Zanero and S. M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," in *Proceedings of the 2004 ACM symposium on Applied computing*. ACM, 2004, pp. 412–419.

[94] I. Jolliffe, *Principal component analysis*. Wiley Online Library, 2005.

[95] N. Cristianini and J. Shawe-Taylor, *An introduction to support vector machines and other kernel-based learning methods*. Cambridge university press, 2000.

[96] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[97] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.

[98] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *Power Apparatus and Systems, IEEE Transactions on*, vol. 94, no. 2, pp. 329–337, 1975.

[99] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 238–243.

[100] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 49–60.

[101] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*. ACM, 2010, pp. 61–66.

[102] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: minimizing the rate of information leakage," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1932–1935.

[103] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *Industrial Informatics, IEEE Transactions on*, vol. 7, no. 3, pp. 381–388, 2011.

[104] F. Saffre and R. Gedge, "Demand-side management for the smart grid," in *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*. IEEE, 2010, pp. 300–303.

[105] W. Granzer, F. Praus, and W. Kastner, "Security in building automation systems," *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 11, pp. 3622–3630, 2010.

[106] A. Treytl, P. Palensky, and T. Sauter, "Security considerations for energy automation networks," in *Proceedings of 6th IFAC International Conference on Fieldbus Systems andtheir Applications, IPV–IFAC Proceedings Volume*, 2005, pp. 158–165.