



Impacts of Bad Data and Cyber Attacks on Electricity Market Operations

Final Project Report

Power Systems Engineering Research Center

*Empowering Minds to Engineer
the Future Electric Energy System*



Impacts of Bad Data and Cyber Attacks on Electricity Market Operations

Final Project Report

Project Team

**Lang Tong, Project Leader
Cornell University**

**Robert J. Thomas
Cornell University**

**Le Xie
Texas A&M University**

PSERC Publication 13-42

September 2013

For more information about this report, contact

Prof. Lang Tong
Cornell University
School of Electrical and Computer Engineering
384 Rhodes Hall
Ithaca, NY, USA
ltong@ece.cornell.edu; 515-294-9175

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: <http://www.pserc.org>.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-965-0745

Notice Concerning Copyright Material

PSERC members are given permission to copy without fee all or part of this publication for internal use if appropriate attribution is given to this document as the source material. This report is available for downloading from the PSERC website.

© 2013 Cornell University. All rights reserved.

Acknowledgements

This is the final report for the Power Systems Engineering Research Center (PSERC) research project titled “Impacts of Bad Data and Cyber Attacks on Electricity Market Operations” (project M-27). We express our appreciation for the support provided by PSERC’s industry members and by the National Science Foundation under the Industry / University Cooperative Research Center program.

The authors thank industry collaborators for their advice and support. including

- Eugene Litvinov, ISO New England
- Jim Price, California ISO
- Elizabeth LaRose, GE
- Wenyan Li, BC Hydro.

Executive Summary

Cybersecurity is a critical concern facing the electric power industry. More needs to be learned about how breaches in cybersecurity could affect the industry. In this project, we explored impacts of bad data and malicious data attacks on real-time market operations. In particular, we investigated the problem from perspectives of an attacker and the control center of a Regional Transmission Organization (RTO).

The overall objectives of this research include:

- (i) providing system operators with a framework and analytical tools to evaluate the impact of bad/malicious data on electricity market operations. In particular, the tools can help system operators to assess the financial risks of bad data attacks in real-time markets.
- (ii) providing software vendors of EMS (Energy Management Systems) and MMS (Market Management Systems) with new models and algorithms to enhance the robustness of state estimation against bad/malicious data attacks in light of secure market operations
- (iii) providing power utilities with the operating protocols to detect malicious data attacks when deploying smart grid communication infrastructures.

This report includes contributions in four related topic areas. The main results are highlighted below.

I. Impacts of Data Quality on Real-Time Locational Marginal Price

In this work, we characterize impacts of data quality on real-time locational marginal price (LMP). We first provide a geometrical characterization of LMP on the state space of the power system. In particular, we show that the state space is partitioned into polytope price regions where each polytope is associated with a unique real-time LMP vector, and the price region is defined by a particular set of congested lines that determine the boundaries of the price region.

Two types of bad data are considered. One is the bad data associated with meter measurements such as the branch power flows in the network. Such bad data will cause errors in state estimation. The analysis of the worst case data then corresponds to finding the worst measurement error such that it perturbs the correct state estimation to the worst price region. The second type of bad data, one that has not been carefully studied in the context of LMP in the literature, is error in digital measurements such as switch or breaker states. Such errors lead directly to topology errors therefore causing a change in the polytope structure.

We performed simulation studies using the IEEE-14 and IEEE-118 networks. We observe that bad data independent of the system state seems to have limited impact on real-time LMPs, and greater price perturbations can be achieved by state dependent bad

data. The results also demonstrate that the real-time LMPs are subject to much larger perturbation if bad topology data are present in addition to bad meter data.

While substantial price changes can be realized for small networks by the worst meter data, as the size of network grows while the measurement redundancy rate remains the same, the influence of worst meter data on LMP is reduced. However, larger system actually gives more possibilities for the bad topology data to perturb the real-time LMP more significantly.

II. Data Attack on LMP in Time-coupled Look-ahead Dispatch

The main objective of this chapter is to study the impact of cyber data attacks on state estimation, which subsequently influence the result of the existing static and newly emerging look-ahead dispatch models in the real-time power market. It is shown that bad/malicious data could be injected into the measurement layer of power system operations, which can lead to corrupted estimation of the states of the physical layer. Consequently, the attacker could distort the feedback information from control/communication layer back to the physical layer in two ways, leading to (1) physical insecurity in the power grid operations, and/or (2) financial misconduct in the power markets. This chapter contributes to topic (2) using realistic dispatch models in power markets. In particular, we propose a novel attack strategy with which the attacker can manipulate, in look-ahead dispatch, the limits of ramp constraints of generators. It is demonstrated that the proposed attack may lead to financial profits via malicious capacity withholding of selected generators, while being undetected by the existing bad data detection algorithm embedded in the state estimator. Numerical examples simulated in the IEEE 14-bus system demonstrate the undetectability and profitability of the proposed cyber data attack.

III. LMP Sensitivity Analysis to Data Corruption-induced Estimation Error

In this chapter, we investigate the sensitivity of real-time LMP with respect to continuous (e.g., the power injection/flow and voltage magnitude) and discrete (e.g., the on/off status of a circuit breaker) data corruption due to state estimation error.

In the first part, corrupted continuous sensor data are shown to deviate power system state estimation from their actual values, which subsequently leads to the distortion of real-time market LMPs. We build two matrices: the first with LMP sensitivity at any bus to any estimate, and the second with sensitivity of any estimate to data at any sensor. A unified matrix that combines these two matrices in multiplication form enables system operators to quantify the impact on LMP of data at any sensor at any bus throughout the entire transmission network.

In the second part, we examine the impact of circuit breaker-induced network topology errors due to discrete data corruption on real-time LMP. We derive an analytical index to compute LMP sensitivity with respect to network topology error, particularly line status error, in the power system. The proposed sensitivity index provides system operators an analytical tool to identify economically sensitive transmission lines and circuit breakers,

whose status error will significantly impact the real-time LMPs. The proposed sensitivity index is tested using the IEEE 14-bus system.

IV. Topology Attack on a Smart Grid: Undetectable Attacks and Countermeasures

Results of this work aim to achieve two objectives. First, we characterize conditions under which undetectable attacks are possible, given a set of vulnerable meters that may be controlled by an adversary. To this end, we consider two attack regimes based on the information set available to the attacker. The more information the attacker has, the stronger its ability to launch a sophisticated attack that is hard to detect.

If the attacker has global information, we obtain a necessary and sufficient algebraic condition under which, given a set of adversary controlled meters, there exists an undetectable attack that misleads the control center with an incorrect “target” topology. This algebraic condition provides not only numerical ways to check if the grid is vulnerable to undetectable attacks but also insights into which meters to protect to defend against topology attacks. We also provide specific constructions of attacks and show certain optimality of the proposed attacks. A more practically significant situation is the local information regime where the attacker has only local information from those meters it has gained control. Under certain conditions, undetectable attacks exist and can be implemented easily based on simple heuristics.

The second objective is to provide conditions under which topology attack cannot be made undetectable. Such a condition, even if it may not be the tightest, provides insights into defense mechanisms against topology attacks. We show that if a set of meters satisfying a certain branch covering property are protected, then topology attacks can always be detected. In practice, protecting a meter may be carried out at multiple levels, from physical protection measures to software protection schemes using more sophisticated authentication protocols.

Project Publications

1. O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” *IEEE Transactions on Smart Grid* Vol. 2, No. 4, pp. 659 - 666, December 2011.
2. L. Xie, Y. Mo and B. Sinopoli, “Integrity Data Attacks in power market operations,” *IEEE Transactions on Smart Grid* Vol. 2, No. 4, pp. 659 - 666, December 2011.
3. L. Jia, R. J. Thomas, and L. Tong, “Impacts of malicious data on real-time price of electricity market operations,” *Hawaii Intl. Conf. on System Sciences (HICSS)*, Jan., 2012.
4. L. Jia, R. J. Thomas, and L. Tong, “On the nonlinearity effects on malicious data attack on power systems,” *Proc. IEEE PES General Meeting*, July 2012.

5. D.-H. Choi, and L. Xie, "Malicious Ramp-Induced Temporal Data Attack in Power Market with Look-ahead Dispatch," *2012 Third International Conference on Smart Grid Communications*, November 2012. (The Best Paper Award)
6. J. Kim and L. Tong, "On topology attack of a smart grid: undetectable attacks and counter measures," *IEEE J. Selected Areas in Communications*, July 2013.
7. D.-H. Choi, and L. Xie, "Ramp-Induced Data Attacks on Look-ahead Dispatch in Real-time Power Markets," *IEEE Transactions on Smart Grid* (accepted, to appear)
8. L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impacts of data quality on real-time locational marginal price," submitted to *IEEE Trans. on Power Systems*.
9. D.-H. Choi and L. Xie, "Sensitivity Analysis of Real-Time Locational Marginal Price to SCADA Sensor Data Corruption," *Submitted to IEEE Transactions on Power Systems*.
10. D.-H. Choi, and L. Xie, "Sensitivity Analysis of Locational Marginal Price to Circuit Breaker-Induced Network Topology Change," *Submitted to 2013 Fourth International Conference on Smart Grid Communications*, October 2013.
11. L. Xie, D.-H. Choi, S. Kar, and H. V. Poor, "Bad/malicious Data Detection in Distributed Power System State Estimation," in *Smart Grid Communications and Networking*, E. Hossain, Z. Han, and H. V. Poor, Eds. Cambridge University Press, 2012

Student Theses

1. Jinsub Kim, "Anomaly Detection in Networks," PhD Dissertation, Cornell University, September, 2013
2. D.-H. Choi, "Impact of Bad/Malicious Data on Electricity Market Operations", PhD Dissertation, Texas A&M University, December 2013.
3. Liyan Jia, "Pricing and mechanism design in a smart grid," PhD Dissertation, Cornell University. In progress.

TABLE OF CONTENTS

Table of Contents	vi
List of Figures	x
List of Tables	xiii
1 Introduction	1
1.1 Impacts of Data Quality on Real-Time Locational Marginal Price .	2
1.2 Data Attack on LMP in Time-coupled Look-ahead Dispatch	3
1.3 LMP Sensitivity Analysis to Data Corruption-induced Estimation Error	4
1.4 Topology Attack on a Smart Grid: Undetectable Attacks and Countermeasures	5
2 Impacts of Data Quality on Real-Time Locational Marginal Price	7
2.1 Introduction	7
2.1.1 Summary of Results and Organization	8
2.1.2 Related Work	11
2.2 Structures of Real-Time LMP	13
2.3 Data Model and State Estimation	18
2.3.1 Bad Data Model	18
2.3.2 State Estimation	21
2.3.3 Bad Data Detection	22
2.4 Impact of Bad Data on LMP	23
2.4.1 Average Relative Price Perturbation	24
2.4.2 Worst ARPP under State Independent Bad Data Model . .	25
2.4.3 Worst ARPP under Partially Adaptive Bad Data	27

2.4.4	Worst ARPP under Fully Adaptive Bad Data	28
2.4.5	A Greedy Heuristic	29
2.5	Bad Topology Data on LMP	30
2.6	Numerical Results	35
2.6.1	Linear model with DC state estimation	35
2.6.2	Nonlinear model with AC state estimation	37
2.6.3	Performance of the greedy search heuristic	39
2.7	Conclusion	40
3	Data Attack on LMP in Time-coupled Look-ahead Dispatch	43
3.1	Introduction	43
3.1.1	Literature Review	44
3.1.2	Report Organization	45
3.2	Preliminaries	46
3.2.1	DC State Estimation Model	46
3.2.2	Economic Dispatch Model	47
3.3	Attack Model and Undetectability	52
3.4	Spatial Data Attack on Static Dispatch	53
3.4.1	Problem Formulation	53
3.4.2	Attack Strategy	54
3.4.3	Simulation Studies	58
3.5	Temporal Data Attack on Look-ahead Dispatch	61
3.5.1	Problem Formulation	62
3.5.2	Attack Strategy	64
3.5.3	Attack Performance Metrics	67

3.5.4	Simulation Studies	69
3.6	Conclusions	75
3.7	Appendix	76
4	LMP Sensitivity Analysis to Data Corruption-Induced Estimation Error	78
4.1	Introduction	78
4.1.1	Literature Review	79
4.1.2	Report Organization	80
4.2	Preliminaries	81
4.2.1	AC State Estimation Model	82
4.2.2	Real-time Electricity Pricing Model	83
4.3	Impact Analysis of LMP Subject to Power Flow Estimate Errors . .	85
4.3.1	Problem Formulation	85
4.3.2	Derivation of the Proposed LMP Sensitivity Index	87
4.3.3	Simulation Studies	93
4.4	Impact Analysis of LMP Subject to Network Topology Estimate Errors	105
4.4.1	Preliminaries	105
4.4.2	Derivation of the Proposed LMP Sensitivity Index	107
4.4.3	Simulation Studies	112
4.5	Conclusions	117
5	Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures	119
5.1	Introduction	119
5.1.1	Related Works	121

5.1.2	Summary of Results and Organization	123
5.2	Preliminaries	125
5.2.1	Network and Measurement Models	125
5.2.2	Adversary Model	127
5.2.3	State Estimation, Bad Data Test, and Undetectable Attacks	130
5.3	Topology Attack with Global Information	132
5.3.1	Condition for an Undetectable Attack	133
5.3.2	State-preserving Attack	135
5.4	Topology Attack with Local Information	142
5.5	Countermeasure for Topology Attacks	145
5.6	Numerical Results	148
5.6.1	Application of Undetectability Condition	148
5.6.2	Undetectability and Effects on Real-time LMP	150
5.7	Conclusion	153
5.8	Proofs	154
5.8.1	Proof of Theorem 5.3.2	154
5.8.2	Proof of Theorem 5.3.3	156
5.8.3	Proof of Theorem 5.3.4	157
5.8.4	Proof of Theorem 5.5.1	159

Bibliography	162
---------------------	------------

LIST OF FIGURES

2.1	Change of real-time LMPs due to bad data.	9
2.2	Hx and $\bar{H}x$: Each row is marked by the corresponding meter (i for injection at i and (i, j) for flow from i to j).	33
2.3	The attack modifies local measurements around the line (i, j) in \mathcal{E}_Δ	34
2.4	Linear model: ARPP vs detection prob.	38
2.5	Nonlinear model: ARPP vs detection prob.	40
3.1	A three-layered framework illustrating cyber data attack.	44
3.2	LMP with and without cyber attacks (only one line congestion).	59
3.3	LMP with and without cyber attacks (three congested lines).	60
3.4	Conceptual diagrams illustrating a ramp-induced data attack.	63
3.5	IEEE 14-bus Test system.	69
3.6	LMP of static and look-ahead dispatch without attack and with Case I,II and III attacks.	71
3.7	$P_{g_3}^{\max} - P_{g_3}^*$ of static and look-ahead dispatch without attack and with Case I,II and III attacks.	73
4.1	Illustrating the impact of corrupted continuous and discrete SCADA sensor data on state estimation and SCED.	79
4.2	A three-layered framework illustrating the coupling of the physical power system, state estimation, and SCED.	85
4.3	IEEE 14-bus system with a given measurement configuration.	94
4.4	Sensitivities of Ex-ante prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 3-4 is congested and P_{g_3} is binding at $\hat{P}_{g_3}^{\min}$ in the IEEE 14-bus system.	95

4.5	Sensitivities of Ex-post prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 6-12 is congested and the corresponding line flow is binding at the capacity limit of line 6-12 in the IEEE 14-bus system.	99
4.6	LMP differences between with and without corrupted data when z_8 is corrupted in Fig. 4.4(c).	100
4.7	LMP differences between with and without corrupted data in Fig. 4.4 (a) P_3 , Q_3 , and V_3 corruptions (b) $P_{5,6}$ and $Q_{5,6}$ corruptions.	101
4.8	Comparison of LMP sensitivities at bus 3 in Fig. 4.4(a) with varying variances of injection measurements P_3 and P_{11}	102
4.9	Sensitivities of Ex-ante prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 15-17 is congested and $P_{g_{19}}$ is binding at $\hat{P}_{g_{19}}^{\max}$ in the IEEE 118-bus system.	103
4.10	IEEE 118-bus system.	104
4.11	Illustration of a linear relationship between $\Delta\pi_l^k$ and \mathbf{v}_l^k	112
4.12	IEEE 14-bus system including bus-breaker model.	113
4.13	LMP results in Fig. 4.12: (a) comparison of LMPs between with and without line exclusion error; (b) comparison of LMP sensitivities obtained by SCED and the proposed approach.	114
4.14	Impact of a varying gap between the energy costs of marginal units on LMP sensitivity.	115
4.15	Comparison of LMP sensitivities with four different branch exclusion errors under the line 5-6 congestion.	116
4.16	Comparison of LMP sensitivities with four different congestion patterns under the line 4-5 exclusion.	117
5.1	Attack Model with Generalized State Estimation	128
5.2	Decomposition of Measurement Matrix	137

5.3	Heuristic Operations Around the Target Line (i, j)	143
5.4	The Cover-up Strategy for IEEE 14-bus System	147
5.5	Detection Probability of Single-line Attack	152

LIST OF TABLES

2.1	Performance of greedy search method	39
3.1	Notations.	46
3.2	Case Description	58
3.3	Attack Efforts and Profits ($\epsilon = 1$ MWh)	61
3.4	Generator Parameters of the IEEE 14-bus Test System.	70
3.5	Attack Performance in Static and Look-ahead Dispatch.	72
3.6	Attack Performance with Varying Attack Magnitude in Case I.	73
3.7	Impact of Ramp Rate on the Attack Performance in Case I.	74
3.8	Impact of Measurement Variance on the Attack Performance in Case I.	74
4.1	Notations.	81
4.2	Generator Parameters in the IEEE 14-bus System.	93
4.3	Generator Parameters of the IEEE 14-bus Test System.	114
5.1	Adversary Meters For Removing Lines (2, 4) and (12, 13)	149
5.2	The Sets of Lines Undetectable Attacks Can Remove	150
5.3	Average Detection Probabilities of Single-line Attacks	152

CHAPTER 1

INTRODUCTION

The electric power industry is undergoing profound changes as the industry aims to capture the promise of a smart grid for a sustainable energy future. Enabled by the advanced sensing devices such as Phasor Measurement Units (PMUs), increasingly powerful computation capability, and ubiquitous communication and networking infrastructure, power system operations in a smart grid era are increasingly rely on real-time information gathered in wide geographical areas. Institutionally, the increasing presence of demand response programs may open the door to more integrated SCADA and end-user networks.

Given the stronger coupling between cyber components (sensors and communication networks, in particular) and physical operations in power systems, smart grid of the future must cope with a variety of anomalies in this cyber-physical system. Classical problems such as line outages and meter malfunction are further complicated by the potential of cyber attacks by adversary. Such attacks can be coordinated in such a way that renders classical bad data detection ineffective.

The goal of this research is to investigate the impact of bad data and malicious data attack on real-time market operations. In particular, we investigate the problem from perspectives of an attacker and the control center of a Regional Transmission Organization (RTO).

The overall objectives of this research include (i) providing system operators with a framework and analytical tools to evaluate the impact of bad/malicious data

on electricity market operations. In particular, the tools can help system operators to assess the financial risks of bad data attacks in real-time markets; (ii) providing software vendors of EMS (Energy Management Systems) and MMS (Market Management Systems) with new models and algorithms to enhance the robustness of state estimation against bad/malicious data attacks in light of secure market operations; (iii) providing power utilities with the operating protocols to detect malicious data attacks when deploying smart grid communication infrastructures.

This report includes contributions in four related topic areas, and the main results are highlighted below.

1.1 Impacts of Data Quality on Real-Time Locational Marginal Price

In this work, we characterize impacts of data quality on real-time locational marginal price (LMP). We first provide a geometrical characterization of LMP on the state space of the power system. In particular, we show that the state space is partitioned into polytope price regions where each polytope is associated with a unique real-time LMP vector, and the price region is defined by a particular set of congested lines that determine the boundaries of the price region.

Two types of bad data are considered. One is the bad data associated with meter measurements such as the branch power flows in the network. Such bad data will cause errors in state estimation. The analysis of the worst case data

then corresponds to finding the worst measurement error such that it perturbs the correct state estimation to the worst price region. The second type of bad data, one that has not been carefully studied in the context of LMP in the literature, is error in digital measurements such as switch or breaker states. Such errors lead directly to topology errors therefore causing a change in the polytope structure.

We performed simulation studies using the IEEE-14 and IEEE-118 networks. We observe that bad data independent of the system state seems to have limited impact on real-time LMPs, and greater price perturbations can be achieved by state dependent bad data. The results also demonstrate that the real-time LMPs are subject to much larger perturbation if bad topology data are present in addition to bad meter data. While substantial price changes can be realized for small networks by the worst meter data, as the size of network grows while the measurement redundancy rate remains the same, the influence of worst meter data on LMP is reduced. However, larger system actually gives more possibilities for the bad topology data to perturb the real-time LMP more significantly.

1.2 Data Attack on LMP in Time-coupled Look-ahead Dispatch

The main objective of this chapter is to study the impact of cyber data attacks on state estimation, which subsequently influence the result of the existing static and newly emerging look-ahead dispatch models in the real-time power market. It is shown that bad/malicious data could be injected into the measurement layer

of power system operations, which can lead to corrupted estimation of the states of the physical layer. Consequently, the attacker could distort the feedback information from control/communication layer back to the physical layer in two ways, leading to (1) physical insecurity in the power grid operations, and/or (2) financial misconduct in the power markets. This chapter contributes to topic (2) using realistic dispatch models in power markets. In particular, we propose a novel attack strategy with which the attacker can manipulate, in look-ahead dispatch, the limits of ramp constraints of generators. It is demonstrated that the proposed attack may lead to financial profits via malicious capacity withholding of selected generators, while being undetected by the existing bad data detection algorithm embedded in the state estimator. Numerical examples simulated in the IEEE 14-bus system demonstrate the undetectability and profitability of the proposed cyber data attack.

1.3 LMP Sensitivity Analysis to Data Corruption-induced Estimation Error

In this chapter, we investigate the sensitivity of real-time LMP with respect to continuous (e.g., the power injection/flow and voltage magnitude) and discrete (e.g., the on/off status of a circuit breaker) data corruption due to state estimation error.

In the first part, corrupted continuous sensor data are shown to deviate power system state estimation from their actual values, which subsequently leads to the

distortion of real-time market LMPs. We build two matrices: the first with LMP sensitivity at any bus to any estimate, and the second with sensitivity of any estimate to data at any sensor. A unified matrix that combines these two matrices in multiplication form enables system operators to quantify the impact on LMP of data at any sensor at any bus throughout the entire transmission network.

In the second part, we examine the impact of circuit breaker-induced network topology errors due to discrete data corruption on real-time LMP. We derive an analytical index to compute LMP sensitivity with respect to network topology error, particularly line status error, in the power system. The proposed sensitivity index provides system operators an analytical tool to identify economically sensitive transmission lines and circuit breakers, whose status error will significantly impact the real-time LMPs. The proposed sensitivity index is tested using the IEEE 14-bus system.

1.4 Topology Attack on a Smart Grid: Undetectable Attacks and Countermeasures

We consider covert data attacks on the network topology of a smart grid. In a so-called man-in-the-middle attack, an adversary alters data from certain meters and network switches to mislead the control center with an incorrect network topology while avoiding detections by the control center.

We obtain necessary and sufficient condition for the existence of an undetectable

attack is obtained for strong adversaries who can observe all meter and network data. For weak adversaries with only local information, a heuristic method of undetectable attack is proposed. Countermeasures to prevent undetectable attacks are also considered. It is shown that undetectable attacks do not exist if a set of meters satisfying a certain branch covering property are protected. The proposed attacks are tested with IEEE 14-bus and IEEE 118-bus system, and their effect on real-time locational marginal pricing is examined.

CHAPTER 2

IMPACTS OF DATA QUALITY ON REAL-TIME LOCATIONAL MARGINAL PRICE

2.1 Introduction

The deregulated electricity market has two interconnected components. The day-ahead market determines the locational marginal price (LMP) based on the dual variables of the optimal power flow (OPF) solution [1, 2], given generator offers, demand forecast, system topology, and security constraints. The calculation of LMP in the day-ahead market does not depend on the actual system operation. In the real-time market, on the other hand, an ex-post formulation is often used (*e.g.*, by PJM and ISO-New England [3]) to calculate the real-time LMP by solving an incremental OPF problem. The LMPs in the day-ahead and the real-time markets are combined in the final clearing and settlement processes.

The real-time LMP is a function of data collected by the supervisory control and data acquisition (SCADA) system. Therefore, anomalies in data, if undetected, will affect prices in the real-time market. While the control center employs a bad data detector to “clean” the real-time measurements, miss detections and false alarms will occur inevitably. The increasing reliance on the cyber system also comes with the risk that malicious data may be injected by an adversary to affect system and real-time market operations. An intelligent adversary can carefully design a data attack to avoid detection by the bad data detector.

Regardless of the source of data errors, it is of significant value to assess potential impacts of data quality on the real-time market, especially when a smart grid may in the future deploy demand response based on real-time LMP. To this end, we are interested in characterizing the impact of *worst case data errors* on the real-time LMP. The focus on the worst case also reflects the lack of an accurate model of bad data and our desire to include the possibility of data attacks.

2.1.1 Summary of Results and Organization

We aim to characterize the worst effects of data corruption on real-time LMP. By “worst”, we mean the maximum perturbation of real-time LMP caused by bad or malicious data, when a fixed set of data is subject to corruption. The complete characterization of worst data impact, however, is not computationally tractable. Our goal here is to develop an optimization based approach to search for *locally worst data* by restricting the network congestion to a set of lines prone to congestion. We then apply computationally tractable (greedy search) algorithms to find the worst data and evaluate the effects of worst data by simulations.

In characterizing the relation between data and real-time LMP, we first present a geometric characterization of the real-time LMP. In particular, we show that the state space of the power system is partitioned into polytope price regions, as illustrated in Fig. 2.1(a), where each polytope is associated with a unique real-time LMP vector, and the price region \mathcal{X}_i is defined by a particular set of congested lines that determine the boundaries of the price region.

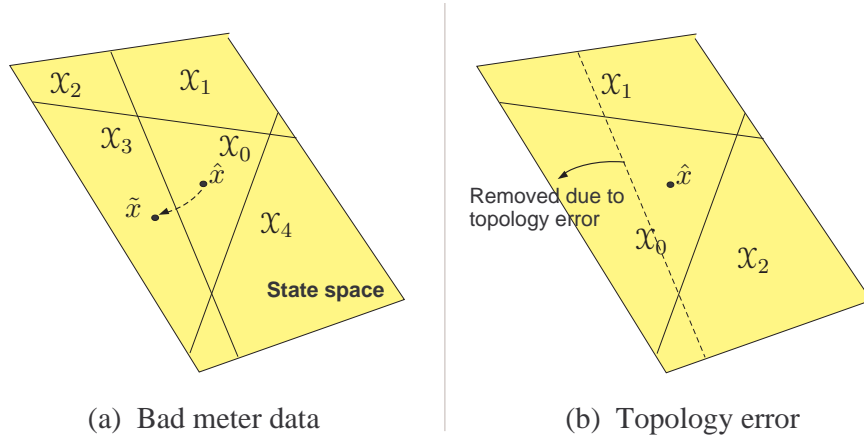


Figure 2.1: Change of real-time LMPs due to bad data.

Two types of bad data are considered in this paper. One is the bad data associated with meter measurements such as the branch power flows in the network. Such bad data will cause errors in state estimation, possibly perturbing, as an example, the correct state estimate \hat{x} in \mathcal{X}_0 to \tilde{x} in \mathcal{X}_3 (as shown in Fig. 2.1(a)). The analysis of the worst case data then corresponds to finding the worst measurement error such that it perturbs the correct state estimation to the worst price region.

The second type of bad data, one that has not been carefully studied in the context of LMP in the literature, is error in digital measurements such as switch or breaker states. Such errors lead directly to topology errors therefore causing a change in the polytope structure as illustrated in Fig. 2.1(b). In this case, even if the estimated system state changes little, the prices associated with each region change, sometimes quite significantly.

Before characterizing impacts of bad meter data on LMP, we need to construct appropriate models for bad data. To this end, we propose three increasingly more powerful bad data models based on the dependencies on real-time system measure-

ments: state independent bad data, partially adaptive bad data, and fully adaptive bad data.

In studying the worst case performance, we adopt a widely used approach that casts the problem as one involving an adversary whose goal is to make the system performance as poor as possible. The approach of finding the worst data is equivalent to finding the optimal strategy of an attacker who tries to perturb the real-time LMP and avoid being detected at the same time. By giving the adversary more information about the network state and endowing him with the ability to change data, we are able to capture the worst case performance, sometimes exactly and sometimes as bounds on performance.

Finally, we perform simulation studies using the IEEE-14 and IEEE-118 networks. We observe that bad data independent of the system state seems to have limited impact on real-time LMPs, and greater price perturbations can be achieved by state dependent bad data. The results also demonstrate that the real-time LMPs are subject to much larger perturbation if bad topology data are present in addition to bad meter data.

While substantial price changes can be realized for small networks by the worst meter data, as the size of network grows while the measurement redundancy rate remains the same, the influence of worst meter data on LMP is reduced. However, larger system actually gives more possibilities for the bad topology data to perturb the real-time LMP more significantly.

Our simulation results also show a degree of robustness provided by the *nonlin-*

ear state estimator. While there have been many studies on data injection attacks based on DC models, very few consider the fact that the control center typically employs the nonlinear WLS state estimator under the AC model. Our simulation shows that effects of bad analog data designed based on DC model may be mitigated by the nonlinear estimator whereas bad topology data coupled with bad analog data can have greater impacts on LMP.

The rest of the paper is organized as follows. Section 2.2 briefly describes a model of real-time LMP and introduces its geometric characterization in the state space of the power system. Section 2.3 establishes the bad data models and summarizes state estimation and bad data detection procedures at the control center. In Section 2.4, a metric of impact on real-time LMP caused by bad meter data is introduced. We then discuss the algorithms of finding worst case bad meter data vector in terms of real-time price perturbation under the three different bad data models. Section 2.5 considers the effect of bad topology data on real-time LMP. Finally, in Section 2.6, simulation results are presented based on IEEE-14 and IEEE-118 networks.

2.1.2 Related Work

Effects of bad data on power system have been studied extensively in the past, see [4, 5, 6]. Finding the worst case bad data is naturally connected with the problem of malicious data. In this context, the results presented in this paper can be viewed as one of analyzing the impact of the worst (malicious) data attack.

In a seminal paper by Liu, Ning, and Reiter [7], the authors first illustrated the possibility that, by compromising enough number of meters, an adversary can perturb the state estimate arbitrarily in some subspace of the state space without being detected by any bad data detector. Such attacks are referred to as strong attacks. It was shown by Kosut *et al.* [8] that the condition for the existence of such undetectable attacks is equivalent to the classical notion of network observability.

When the adversary can only inject malicious data from a small number of meters, strong attacks do not exist, and any injected malicious data can be detected with some probability. Such attacks are referred to as weak attacks [8]. In order to affect the system operation in some meaningful way, the adversary has to risk being detected by the control center. The impacts of weak attack on power system are not well understood because the detection of such bad data is probabilistic. Our results are perhaps the first to quantify such impacts. Most related research works focused on DC model and linear estimator while only few have addressed the nonlinearity effect [9, 10].

It is well recognized that bad data can also cause topology errors [11, 12], and techniques have been developed to detect topology errors. For instance, the residue vector from state estimation was analyzed for topology error detection [12, 11, 13]. Monticelli [14] introduced the idea of generalized state estimation where, roughly speaking, the topology that fits the meter measurements best is chosen as the topology estimate. The impacts of topology errors on electricity market have not been reported in the literature, and this paper aims to bridge this gap.

The effect of data quality on real-time market was first considered in [15, 16].

In [16], the authors presented the financial risks induced by the data perturbation and proposed a heuristic technique for finding a case where price change happens. While there are similarities between this paper and [16], several significant differences exist: (i) This paper focuses on finding the worst case, not only a feasible case. (ii) This paper considers a more general class of bad data where bad data may depend dynamically on the actual system measurements rather than static. (iii) This paper considers a broader range of bad data that also include bad topology data, and our evaluations are based on the AC network model and the presence of nonlinear state estimator.

2.2 Structures of Real-Time LMP

In this section, we present first a model for the computation of real-time locational marginal price (LMP). While ISOs have somewhat different methods of computing real-time LMP, they share the same two-settlement architecture and similar ways of using real-time measurements. In the following, we will use a simplified ex-post real-time market model, adopted by PJM, ISO New England, and other ISOs [17, 3]. We view this model as a convenient mathematical abstraction that captures the essential components of the real-time LMP calculation. For this reason, our results should be interpreted within the specified setup. Our purpose is not to include all details; we aim to capture the essential features.

In real-time, in order to monitor and operate the system, the control center will calculate the estimated system conditions (including bus voltages, branch flows, generation, and demand) based on real-time measurements. We call a branch

congested if the estimated flow is larger than or equal to the security limit. The congestion pattern is defined as the set of all congested lines, denoted as $\hat{\mathcal{C}}$. Note that we use hat (*e.g.*, $\hat{\mathcal{C}}$) to denote quantities or sets that are estimated based on real-time measurements. Details of state estimation and bad data detection are discussed in Section 2.3.2.

One important usage of state estimation is calculating the real-time LMP. Given the estimated congestion pattern $\hat{\mathcal{C}}$, the following linear program is solved to find the incremental OPF dispatch and associated real-time LMP, $\hat{\lambda} = (\hat{\lambda}_i)$ [17]:

$$\begin{aligned}
& \text{minimize} && \sum c_i^G \Delta p_i - \sum c_j^L \Delta d_j \\
& \text{subject to} && \sum \Delta p_i = \sum \Delta d_j \\
& && \Delta p_i^{\min} \leq \Delta p_i \leq \Delta p_i^{\max} \\
& && \Delta d_j^{\min} \leq \Delta d_j \leq \Delta d_j^{\max} \\
& && \sum_i A_{ki} \Delta p_i - \sum_j A_{kj} \Delta d_j \leq 0, \text{ for all } k \in \hat{\mathcal{C}},
\end{aligned} \tag{2.1}$$

where $\Delta d = (\Delta d_j)$ is the vector of incremental dispatchable load, $\Delta p = (\Delta p_i)$ the vector of incremental generation dispatch, $c^G = (c_i^G)$ and $c^L = (c_j^L)$ the corresponding real-time marginal cost of generations and dispatchable loads, Δp_i^{\min} and Δp_i^{\max} the lower and upper bounds for incremental generation dispatch, Δd_j^{\min} and Δd_j^{\max} the lower and upper bounds for incremental dispatchable load, and A_{ki} the sensitivity of branch flow on branch k with respect to the power injection at bus i .

The real-time LMP at bus i is defined as the overall cost increase when one unit of extra load is added at bus i , which is calculated as

$$\hat{\lambda}_i = \eta - \sum_{k \in \hat{\mathcal{C}}} A_{ki} \mu_k. \tag{2.2}$$

where η is the dual variable for the load-generation equality constraint, and μ_k is the dual variable corresponding to the line flow constraint in (2.1).

Note that in practice, the control center may use the ex-ante congestion pattern, which is obtained by running a 5 minute ahead security-constrained economic dispatch with the state estimation results and the forecasted loads (for the next five-minute interval) and choosing the lines congested at the dispatch solution [17, 18]. However, to avoid the complication due to ex-ante dispatch calculation, we assume that real-time pricing employs the estimated congestion pattern $\hat{\mathcal{C}}$ obtained from state estimation results. By doing so, we attempt to find direct relations among bad data, the state estimate, and real-time LMPs. Notice that once the congestion pattern $\hat{\mathcal{C}}$ is determined, the whole incremental OPF problem (2.1) no longer depends on the measurement data.

Under the DC model, the power system state, x , is defined as the vector of voltage phases, except the phase on the reference bus. The power flow vector f is a function of the system state x ,

$$f = Fx, \quad (2.3)$$

where F is the sensitivity matrix of branch flows with respect to the system state.

Assume the system has $n+1$ buses. Then, $x \in \mathcal{X} = [-\pi, \pi]^n$, where \mathcal{X} represents the state space. Any system state corresponds to a unique point in \mathcal{X} . From (2.3), the branch flow f is determined by the system state x . Comparing the flows with the flow limits, we obtain the congestion pattern associated with this state. Hence, each point in the state space corresponds to a particular congestion pattern.

We note that the above expression in (2.2) appears earlier in [1] where the role of congestion state in LMP computation was discussed. In this paper, our objective is to make explicit the connection between data and LMP. We therefore

need a linkage between data and congestion. To this end, we note that the power system state, the congestion state, and LMP form a Markov chain, which led to a geometric characterization of LMP on the power system state space, as shown in the following theorem.

Theorem 2.2.1 (Price Partition of the State Space). *Assume that the LMP exists for every possible congestion pattern*. Then, the state space \mathcal{X} is partitioned into a set of polytopes $\{\mathcal{X}_i\}$ where the interior of each \mathcal{X}_i is associated with a unique congestion pattern \mathcal{C}_i and a real-time LMP vector. Each boundary hyperplane of \mathcal{X}_i is defined by a single transmission line.*

Proof. For a particular congestion pattern \mathcal{C} defined by a set of congested lines, the set of states that gives \mathcal{C} is given by

$$\mathcal{X}_i \triangleq \{x : F_i \cdot x \geq T_i^{\max} \ \forall i \in \mathcal{C}, F_j \cdot x < T_j^{\max} \ \forall j \notin \mathcal{C}\},$$

where F_i is the i th row of F (see (2.3)), and T_j^{\max} the flow limit on branch j . Since \mathcal{X}_i is defined by the intersection of a set of half spaces, it is a polytope.

Given an estimated congestion pattern $\hat{\mathcal{C}}$, the envelop theorem implies that for any optimal primal solution and dual solution of (2.1) that satisfy the KKT conditions, (2.2) always gives the derivative of the optimal objective value with respect to the demand at each bus, which we assume exists, *i.e.*, each congestion pattern is associated with a unique real-time LMP vector λ . Hence, all states with the same congestion pattern share the same real-time LMP, which means each polytope \mathcal{X}_i in \mathcal{X} corresponds to a unique real-time LMP vector.

*This is equivalent to assuming that the derivative of the optimal value of (2.1) with respect to demand at each bus exists

□

Theorem 2.2.1 characterizes succinctly the relationship between the system state and LMP. As illustrated in Fig. 2.1(a), if bad data are to alter the LMP in real-time, the size of the bad data has to be sufficiently large so that the state estimate at the control center is moved to a different price region from the true system state.

On the other hand, if some lines are erroneously removed from or added to the correct topology, as illustrated in Fig. 2.1(b), it affects the LMP calculation in three ways[†]. First, the state estimate is perturbed since the control center employs an incorrect topology in state estimation. Secondly, the price partition of the state space changes due to the errors in topology information. Third, the shift matrix A in (2.1), which is a function of topology, changes thereby altering prices attached to each price region.

[†]In addition to these, the change in topology will affect contingency analysis. Such effect will appear as changes in contingency constraints in real-time LMP calculation (2.1) [17]. However, dealing with contingency constraints will significantly complicate our analysis and possibly obscure the more direct link between bad data and real-time LMP. Hence, we consider only line congestion constraints in (2.1).

2.3 Data Model and State Estimation

2.3.1 Bad Data Model

Meter data

In order to monitor the system, various meter measurements are collected in real time, such as power injections, branch flows, voltage magnitudes, and phasors, denoted by a vector $z \in \mathbb{R}^m$. If there exists bad data a among the measurements, the measurement with bad data, denoted by z_a , can be expressed as a function of the system states x ,

$$z_a = z + a = h(x) + w + a, \quad a \in \mathcal{A}, \quad (2.4)$$

where w represents the random measurement noise.

Notice here both conventional measurements and PMU measurements can be incorporated. The relationship between PMU measurements and system has been established by researchers, see [19, 20]. To simplify the problem, we can treat those PMU measurement equations as part of $h(x)$ to fit the PMU data into our framework. Therefore, we won't differentiate the types of measurements in the following discussion, although PMU data seem to have more direct impact on state estimation and real-time LMP calculation.

We make a distinction here between the measurement noise and bad data; the former accounts for random noise independently distributed across all meters

whereas the latter represents the perturbation caused by bad or malicious data. We assume no specific pattern for bad data except that they do not happen everywhere. We assume that bad data can only happen in a subset of the measurements, \mathcal{S} . We call \mathcal{S} as set of suspectable meters, which means the meter readings with in \mathcal{S} may subject to corruption. If the cardinality of \mathcal{S} is k , the feasible set of bad data a is a k -dimensional subspace, denoted as $\mathcal{A} = \{a : a_i = 0 \text{ for all } i \notin \mathcal{S}\}$.

We will consider three bad data models with increasing power of affecting state estimates.

M1. *State independent bad data:* This type of bad data is independent of real-time measurements. Such bad data may be the replacement of missing measurements.

M2. *Partially adaptive bad data:* This type of bad data may arise from the so-called man in the middle (MiM) attack where an adversary intercepts the meter data and alter the data based on what he has observed. Such bad data can adapt to the system operating state.

M3. *Fully adaptive bad data:* This is the most powerful type of bad data, constructed based on the actual measurement $z = h(x) + w$.

Note that M3 is in general not realistic. Our purpose of considering this model is to use it as a conservative proxy to obtain performance bounds for the impact of worst case data.

We assume herein a DC model in which the measurement function $h(\cdot)$ in (2.4) is linear. Specifically,

$$z_a = Hx + w + a, \quad a \in \mathcal{A}, \quad (2.5)$$

where H is the measurement matrix. Such a DC model, while widely used in the literature, may only be a crude approximation of the real power system. By making such a simplifying assumption and acknowledging its weaknesses, we hope to obtain tractable solutions in searching for worst case scenarios. It is important to note that, although the worst case scenarios are derived from the DC model, we carry out simulations using the actual nonlinear system model.

Topology data

Topology data are represented by a binary vector $s \in \{0, 1\}^l$, where each entry of s represents the state of a line breaker (0 for open and 1 for closed). The bad topology data is modeled as

$$s_b = s + b \pmod{2}, \quad b \in \mathcal{B}, \quad (2.6)$$

where $\mathcal{B} \subset \{0, 1\}^l$ is the set of possible bad data. When bad data are present, the topology processor will generate the topology estimate corresponding to s_b , and this incorrect topology estimate will be passed to the following operations unless detected by the bad data detector.

2.3.2 State Estimation

We assume that the control center employs the standard weighted least squares (WLS) state estimator. Under DC model,

$$\hat{x} = \arg \min_x (z - Hx)^T R^{-1} (z - Hx) = Kz, \quad (2.7)$$

where R is the covariance matrix of measurement noise w , and $K \triangleq (H^T R^{-1} H)^{-1} H^T R^{-1}$.

If the noise w is Gaussian, the WLS estimator is also the maximum likelihood estimate (MLE) of state x . By the invariant property of MLE, from (2.3), the maximum likelihood estimate of the branch flows is calculated as

$$\hat{f} = F\hat{x} = FKz. \quad (2.8)$$

The congestion pattern used in real-time LMP calculation (2.1) is directly from state estimation and consists of all the estimated branch flows which are larger than or equal to the branch flow limits, *i.e.*,

$$\hat{\mathcal{C}} = \{j : \hat{f}_j \geq T_j^{\max}\}, \quad (2.9)$$

where T_j^{\max} is the flow limit on branch j .

In the presence of bad meter data a , the meter measurements collected by control center is actually $z_a = Hx + w + a$. By using z_a , the WLS state estimate is

$$\hat{x}_a = Kz_a = \hat{x}^* + Ka, \quad (2.10)$$

where $\hat{x}^* = Kz$ is the “correct” state estimate without the presence of the bad data (*i.e.*, $a = 0$).

Eq. (2.10) shows that the effect of bad data on state estimation is linear. However, because a is confined in a k -dimensional subspace \mathcal{A} , the perturbation on the actual system state is limited to a certain direction.

When bad data exist both in meter and topology data, the control center uses a wrong measurement matrix \bar{H} , corresponding to the altered topology data, and the altered meter data z_a . Then, the WLS state estimate becomes

$$\hat{x}_a = \bar{K}z_a = \bar{K}z + \bar{K}a, \quad (2.11)$$

where $\bar{K} \triangleq (\bar{H}^T R^{-1} \bar{H})^{-1} \bar{H}^T R^{-1}$. Note that unlike the linear effect of bad meter data, bad topology data affects the state estimate by altering the measurement matrix H to \bar{H} .

2.3.3 Bad Data Detection

The control center uses bad data detection to minimize the impact of bad data. Here, we assume a standard bad data detection used in practice, the $J(\hat{x})$ -detector in [5]. In particular, the $J(\hat{x})$ -detector performs the test on the residue error, $r \triangleq z - H\hat{x}$, based on the state estimate \hat{x} . From the WLS state estimate (2.7), we have

$$r = (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) z = Uz. \quad (2.12)$$

where $U \triangleq (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})$

The $J(\hat{x})$ -detector is a threshold detector defined by

$$r^T R^{-1} r = z^T W z \underset{\text{good data}}{\overset{\text{bad data}}{\geq}} \tau, \quad (2.13)$$

where τ is the threshold calculated from a prescribed false alarm probability, and $W \triangleq U^T R^{-1} U$. When the measurement data fail to pass the bad data test, the control center declares the existence of bad data and takes corresponding actions to identify and remove the bad data.

In this paper, we are interested in those cases when bad data are present while the $J(\hat{x})$ -detector fails to detect them.

2.4 Impact of Bad Data on LMP

In this section, we examine the impact of bad data on LMP, assuming that the topology estimate of the network is correct.

One thing to notice is that in searching for the “worst” case, we take the perspective of the control center, not that of the attacker. In particular, we look for the worst congestion pattern for the LMP computation, even if this particular congestion pattern is difficult for the attacker to discover. So the focus here is not how easy it is for an attacker to find a locally worst congestion pattern; it is how much such a congestion pattern affects the LMP.

2.4.1 Average Relative Price Perturbation

In order to quantify the effect of bad data on real-time price, we need to first define the metric to measure the effect. We define the *relative price perturbation* (RPP) as the expected percentage price perturbation caused by bad data. Given that LMP varies at different buses, RPP also varies at different locations.

Let z_a be the data received at the control center and $\lambda_i(z_a)$ the LMP at bus i . The RPP at bus i is a function of bad data a , given by

$$\text{RPP}_i(a) = \mathbb{E} \left(\left| \frac{\lambda_i(z_a) - \lambda_i(z)}{\lambda_i(z)} \right| \right), \quad (2.14)$$

where the expectation is over random state and measurement noise.

To measure the system-wide price perturbation, we define the *average relative price perturbation* (ARPP) by

$$\text{ARPP}(a) = \frac{1}{n+1} \sum_i \text{RPP}_i(a), \quad (2.15)$$

where $n+1$ is the number of buses in the system.

The worst case analysis to be followed can be used for other metrics (e.g., price increase ratios or price decrease ratios, which are closely related to the market participants' gain or loss). Similar results can be showed following the same strategies. However, the comparison among different metrics is beyond the scope of this paper.

2.4.2 Worst ARPP under State Independent Bad Data Model

First, we consider the state independent bad data model (M1) given in Section 2.3.1. In this model, the bad data are independent of real-time measurements.

In constructing the state independent worst data, it is useful to incorporate prior information about the state. To this end, we assume that system state follows a Gaussian distribution with mean x_0 , covariance matrix Σ_x . Typically, we choose x_0 as the day-ahead dispatch since the nominal system state in real-time varies around its day-ahead projection.

In the presence of bad data a , the expected state estimate and branch flow estimate on branch i are given by

$$\mathbb{E}[\hat{x}] = x_0 + Ka. \quad (2.16)$$

$$\mathbb{E}[f_i] = F_i \mathbb{E}[\hat{x}] = F_i x_0 + F_i Ka, \quad (2.17)$$

where F_i is the corresponding row of branch i in F .

Our strategy is to make this expected state estimate into the region with the largest price perturbation among all the possible regions, $\hat{\mathcal{C}}^*$. From (2.9), this means making all the expected branch flows satisfy the boundary condition of $\hat{\mathcal{C}}^*$,

$$\begin{aligned} \mathbb{E}[f_i] &\geq T_i^{\max} & \text{for } i \in \hat{\mathcal{C}}^* \\ \mathbb{E}[f_i] &\leq T_j^{\max} & \text{for } j \notin \hat{\mathcal{C}}^*. \end{aligned} \quad (2.18)$$

However, due to the uncertainty (from both system state x and measurement

noise w), the actual estimated state after attack, \hat{x} , may be different from $\mathbb{E}[\hat{x}]$. Therefore, we want to make $\mathbb{E}[\hat{x}]$ at the “center” of the desired price region, *i.e.*, maximizing the shortest distance from $\mathbb{E}[\hat{x}]$ to the boundaries of the polytope price regions while still holding the boundary constraints. The shortest distance can be calculated as

$$\beta = \min\{\tilde{\beta} : |\mathbb{E}[f_i] - T^{\max}| \geq \tilde{\beta} \text{ for all } i\}. \quad (2.19)$$

However, the existence of bad data detector prevents the bad data vector a from being arbitrarily large. According to (2.12), the weighted squared residue with a is

$$r^T R^{-1} r = z_a^T W z_a = (w + a)^T W (w + a). \quad (2.20)$$

since $WHx = 0$

Heuristically, since w has zero mean, the term $a^T W a$ can be used to quantify the effect of data perturbation on estimation residue. Then we use $a^T W a \leq \epsilon$ to control the detection probability in the following optimization.

Therefore, for a specific congestion pattern $\hat{\mathcal{C}}$, the adversary will solve the following optimization problem to move the state estimate to the “center” of the price region $\hat{\mathcal{C}}$ and keeping the detection probability low.

$$\begin{aligned} & \max_{a \in \mathcal{A}, \tilde{\beta} \geq 0} && \tilde{\beta} \\ & \text{subject to} && \mathbb{E}[f_i] - \tilde{\beta} \geq T_i^{\max}, i \in \hat{\mathcal{C}} \\ & && \mathbb{E}[f_i] + \tilde{\beta} < T_j^{\max}, j \notin \hat{\mathcal{C}} \\ & && a^T W a \leq \epsilon, \end{aligned} \quad (2.21)$$

which is a convex program that can be solved easily in practice. We call a region $\hat{\mathcal{C}}$ *feasible* if it makes problem (2.21) feasible.

Among all the feasible congestion patterns, the worst region $\hat{\mathcal{C}}^*$ is chosen as the one giving the largest ARPP.

$$\hat{\mathcal{C}}^* = \arg \max_{\hat{\mathcal{C}} \in \Gamma} |\tilde{\lambda}_i - \lambda_i(\hat{\mathcal{C}})|, \quad (2.22)$$

where $\tilde{\lambda}_i$ is the LMP at bus i if the x_0 is the system state, and Γ the set of all the feasible congestion patterns. Hence, the worst case constant bad data vector is the solution to optimization problem (2.21) by setting the congestion pattern as $\hat{\mathcal{C}}^*$.

2.4.3 Worst ARPP under Partially Adaptive Bad Data

For bad data model M2, only part of the measurement values in real-time are known to the adversary, denoted as z_o . The adversary has to first make an estimation of the system state from the observation and prior distribution, then make the attack decision based on the estimation result.

Without the presence of bad data vector, *i.e.*, $a = 0$, the system equation (2.5) gives

$$z_o = H_o x + w_o, \quad (2.23)$$

where H_o is the rows of H corresponding to the observed measurements and w_o the corresponding part in the measurement noise w .

The minimum mean square error (MMSE) estimate of x given z_o is given by the conditional mean

$$\mathbb{E}(x|z_o) = x_0 + \Sigma_x H_o^T (H_o \Sigma_x H_o^T)^{-1} (z_o - H_o x_0). \quad (2.24)$$

Then, the flow estimate on branch i after attack is

$$\mathbb{E}[f_i|z_o] = F_i \mathbb{E}[\hat{x}|z_o]. \quad (2.25)$$

Still, we want to move the estimation of state to the “center”. On the other hand, the expected measurement value $\mathbb{E}[z_a|z_o] = H\mathbb{E}[\hat{z}|z_o] + a$. Again, we need a pre-designed parameter ϵ to control the detection probability. Therefore, the solution to the following optimization problem is the best attack given congestion pattern \mathcal{A}

$$\begin{aligned} \max_{a \in \mathcal{A}, \tilde{\beta} \geq 0} \quad & \tilde{\beta} \\ \text{subject to} \quad & \mathbb{E}[f_i|z_o] - \tilde{\beta} \geq T_i^{\max}, i \in \hat{\mathcal{C}} \\ & \mathbb{E}[f_i|z_o] + \tilde{\beta} < T_j^{\max}, j \notin \hat{\mathcal{C}} \\ & (H\mathbb{E}[z_a|z_o]^T)W(H\mathbb{E}[z_a|z_o]) \leq \epsilon. \end{aligned} \quad (2.26)$$

This problem is also a convex optimization problem, which can be easily solved. Among all the $\hat{\mathcal{C}}$'s which make the above problem feasible, we choose the one with the largest price perturbation, denoted as $\hat{\mathcal{C}}^*$. The solution to problem (2.26) with $\hat{\mathcal{C}}^*$ as the congestion pattern is the worst bad data vector.

2.4.4 Worst ARPP under Fully Adaptive Bad Data

Finally, we consider the bad data model M3, in which the whole set of measurements z is known to the adversary. The worst bad data vector depends on the value of z . Different from the previous two models, with bad data vector a , the estimated state is deterministic without uncertainty. In particular

$$\hat{x} = Kz + Ka. \quad (2.27)$$

And the estimated flow on branch i after attack is also deterministic

$$\hat{f}_i = F_i \cdot \hat{x} = F_i \cdot Kz + F_i \cdot Ka. \quad (2.28)$$

Similar to the previous two models, congestion pattern is called feasible if there exists some bad data vector a to make the following conditions satisfied:

$$\begin{aligned} \hat{f}_i &\geq T_i^{\max}, i \in \hat{\mathcal{C}} \\ \hat{f}_i &< T_j^{\max}, j \notin \hat{\mathcal{C}} \\ (z + a)^T W(z + a) &\leq \tau, \quad a \in \mathcal{A}. \end{aligned} \quad (2.29)$$

Among all the feasible congestion patterns, we choose the one with the largest price perturbation, $\hat{\mathcal{C}}^*$. Any bad data vector a satisfying condition (2.29) can serve as the worst fully adaptive bad data.

2.4.5 A Greedy Heuristic

The strategies presented above are based on the exhaustive search over all possible congestion patterns. Such approaches are not scalable for large networks with a large number of possible congestion patterns. We now present a greedy heuristic approach aimed at reducing computation cost. In particular, we develop a gradient like algorithm that searches among a set of likely congestion patterns.

First, we restrict ourselves to the set of lines that are close to their respective flow limits and look for bad data that will affect the congestion pattern. The intuition is that it is unlikely that bad data can drive the system state sufficiently

far without being detected by the bad data detector. In practice, the cardinality of such a set is usually very small compared with the systems size.

Second, we search for the worst data locally by changing one line in the congestion pattern at a time. Specifically, suppose that a congestion pattern is the current candidate for the worst data. Given a set of candidate lines that are prone to congestions, we search locally by flipping one line at a time from the congested state to the un-congested state and vice versa. If no improvement can be made, the algorithm stops. Otherwise, the algorithm updates the current “worst congestion pattern” and continue. The effectiveness of this greedy heuristic is tested in Section 2.6.3.

2.5 Bad Topology Data on LMP

So far, we have considered bad data in the analog measurements. In this section, we include the bad *topology* data, and describe another bad data model.

We represent the network topology by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where each $i \in \mathcal{V}$ denotes a bus and each $(i, j) \in \mathcal{E}$ denotes a *connected* transmission line. For each physical transmission line (*e.g.*, a physical line between i and j), we assign an arbitrary direction (*e.g.*, (i, j)) for the line, and (i, j) is in \mathcal{E} if and only if bus i and bus j are connected.

Bad data may appear in both analog measurements and digital (*e.g.*, breaker

status) data, as described in Section 2.3.1:

$$\begin{aligned} z_a &= z + a = (Hx + w) + a, & a \in \mathcal{A}, \\ s_b &= s + b \pmod{2}, & b \in \mathcal{B}. \end{aligned} \tag{2.30}$$

As in Section 2.4, we employ the adversary model to describe the worst case. The adversary alters s to s_b by adding b from the set of feasible attack vectors $\mathcal{B} \subset \{0, 1\}^l$ such that the topology processor produces the “target” topology $\bar{\mathcal{G}}$ as the topology estimate. In addition, the adversary modifies z by adding $a \in \mathcal{A}$ such that z_a looks consistent with $\bar{\mathcal{G}}$.

In this section, we focus on the worst case when the adversary is able to alter the network topology without changing the state estimate[‡]. We also require that such bad data are generated by an adversary causing undetectable topology change, *i.e.*, the bad data escape the system bad data detection. For the worst case analysis, we will maximize the LMP perturbation among the attacks within this specific class. Even though this approach is suboptimal, the simulation results in Section 2.6 demonstrate that the resulting LMP perturbation is much greater than the worst case of the bad meter data.

Suppose the adversary wants to mislead the control center with the target topology $\bar{\mathcal{G}} = (\mathcal{V}, \bar{\mathcal{E}})$, a topology obtained by *removing*[§] a set of transmission lines \mathcal{E}_Δ in \mathcal{G} (*i.e.*, $\bar{\mathcal{E}} = \mathcal{E} \setminus \mathcal{E}_\Delta$). We assume that the system with $\bar{\mathcal{G}}$ is observable: *i.e.*,

[‡]In general, the adversary can design the worst data to affect both the state estimate and network topology. It is, however, much more difficult to make such attack undetectable.

[§]Line addition by the adversary is also possible [21]. However, compared to line removal attacks, line addition attacks require the adversary to observe a much larger set of meter measurements to design undetectable attacks. In addition, the number of necessary modifications in breaker data is also much larger: to make a line appear to be connected, the adversary should make all the breakers on the line appear to be closed. Please see [22] for the detail.

the corresponding measurement matrix \bar{H} has full column rank[¶].

Suppose that the adversary changes the breaker status such that the target topology $\bar{\mathcal{G}} = (\mathcal{V}, \bar{\mathcal{E}})$ is observed at the control center. Simultaneously, if the adversary introduces bad data $a = \bar{H}x - Hx$, then

$$z_a = Hx + a + w = \bar{H}x + w, \quad (2.31)$$

which means that the meter data received at the control center are completely consistent with the model generated from $\bar{\mathcal{G}}$. Thus, any bad data detector will not be effective.

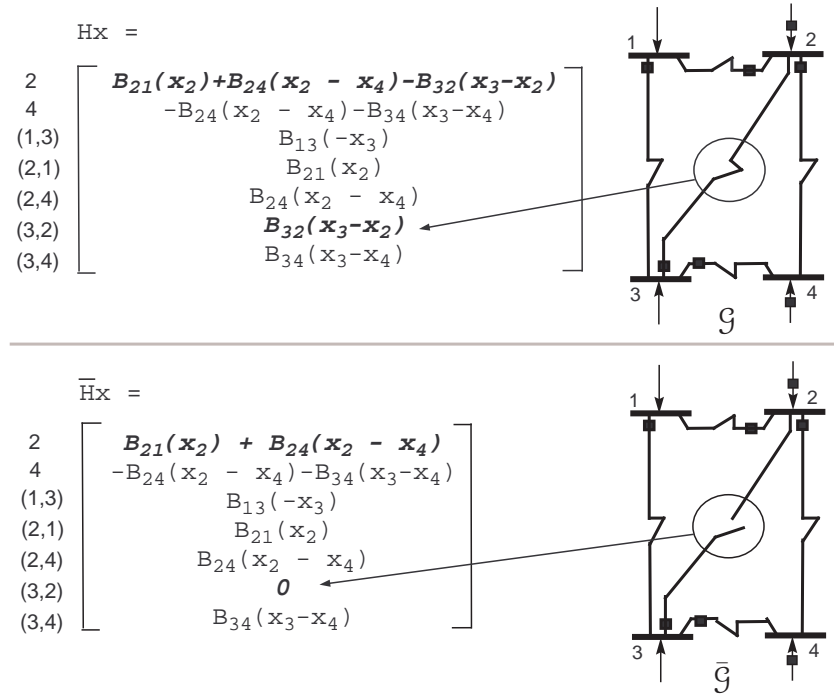
It is of course not obvious how to produce the bad data a , especially when the adversary can only modify a limited number of measurements, and it may not have access to the entire state vector x . Fortunately, it turns out that a can be generated by observing only a few entries in z without requiring global information (such as the state vector x) [21].

A key observation is that Hx and $\bar{H}x$ differ only in a few entries corresponding to the modified topology (lines in \mathcal{E}_Δ) as illustrated in Fig. 2.2. Consider first the noiseless case. Let z_{ij} denote the entry of z corresponding to the flow measurement from i to j . As hinted from Fig. 2.2, it can be easily seen that $\bar{H}x - Hx$ has the following sparse structure [21]:

$$\bar{H}x - Hx = - \sum_{(i,j) \in \mathcal{E}_\Delta} \alpha_{ij} m_{(i,j)}, \quad (2.32)$$

where $\alpha_{ij} \in \mathbb{R}$ denotes the line flow from i to j when the line is connected and the system state is x , and $m_{(i,j)}$ is the column of the measurement-to-branch incidence

[¶]Without observability, the system may not proceed to state estimation and real-time pricing. Hence, for the adversary to affect pricing, the system with the target topology has to be observable.



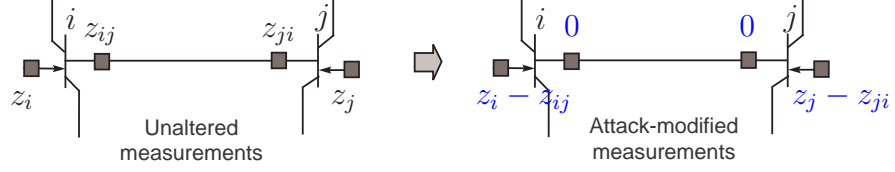


Figure 2.3: The attack modifies local measurements around the line (i, j) in \mathcal{E}_Δ .

2. Set z_{ij} and z_{ji} to be 0.

where z_i is the entry of z corresponding to the injection measurement at bus i .

When measurement noise is present (*i.e.*, $z = Hx + w$), the idea of the attack is still the same: to make a approximate $\bar{H}x - Hx$ so that z_a is close to $\bar{H}x + w$. Since $z_{ij} = \alpha_{ij} + w_{ij}$, z_{ij} is an unbiased estimate of α_{ij} for each $(i, j) \in \mathcal{E}_\Delta$, and this implies that $-\sum_{(i,j) \in \mathcal{E}_\Delta} z_{ij} m_{(i,j)}$ is an unbiased estimate of $-\sum_{(i,j) \in \mathcal{E}_\Delta} \alpha_{ij} m_{(i,j)} = \bar{H}x - Hx$. Hence, we set a to be $-\sum_{(i,j) \in \mathcal{E}_\Delta} z_{ij} m_{(i,j)}$, the same as in the noiseless setting, and the attack is executed by the same steps as above.

For launching this attack to modify the topology estimate from \mathcal{G} to $\bar{\mathcal{G}}$, the adversary should be able to (i) set b such that the topology processor produces $\bar{\mathcal{G}}$ instead of \mathcal{G} and (ii) observe and modify z_{ij} , z_{ji} , z_i , and z_j for all $(i, j) \in \mathcal{E}_\Delta$. The attack is feasible if and only if \mathcal{A} and \mathcal{B} contain the corresponding attack vectors.

To find the worst case LMP perturbation due to undetectable, state-preserving attacks, let \mathcal{F} denote the set of feasible $\bar{\mathcal{G}}$ s, for which the attack can be launched with \mathcal{A} and \mathcal{B} . Among the feasible targets in \mathcal{F} , we consider the best target topology that results in the maximum perturbation in real-time LMPs. If ARPP

is used as a metric, the best target is chosen as

$$\bar{\mathcal{G}}^*[z] = \arg \max_{\bar{\mathcal{G}} \in \mathcal{F}} \sum_i \left| \frac{\lambda_i(z; \bar{\mathcal{G}}) - \lambda_i(z; \mathcal{G})}{\lambda_i(z; \mathcal{G})} \right|. \quad (2.34)$$

where $\lambda_i(z; \bar{\mathcal{G}})$ denotes the real-time LMP at bus i when the attack with the target $\bar{\mathcal{G}}$ is launched on z , and $\lambda_i(z; \mathcal{G})$ is the real-time LMP under no attack.

2.6 Numerical Results

In this section, we demonstrate the impact of bad data on real-time LMPs with the numerical simulations on IEEE-14 and IEEE-118 systems. We conducted simulations in two different settings: the linear model with the DC state estimator and the nonlinear model with the AC state estimator. The former is usually employed in the literature for the ease of analysis whereas the latter represents the practical state estimator used in the real-world power system. In all simulations, the meter measurements consist of real power injections at all buses and real power flows (both directions) at all branches.

2.6.1 Linear model with DC state estimation

We first present the simulation results for the linear model with the DC state estimator. We modeled bus voltage magnitudes and phases as Gaussian random variables with the means equal to the day-ahead dispatched values and small standard deviations. In each Monte Carlo run, we generated a state realization from the statistical model, and the meter measurements were created by the DC model

with Gaussian measurement noise. Once the measurements were created, bad data were added in the manners discussed in Section 2.4 and Section 2.5. With the corrupted measurements, the control center executed the DC state estimation and the bad data test with the false alarm probability constraint 0.1. If the data passed the bad data test, real-time LMPs were evaluated based on the state estimation results. For IEEE-14 and IEEE-118 system, the network parameters^{||} are available in [23].

We used the number of meter data to be modified by the adversary as the metric for the attack effort. For the 14 bus system, in each Monte Carlo run, we randomly chose two lines, and the adversary was able to modify all the line flow meters on the lines and injection meters located at the ends of the lines. For the 118 bus system, we randomly chose three lines, and the adversary had control over the associated line and injection meters. Both state and topology attacks were set to control the same number of meter data^{**} so that we can fairly compare their impacts on real-time LMPs. As for the meter data attack, we only considered the lines that are close to their flow limits (estimated flows under M1 and M2, or actual flows under M3) as candidates for congestion pattern search. The threshold is chosen as 10MW in our simulation.

^{||}In addition to the network parameters given in [23], we used the following line limit and real-time offer parameters. In the IEEE-14 simulation, the generators at the buses 1, 2, 3, 6, and 8 had capacities 330, 140, 100, 100, and 100 MW and the real-time offers 15, 31, 30, 10, and 20 \$/MW. Lines (2, 3), (4, 5), and (6, 11) had line capacities 50, 50, and 20 MW, and other lines had no line limit. In the IEEE-118 simulation, the generators had generation costs arbitrarily selected from {20, 25, 30, 35, 40 \$/MW} and generation capacities arbitrarily selected from {200, 250, 300, 350, 400 MW}. Total 16 lines had the line capacities arbitrarily selected from {70, 90, 110 MW}, and other lines had no line limit. To handle possible occurrence of price spikes, we set the upper and lower price caps as 500\$/MW and -100\$/MW respectively. Total 1000 Monte Carlo runs were executed for each case.

^{**}Topology attacks need to make few additional modifications on breaker state data such that the target lines appear to be disconnected to the topology processor. However, for simplicity, we do not take into account this additional effort.

Fig. 2.4 is the plot of ARPPs^{††} versus detection probabilities of bad data. They show that even when bad data were detected with low probability, ARPPs were large, especially for the fully adaptive bad meter data and the bad topology data.

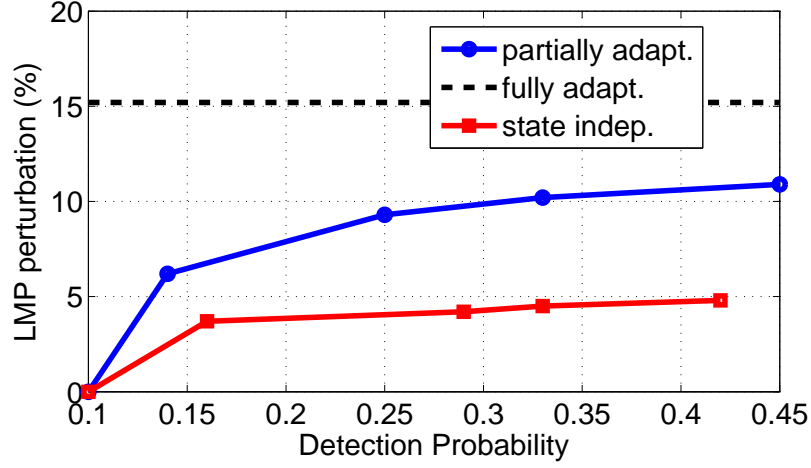
Comparing ARPPs of the three bad meter data models, we observe that the adversary may significantly improve the perturbation amount by exploiting partial or all real-time meter data (for the partially adaptive case, the adversary observed a half of all meters.) It is worthy to point out that bad topology data result in much greater price perturbation than bad meter data.

Recall the discussion in Section 2.2 and Section 2.5 that bad topology data and bad meter data employ different price-perturbing mechanisms: bad topology data perturb real-time LMP by restructuring the price regions without perturbing the state estimate (the line-removal attack introduced in Section 2.5 does not perturb state estimate) whereas bad meter data perturb real-time LMP by simply moving the state estimate to a different price region. Therefore, the observation implies that restructuring the price regions has much greater impact on real-time LMP than merely perturbing the state estimate.

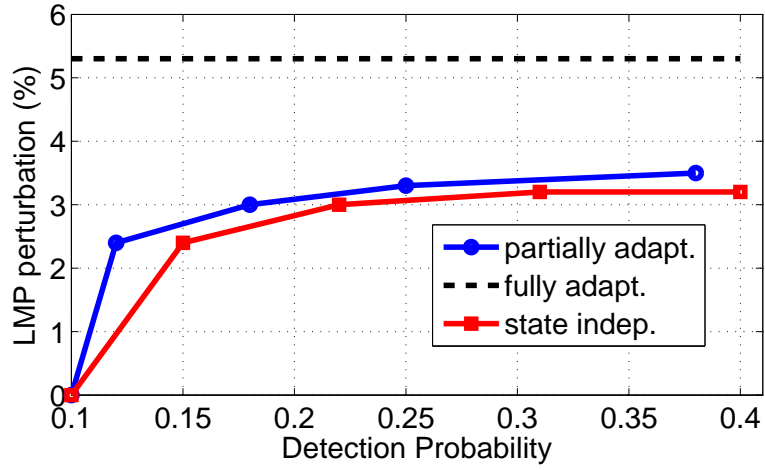
2.6.2 Nonlinear model with AC state estimation

The simulations with the nonlinear model intend to investigate the vulnerability of the real-world power system to the worst adversarial act, designed based on the

^{††}The detection probabilities for the fully adaptive bad meter data and the bad topology data cases were less than 0.1 in all the simulations. In the figures, we draw ARPPs of those cases as horizontal lines so that we can compare them with other cases.



(a) IEEE-14: ARPP of the worst topology data is 66.1%.



(b) IEEE-118: ARPP of the worst topology data is 22.4%.

Figure 2.4: Linear model: ARPP vs detection prob.

linear model. The simulations were conducted on IEEE-14 and IEEE-118 systems in the same manner as the linear case except that we employed the nonlinear model and the AC state estimation.

Fig. 2.5 is the plot of ARPPs versus detection probabilities. The result shows that the proposed methodology can affect the system to some extent even when nonlinear estimator is used, especially when the bad data are present in the topol-

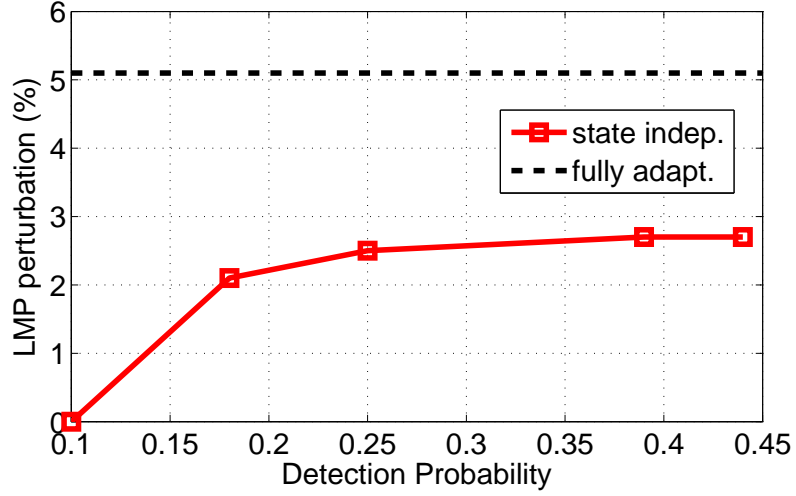
ogy data, although the nonlinear estimator makes this effect relatively less significant compared with the linear case results.

2.6.3 Performance of the greedy search heuristic

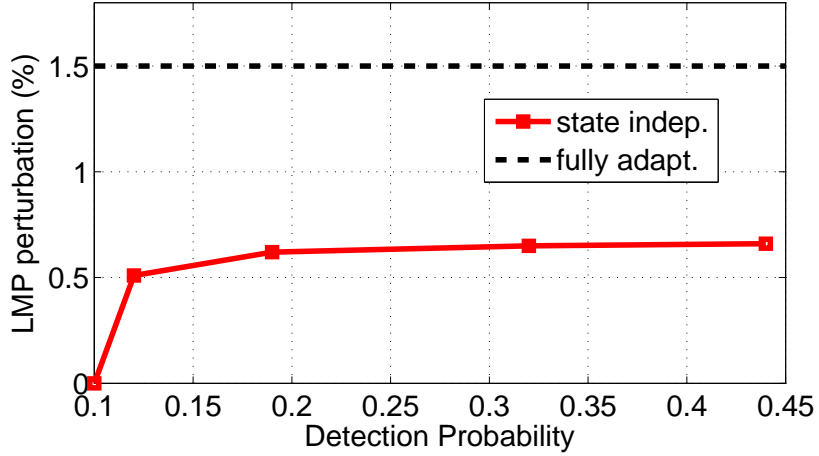
We also conducted simulation based on the proposed greedy search technique in Section 2.4.5. The simulation was based on 118 bus system, and all parameters were the same as those presented in Section 2.6.1. We compared the performance and computation time of the greedy heuristics with exhaustive search benchmark, as shown in Table 2.1. Notice here the exhaustive search and greedy search are both over the lines that are close to their flow limits (estimated flows under M1 and M2, or actual flows under M3), the same as in Section 2.6.1. In Table 2.1, the second column (average search time) is the average searching time for worst congestion pattern over 1000 Monte Carlo runs, and the third column (accuracy) is the percentage that the greedy search find the same worst congestion pattern as the exhaustive search. From the result, we can see that using greedy heuristic can give us much faster processing algorithm without losing much of the accuracy.

Table 2.1: Performance of greedy search method

method	average search time	accuracy
exhaustive search	1.23s	-
greedy search	0.51s	97.3%



(a) IEEE-14: ARPP of the worst topology data is 95.4%.



(b) IEEE-118: ARPP of the worst topology data is 76.9%.

Figure 2.5: Nonlinear model: ARPP vs detection prob.

2.7 Conclusion

We report in this paper a study on impacts of worst data on the real-time market operation. A key result of this paper is the geometric characterization of real-time LMP given in Theorem 2.2.1. This result provides insights into the relation between data and the real-time LMP; it serves as the basis of characterizing impacts

of bad data.

Our investigation includes bad data scenarios that arise from both analog meter measurements and digital breaker state data. To this end, we have presented a systematic approach by casting the problem as one involving an adversary injecting malicious data. While such an approach often gives overly conservative analysis, it can be used as a measure of assurance when the impacts based on worst case analysis are deemed acceptable. We note that, because we use adversary attacks as a way to study the worst data, our results have direct implications when cybersecurity of smart grid is considered. Given the increasing reliance on information networks, developing effective countermeasures against malicious data attack on the operations of a future smart grid is crucial. See [8, 24, 10, 22] for discussion about countermeasures.

From a practical viewpoint, our result can serve as the guideline to the real-time operation. Following the methodology in our paper, worst effect of a specific set of meters on real-time LMP can be checked. Once a huge potential perturbation is detected, alarm should be made and the operator needs to check the accuracy of these specific data, add protection devices, or even add more redundant meters.

Although our findings are obtained from academic benchmarks involving relatively small size networks, we believe that the general trend that characterizes the effects of bad data is likely to persist in practical networks of much larger size. In particular, as the network size increases and the number of simultaneous appearance of bad data is limited, the effects of the worst meter data on LMP decrease whereas the effects of the worst topology data stay nonnegligible regardless of the

network size. This observation suggests that the bad topology data are potentially more detrimental to the real-time market operation than the bad meter data.

CHAPTER 3

DATA ATTACK ON LMP IN TIME-COUPLED LOOK-AHEAD DISPATCH

3.1 Introduction

The main objective of this chapter is to study the impact of cyber data attacks on state estimation, which subsequently influence the result of the existing *static* and newly emerging *look-ahead* dispatch models in the real-time power market. Figures 1(a),(b) illustrate the information flow in a three-layered framework (with physical, measurement, and control/computation layer) without and with such cyber attacks, respectively. The information includes the physical state such as the nodal power injection and flow and the dispatch instruction such as the optimal generation output and nodal price. Compared to Figure 1(a), Figure 1(b) describes that bad/malicious data injected into the measurement layer can lead to corrupted estimation of the states of the physical layer. Consequently, the attacker could distort the feedback information from control/communication layer back to the physical layer in two ways, leading to (1) physical insecurity in the power grid operations, and/or (2) financial misconduct in the power markets as shown in Figures 1(b). This chapter contributes to topic (2) using realistic dispatch models in power markets.

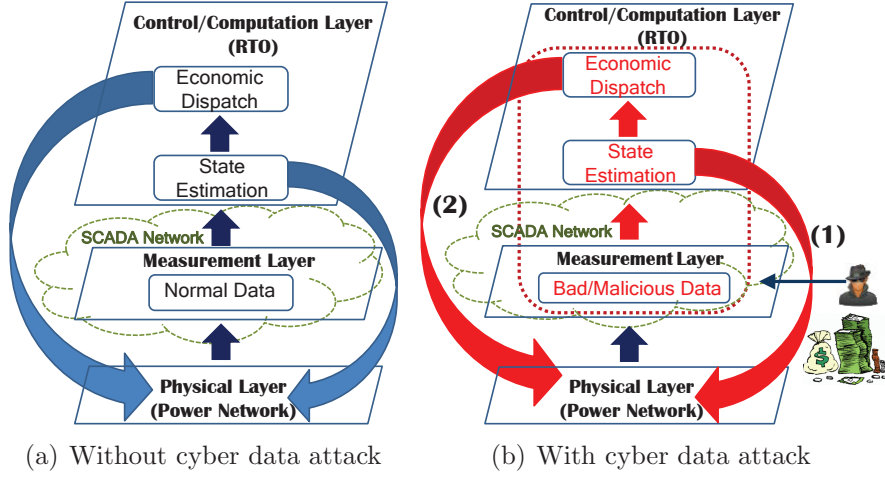


Figure 3.1: A three-layered framework illustrating cyber data attack.

3.1.1 Literature Review

A large body of literature has been accumulated recently on the subject of cyber security in power grids, ranging from risk mitigation [25], generation control security (e.g., automatic generation control (AGC) attack [26], [27]), control security in distribution system [28], and privacy protection [29], [30], [31], [32]. A concise summary paper is presented in [33], including risk assessment methodology, power system control application and cyber infrastructure security. Meanwhile, many researchers have been studying *false data injection attacks*, which malfunction the state estimator by injecting false data into sensors. For the subject of false data injection attacks, two major categories of work have been presented:

- *Vulnerability analysis of state estimation*: a false data injection attack was formulated and analyzed in [34], [35]. Efficient algorithm to find sparse attacks and Phasor Measurement Units (PMUs) placement algorithm to prevent sparse attacks were developed in [36], [37]. A distributed joint detection-estimation approach to malicious data attack was presented in [38]. In [39],

it was shown that the attacker can hack the power grid without the knowledge of the power network topology, which can be estimated using linear independent component analysis (ICA).

- *Financial risk analysis in electricity market operations:* this area examined the economic impact of false data injection attacks on electricity market operations. In [40], undetectable and profitable attack strategy was formulated in the real-time electricity market. In [41], the scenario for the attacker and defender was modeled as a zero-sum game between them, and simulation results showed the effectiveness of attack on the real-time market prices.

3.1.2 Report Organization

The remainder of this chapter is organized as follows. Section 3.2 provides the brief overview of DC state estimation and real-time power market with static dispatch and look-ahead dispatch models. Section 3.3 illustrates the attack model and attack undetectability. Section 3.4 presents a new class of cyber data attacks on static dispatch, which is followed by cyber data attack on look-ahead dispatch in Section 3.5. In these sections, undetectable and profitable attack strategies are formulated and their performance is evaluated in real-time power markets in the IEEE 14-bus system. Section 3.6 presents the conclusions and future work.

3.2 Preliminaries

The notations used in this section are summarized in Table 3.1.

Table 3.1: Notations.

i	Index for generators i
n	Index for buses n
l	Index for transmission line l
K	Total number of sampling period
N	Total number of buses
L	Total number of transmission lines
M	Total number of measurements
G	Set of generation units
G_M	Set of marginal units
\underline{G}_M^c	Set of binding units with lower marginal cost than marginal unit
\overline{G}_M^c	Set of binding units with higher marginal cost than marginal unit
D	Set of demands
D_n	n th bus fixed demand
$D_n[k]$	n th bus fixed demand at time k
$P_{gi}[k]$	Scheduled i th generator power at time k
F_l	Transmission flow at line l
$F_l[k]$	Transmission flow at line l at time k
R_i	Ramp rate of generator i
ΔT	Dispatch interval
$P_{gi}^{\min}, P_{gi}^{\max}$	Min/max generation limits for generator i
F_l^{\min}, F_l^{\max}	Min/max flow limits at line l

3.2.1 DC State Estimation Model

We consider the linearized DC state estimation model:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} = \begin{bmatrix} \mathbf{I} \\ \mathbf{H}^d \end{bmatrix} \mathbf{x} + \mathbf{e}, \quad (3.1)$$

where \mathbf{x} is the state vector (nodal power injections), \mathbf{z} is the measurement vector (power injection and flow measurements), \mathbf{e} is the independent identically distributed (i.i.d.) Gaussian measurement error vector following $\mathcal{N}(0, \mathbf{R})$, and \mathbf{H} is the system factor matrix specifying the relationship between \mathbf{x} and \mathbf{z} . Here the matrix \mathbf{H} is concatenated with two submatrices, \mathbf{H}^d and \mathbf{I} , which denote the distribution factor matrix and the identity matrix, respectively. The state estimation problem is to find the optimal estimate of \mathbf{x} to minimize the weighted least square of measurement error:

$$\begin{aligned} & \text{minimize} \quad J(\mathbf{x}) = \mathbf{r}^T \mathbf{R}^{-1} \mathbf{r} \\ & \text{s.t.} \quad \mathbf{r} = \mathbf{z} - \mathbf{H}\mathbf{x}, \end{aligned} \tag{3.2}$$

where \mathbf{r} is the estimated residual vector. If the system is observable (i.e., the system factor matrix \mathbf{H} is full rank), the unique weighted least squares estimate of \mathbf{x} is given by

$$\hat{\mathbf{x}}(\mathbf{z}) = (\mathbf{H}^T \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{R}^{-1} \mathbf{z} = \mathbf{B}\mathbf{z}. \tag{3.3}$$

3.2.2 Economic Dispatch Model

The electric power market consists of two-settlement system, day-ahead and real-time spot markets. In real-time spot markets, LMP is obtained as the by-product of security constrained economic dispatch (SCED) in either of the two main pricing models: Ex-ante (e.g. in ERCOT, NY ISO) and Ex-post (e.g. in ISO New England, PJM, and Midwest ISO) [42].

The Ex-ante Model: In ex-ante real-time market models, LMPs are computed before the actual deployment of dispatch orders. For the system operator, the Ex-ante dispatch is formulated as follows [43]:

$$\min_{P_{g_i}} \sum_{i \in G} C_i(P_{g_i}) \quad (3.4)$$

s.t.

$$\sum_{i \in G} P_{g_i} = \sum_{n=1}^N D_n \quad (3.5)$$

$$\hat{P}_{g_i}^{\min} \leq P_{g_i} \leq \hat{P}_{g_i}^{\max} \quad \forall i \in G \quad (3.6)$$

$$F_l^{\min} \leq F_l \leq F_l^{\max} \quad \forall l = 1, \dots, L \quad (3.7)$$

where

$$\begin{aligned} \hat{P}_{g_i}^{\max} &= \min\{P_{g_i}^{\max}, \hat{P}_{g_i}(\mathbf{z}) + R_i \Delta T\} \\ \hat{P}_{g_i}^{\min} &= \max\{P_{g_i}^{\min}, \hat{P}_{g_i}(\mathbf{z}) - R_i \Delta T\}. \end{aligned}$$

In this formulation, the objective function is to minimize the total generation costs in (3.4). (3.5) is the system-wide energy balance equation. (3.6) is the physical capacity constraints of each generator embedded with its ramp constraints. (3.7) is the transmission line constraints.

The Ex-post Model: In ex-post real-time market models, LMPs are computed after the fact using real-time estimates for settlement purposes. Assuming no demand elasticity, the Ex-post dispatch is written as [44]:

$$\min_{P_{g_i}} \sum_{i \in G} C_i(P_{g_i}) \quad (3.8)$$

s.t.

$$\sum_{i \in G} \Delta P_{g_i} = 0 \quad (3.9)$$

$$\Delta P_{g_i}^{\min} \leq \Delta P_{g_i} \leq \Delta P_{g_i}^{\max} \quad \forall i \in G \quad (3.10)$$

$$\Delta F_l \leq 0 \quad \forall l \in \mathcal{CL}_+ \quad (3.11)$$

$$\Delta F_l \geq 0 \quad \forall l \in \mathcal{CL}_- \quad (3.12)$$

where

$$\begin{aligned} \Delta P_{g_i} &= P_{g_i} - \hat{P}_{g_i}(\mathbf{z}), \quad \Delta F_l = F_l - \hat{F}_l(\mathbf{z}) \\ \mathcal{CL}_+ &= \{l : \hat{F}_l(\mathbf{z}) \geq F_l^{\max}\}, \quad \mathcal{CL}_- = \{l : \hat{F}_l(\mathbf{z}) \leq F_l^{\min}\} \end{aligned}$$

and $\Delta P_{g_i}^{\max}$ and $\Delta P_{g_i}^{\min}$ are usually chosen to be 0.1MWh and -2MWh, respectively.

The Lagrangian of the above minimization problem is defined as

$$\begin{aligned} \mathcal{L} &= \sum_{i \in G} C_i(P_{g_i}) - \lambda \sum_{i \in G} \Delta P_{g_i} + \sum_{i \in G} \mu_{i,\max} (\Delta P_{g_i} - \Delta P_{g_i}^{\max}) + \\ &\quad \sum_{i \in G} \mu_{i,\min} (\Delta P_{g_i}^{\min} - \Delta P_{g_i}) + \sum_{l \in \mathcal{CL}_+} \eta_l \Delta F_l + \sum_{l \in \mathcal{CL}_-} \zeta_l (-\Delta F_l) \end{aligned} \quad (3.13)$$

It is well known that the optimal solution of the optimization problem must satisfy the KKT conditions. In particular, we know that the following holds: $\eta_l \geq 0$, $\zeta_l \geq 0$. To simplify the notation, we define $\eta_l = 0$ if $l \notin \mathcal{CL}_+$, $\zeta_l = 0$ if $l \notin \mathcal{CL}_-$. We can define the nodal price at each bus n ($n = 2, \dots, N$), given by

$$\lambda_n = \lambda + \sum_{l=1}^L (\eta_l - \zeta_l) \frac{\partial F_l}{\partial D_n}. \quad (3.14)$$

Now let us write (3.14) in a more compact matrix form. Let us define $\eta = [\eta_1, \dots, \eta_L]'$ to be a vector of all η_l and $\zeta = [\zeta_1, \dots, \zeta_L]'$. Since $\partial F_l / \partial D_n = H_{ln}^d$ where H_{ln}^d is the element on the l th row and n th column of \mathbf{H}^d , (3.14) can be simplified as

$$\lambda_n = \lambda + \mathbf{H}_n^{dT} (\eta - \zeta), \quad (3.15)$$

where $\mathbf{H}_{\mathbf{n}}^{\mathbf{d}}$ is the n th column of $\mathbf{H}^{\mathbf{d}}$ matrix. The difference of price at two nodes n_1 and n_2 is given by

$$\lambda_{n_1} - \lambda_{n_2} = (\mathbf{H}_{\mathbf{n}_1}^{\mathbf{d}} - \mathbf{H}_{\mathbf{n}_2}^{\mathbf{d}})^T (\eta - \zeta). \quad (3.16)$$

Look-ahead Dispatch Model: Recently, due to limited predictability in day-ahead and high inter-temporal variability of renewable resources (e.g., wind and solar), RTOs are upgrading real-time market clearing engine from static dispatch to look-ahead dispatch models for more flexible operations in support of high penetration of variable resources [45]. For the system operator, look-ahead dispatch is formulated as follows,

$$\min_{P_{g_i}[k]} \sum_{k=1}^K \sum_{i \in G} C_i(P_{g_i}[k]) \quad (3.17)$$

s.t.

$$\sum_{i \in G} P_{g_i}[k] = \sum_{n=1}^N D_n[k] \quad \forall k = 1, \dots, K \quad (3.18)$$

$$|P_{g_i}[k] - P_{g_i}[k-1]| \leq R_i \Delta T \quad \forall k = 1, \dots, K \quad (3.19)$$

$$P_{g_i}^{\min} \leq P_{g_i}[k] \leq P_{g_i}^{\max} \quad \forall k = 1, \dots, K \quad (3.20)$$

$$F_l^{\min} \leq F_l[k] \leq F_l^{\max} \quad \forall k = 1, \dots, K, \forall l = 1, \dots, L. \quad (3.21)$$

In this formulation, the objective function is to minimize the total generation costs in (3.17). (3.18) is the system-wide energy balance equations. (3.19) and (3.20) are the ramp constraints and the physical capacity constraints of each generator, respectively. (3.21) is the transmission line constraints. In this paper, we define one-step look-ahead dispatch with $K = 1$ as static dispatch. The Lagrangian

function of the aforementioned look-ahead dispatch is written as

$$\begin{aligned}
\mathcal{L} = & \sum_{k=1}^K \sum_{i \in G} C_i(P_{g_i}[k]) - \sum_{k=1}^K \lambda[k] \left[\sum_{i \in G} P_{g_i}[k] - \sum_{n=1}^N D_n[k] \right] \\
& + \sum_{k=1}^K \sum_{i \in G} [\omega_{i,\max}[k](P_{g_i}[k] - P_{g_i}[k-1] - R_i \Delta T)] \\
& + \sum_{k=1}^K \sum_{i \in G} [\omega_{i,\min}[k](P_{g_i}[k-1] - P_{g_i}[k] - R_i \Delta T)] \\
& + \sum_{k=1}^K \sum_{i \in G} [\tau_{i,\max}[k](P_{g_i}[k] - P_{g_i}^{\max})] + \sum_{k=1}^K \sum_{i \in G} [\tau_{i,\min}[k](P_{g_i}^{\min} - P_{g_i}[k])] \\
& + \sum_{k=1}^K \sum_{l=1}^L [\mu_{l,\max}[k](F_l[k] - F_l^{\max})] + \sum_{k=1}^K \sum_{l=1}^L [\mu_{l,\min}[k](F_l^{\min} - F_l[k])],
\end{aligned}$$

where all the Lagrangian multipliers at time k ($\lambda[k]$, $\omega_{i,\max}[k]$, $\omega_{i,\min}[k]$, $\tau_{i,\max}[k]$, $\tau_{i,\min}[k]$, $\mu_{l,\max}[k]$, and $\mu_{l,\min}[k]$) are positive. According to the definition of the nodal price [46], and assuming that bus 1 is the slack bus, the locational marginal price (LMP) for each bus n ($n = 2, \dots, N$) at time k is given by

$$\lambda_n[k] = \lambda[k] - \mathbf{H}_n^{\mathbf{d}T}(\mu_{\max}[k] - \mu_{\min}[k]), \quad (3.22)$$

where $\lambda[k]$ is the LMP for the slack bus 1 at time k , $\mathbf{H}_n^{\mathbf{d}} = [\frac{\partial F_1}{\partial D_n}, \dots, \frac{\partial F_L}{\partial D_n}]^T$, $\mu_{\max}[k] = [\mu_{1,\max}[k], \dots, \mu_{L,\max}[k]]^T$, and $\mu_{\min}[k] = [\mu_{1,\min}[k], \dots, \mu_{L,\min}[k]]^T$.

Alternatively, by the first-order KKT condition of look-ahead dispatch formulation, the LMP for each generator i connected to bus n is written as

$$\begin{aligned}
\lambda_i[k] = & \frac{\partial C_i(P_{g_i}[k])}{\partial P_{g_i}[k]} + (\tau_{i,\max}[k] - \tau_{i,\min}[k]) \\
& + (\omega_{i,\max}[k] - \omega_{i,\max}[k+1]\mathbb{1}_A[k]) + (\omega_{i,\min}[k+1]\mathbb{1}_A[k] - \omega_{i,\min}[k]), \quad (3.23)
\end{aligned}$$

where $\mathbb{1}_A[k]$ is the indicator function based on the set $A = \{1 \leq k \leq K-1\}$. In other words, $\mathbb{1}_A[k]=1$ when $k \in A$, otherwise (i.e., $k \in A^c = \{k = K\}$) $\mathbb{1}_A[k]=0$. We can observe from (3.23) that the Lagrangian multipliers, $\omega_{i,\max}[k+1]$ and

$\omega_{i,\min}[k+1]$, corresponding to the ramp constraints at the future time $k+1$ influence the LMPs calculation at the current time k . However, the LMP formulation in static dispatch (one-step look-ahead) does not capture future constraints.

3.3 Attack Model and Undetectability

We consider the additive attack measurement model:

$$\mathbf{z}_{\mathbf{a}} = \mathbf{H}\mathbf{x} + \mathbf{e} + \mathbf{a}, \quad (3.24)$$

where \mathbf{a} is the attack vector, which leads to the corrupted measurement vector $\mathbf{z}_{\mathbf{a}}$. The new residual vector $\mathbf{r}_{\mathbf{a}}$ can be decomposed into two terms, corresponding to without and with attack, respectively:

$$\mathbf{r}_{\mathbf{a}} = \mathbf{r} + (\mathbf{I} - \mathbf{H}\mathbf{B})\mathbf{a} \quad (3.25)$$

, and by triangular inequality of the L_2 -norm $\|\cdot\|_2$,

$$\|\mathbf{r}_{\mathbf{a}}\|_2 = \|\mathbf{r} + (\mathbf{I} - \mathbf{H}\mathbf{B})\mathbf{a}\|_2 \quad (3.26)$$

$$\leq \|\mathbf{r}\|_2 + \|(\mathbf{I} - \mathbf{H}\mathbf{B})\mathbf{a}\|_2 < \eta, \quad (3.27)$$

where η is the bad data detection threshold. For bypassing the bad data detection algorithm, the attacker aims at constructing the attack vector \mathbf{a} so that the value of $\|(\mathbf{I} - \mathbf{H}\mathbf{B})\mathbf{a}\|_2$ added to $\|\mathbf{r}\|_2$ still makes the above undetectable condition hold true.

3.4 Spatial Data Attack on Static Dispatch

3.4.1 Problem Formulation

We assume that the attacker will exploit the virtual bidding mechanism to make a profit. In many RTOs such as ISO-New England, virtual bidding activities are legitimate financial instruments in electricity markets. A market participant purchase/sell a certain amount of virtual power at location in day-ahead forward market, and will be obliged to sell/purchase the exact same amount in the subsequent real-time market. Therefore, the attacker's action can be summarized as:

1. In day-ahead forward market, buy and sell virtual power P_O at locations n_1 and n_2 at price $\lambda_{n_1}^{DA}$, $\lambda_{n_2}^{DA}$, respectively.
2. Inject the attack vector \mathbf{a} to manipulate the nodal price of ex-post market.
3. In ex-post market, sell and buy virtual power P_O at locations n_1 and n_2 at price λ_{n_1} , λ_{n_2} , respectively.

The profit that the attacker could obtain from this combination of virtual trading is

$$\text{Profit} = (\lambda_{n_1} - \lambda_{n_1}^{DA}) P_O + (\lambda_{n_2}^{DA} - \lambda_{n_2}) P_O = (\lambda_{n_1} - \lambda_{n_2} + \lambda_{n_2}^{DA} - \lambda_{n_1}^{DA}) P_O. \quad (3.28)$$

Let us define

$$p = \lambda_{n_1} - \lambda_{n_2} + \lambda_{n_2}^{DA} - \lambda_{n_1}^{DA} \quad (3.29)$$

Combined with (3.16), (3.29) can be written as

$$p(\mathbf{z}_a) = (\mathbf{H}_{n_1}^d - \mathbf{H}_{n_2}^d)^T (\eta(\mathbf{z}_a) - \xi(\mathbf{z}_a)) + \lambda_{n_2}^{DA} - \lambda_{n_1}^{DA}. \quad (3.30)$$

3.4.2 Attack Strategy

In this subsection, we consider two scenarios where the subset of compromised sensors is fixed and only a limited number of measurement sensors could be compromised.

Scenario I: predetermined subset of compromised sensors

We develop a heuristic for the attacker to find a profitable input \mathbf{a} when the subset of compromised sensors is fixed. We will show that such a problem can be effectively formulated as a convex optimization problem and solved efficiently. Let us define the set

$$L_+ = \{l : H_{ln_1}^d > H_{ln_2}^d\}, \quad L_- = \{l : H_{ln_1}^d < H_{ln_2}^d\}.$$

As a result, $p(\mathbf{z}_a)$ can be written as

$$\begin{aligned} p(\mathbf{z}_a) &= \sum_{l \in L_+} (H_{ln_1}^d - H_{ln_2}^d) (\eta_l(\mathbf{z}_a) - \zeta_l(\mathbf{z}_a)) \\ &+ \sum_{l \in L_-} (H_{ln_2}^d - H_{ln_1}^d) (\zeta_l(\mathbf{z}_a) - \eta_l(\mathbf{z}_a)) + \lambda_{n_2}^{DA} - \lambda_{n_1}^{DA}. \end{aligned} \quad (3.31)$$

By the fact that $\eta_l(\zeta_l)$ is nonnegative and it is 0 if the line is not positive (or negative) congested, we can see that the following conditions are sufficient for $p(\mathbf{z}_a) > 0$

$$(A1) \quad \lambda_{n_2}^{DA} > \lambda_{n_1}^{DA}.$$

(A2) $\hat{F}_l' < F_l^{\max}$ if $l \in L_-$, i.e., the line is not positive congested.

(A3) $\hat{F}_l' > F_l^{\min}$ if $l \in L_+$, i.e., the line is not negative congested.

(A1) can be easily satisfied in the day-ahead market. Hence, the attacker needs to manipulate the measurement to make sure that (A2) and (A3) hold or at least hold with a large probability. Following such intuition, we give the following definition:

Definition 3.4.1. *An attack input \mathbf{a} is called δ -profitable if the following inequalities hold*

$$\mathbb{E}[\hat{F}_l'] \leq F_l^{\max} - \delta, \quad \forall l \in L_-, \quad (3.32)$$

$$\mathbb{E}[\hat{F}_l'] \geq F_l^{\min} - \delta, \quad \forall l \in L_+, \quad (3.33)$$

where $\mathbb{E}[\hat{F}_l'] = F^* + \mathbf{H}^d \mathbf{B} \mathbf{a}$ and F^* is the result of the ex-ante dispatch.

Remark 1. *It is worth mentioning that δ does not directly relate to the profit (or expected profit). However, it is related to the probability that (A2) and (A3) hold. Recall that from the attacker's perspective, \hat{F}_l' is a Gaussian random variable with mean $\mathbb{E}[\hat{F}_l']$. As a result, a large margin will guarantee that with large probability (A2) and (A3) are not violated.*

Therefore, the attackers strategy during the run time is to find an ϵ feasible \mathbf{a} such that the margin δ is maximized. The problem can be formulated as

$$\max_{\mathbf{a} \in \text{span}(\mathcal{A})} \delta \quad (3.34)$$

s.t.

$$||(\mathbf{I} - \mathbf{HB})\mathbf{a}||_2 \leq \epsilon \quad (3.35)$$

$$\mathbb{E}[\hat{F}'_l] \leq F_l^{\max} - \delta, \quad \forall l \in L_-, \quad (3.36)$$

$$\mathbb{E}[\hat{F}'_l] \geq F_l^{\min} - \delta, \quad \forall l \in L_+, \quad (3.37)$$

$$\delta > 0 \quad (3.38)$$

where the set \mathcal{A} represents the attack vector space, which describes the attack pattern related to the type and number of compromised sensors. It is easy to verify that the objective function and all the constraints are convex. Therefore, the problem itself is a convex programming problem and can be solved efficiently.

Scenario II: limited resources to compromise sensors

We consider a scenario in which the attacker can select the set of sensors to compromise. However, due to limited resources, the total number of compromised sensor cannot exceed certain threshold κ . As a result, not only does the attacker need to design an optimal input to system, but also it need to choose the optimal set of sensors to compromise.

Following the previous argument, we can write the optimization problem as

$$\max_{\mathbf{a} \in \text{span}(\mathcal{A})} \delta \quad (3.39)$$

s.t.

$$||(\mathbf{I} - \mathbf{HB})\mathbf{a}||_2 \leq \epsilon \quad (3.40)$$

$$\mathbb{E}[\hat{F}'_l] \leq F_l^{\max} - \delta, \quad \forall l \in L_-, \quad (3.41)$$

$$\mathbb{E}[\hat{F}'_l] \geq F_l^{\min} - \delta, \quad \forall l \in L_+, \quad (3.42)$$

$$\delta > 0 \quad (3.43)$$

$$||\mathbf{a}||_0 \leq \kappa, \quad (3.44)$$

where $\|\cdot\|_0$ is the zero norm, which is defined as the number of nonzero elements in a vector. Note that in this formulation we do not require that \mathbf{a} lies in the span of \mathcal{A} , but instead we require \mathbf{a} to have no more than κ nonzero elements. The nonzero elements of \mathbf{a} correspond to the sensors the attacker needs to compromise.

However, the above formulation is a hard combinatorial problem, since it involves a constraint involving the zero norm of a vector, which is not convex. To render the problem solvable, we resort to a convex relaxation of the original optimization problem. The L_0 norm is substituted with a weighted L_1 norm, where the weights are chosen to avoid the penalization, given by the L_1 norm, of the bigger coefficients. In that paper, the authors propose an iterative algorithm that alternates between an estimation phase and a redefinition the weights, based on the empiric consideration that the weights should relate inversely to the true signal magnitudes. The resulting algorithm is composed of the following four steps:

1. Set the iteration count c to zero and set the weights vector to $\omega_i^0 = 1$ for $i = 1, \dots, N_m$. (N_m is a total number of measurements)
2. Solve the weighted L_1 minimization problem

$$\max_{\mathbf{a} \in \text{span}(\mathcal{A})} \delta \quad (3.45)$$

s.t.

$$\|(\mathbf{I} - \mathbf{HB})\mathbf{a}\|_2 \leq \epsilon \quad (3.46)$$

$$\mathbb{E}[\hat{F}_l'] \leq F_l^{\max} - \delta, \quad \forall l \in L_-, \quad (3.47)$$

$$\mathbb{E}[\hat{F}_l'] \geq F_l^{\min} - \delta, \quad \forall l \in L_+, \quad (3.48)$$

$$\delta > 0 \quad (3.49)$$

$$\sum_i z_i^a \omega_i^c \leq \kappa, \quad (3.50)$$

Let the solution be $z_1^{a,c}, \dots, z_{N_m}^{a,c}$.

3. Update the weights

$$\omega_i^{c+1} = \frac{1}{z_i^{a,c} + \zeta}, \quad i = 1, \dots, N_m$$

where ζ is a small positive constant.

4. Terminate on convergence or when c reaches a specified maximum number of iterations c_{\max} . Otherwise, increment c and go to step 2.

3.4.3 Simulation Studies

In this subsection we consider the standard IEEE 14-bus system to discuss the economic impact of malicious data attacks against state estimation. The system comprises a total of five generators. Three cases, summarized in Table 3.2, are analyzed. In Case I, only one transmission line is congested and two line flow sensors are assumed to be compromised using false data injection attack. In Cases II and III, we assume there are multiple congested transmission lines. Compared with Case II, Case III only allows a limited number of sensors which can be compromised. As a result, the attacker needs to both pick a subset of sensors and its input.

Table 3.2: Case Description

Case	congested lines in day-ahead	virtual bidding nodes	compromised sensors
I	1-2	2 and 4	line flow sensors 1-2, 3-4
II	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3, 2-4
III	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3

In Cases I and II, an attacker follows the procedure described in Scenario I with the purpose of gaining profit from virtual bidding. In Case III, the attacker

follows the limited sensor attack algorithm described in Scenario II. At the pair of the nodes that are prespecified in the third column of Table 3.2, the attacker buys and sells the same amount of virtual power in day-ahead market at nodes n_1 and n_2 , respectively. Based on historical trends, the attacker buys at the lower priced node and sell at the higher priced node. In real-time market operations, the attacker compromises the selected line flow sensors by injecting false data without being detected. By doing so, the congested transmission lines in day-ahead operations appear no longer congested from the system state estimation. This, in turn, will result different real-time ex-post LMPs with controllable bias compared to the day-ahead LMPs.

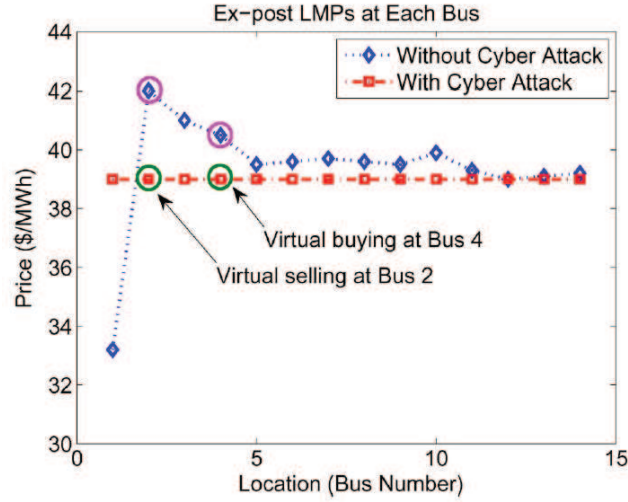


Figure 3.2: LMP with and without cyber attacks (only one line congestion).

In Case I, only one transmission line (from bus 1 to bus 2) is congested. The attacker chooses to buy same amount of virtual power at bus 4 (lower price) and sells virtual power at bus 2 (higher price) in day-ahead market. By compromising two line flow measurement sensors with false data injection, the transmission line congestion appears to be relieved in real-time EMS. This manipulated system state is then passed to real-time market clearing procedure, which computes a uniform

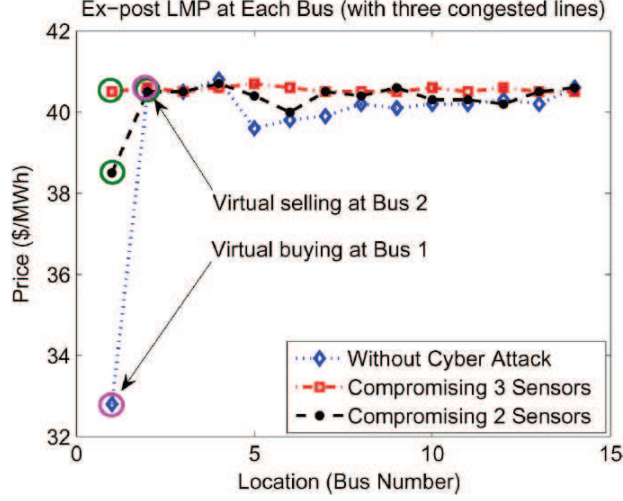


Figure 3.3: LMP with and without cyber attacks (three congested lines).

ex-post LMP across the system. Fig. 3.2 shows the LMPs with and without the cyber attacks. Based on (3.29), the profit of such transaction is about \$2/MWh. In Case II, day-ahead market clearing shows that there are three congested lines, bus 1 and bus 2 have LMP difference of about \$8/MWh. By compromising three line flow sensors indicated in the third column of Table 3.2, the designated pair of nodes (buses 1 and 2) has the same LMP in ex-post real-time market. The reason is that malicious data injection attacks to these three sensors lower the estimated line flow, thereby setting the shadow prices of the actual congested lines to be zero. The profit of such transaction is approximately \$8.2/MWh. In Case III, we assume that an attacker can compromise at most two sensors. By applying the algorithm described in Section V, the attacker chooses to compromise line flow sensors between nodes 1-2, and nodes 2-3. Compromising only these two sensors cannot make all the congested lines appear uncongested in real-time operations. However, as shown in Fig. 3.3, compromising just two sensors can still generate \$6.0/MWh of profit for the attacker.

In Table 3.3 we compare the attack efforts and the associated expected financial

Table 3.3: Attack Efforts and Profits ($\epsilon = 1$ MWh)

Case	relative efforts $\left(\frac{\ \mathbf{a}\ _\infty}{\ \mathbf{z}\ _\infty}\right)$	profits (% of transaction cost)
I	1.23%	2.40%
II	1.41%	9.46%
III	1.31%	7.54%

profits for all the three cases. We use the infinity norm of normalized by the infinity norm of as an indicator of the attackers effort. As the system congestion becomes more complex, the potential of financial gain by maliciously placing false data attacks is also higher. One can observe from the comparison between Case II and Case III that if the attacker can only compromise a limited number of sensors, then the expected profits decrease. However, even compromising a very small number of sensors (e.g. two sensors in the Case III) can lead to profits, showing how the economic losses due to even small false data injection attacks can be significant in the long run.

3.5 Temporal Data Attack on Look-ahead Dispatch

In this subsection, we present a new type of potential cyber attacks in more realistic economic dispatch model, i.e., *look-ahead* dispatch. Motivated by the increasing penetration of variable resources such as wind and solar [47], look-ahead dispatch has been implemented by major Independent System Operators (ISOs)/Regional Transmission Organizations (RTOs) in the past few years in order to improve the market dispatch efficiency [45], [48], [49]. Look-ahead dispatch is different from conventional static dispatch in that it calculates the optimal dispatch in an extended period of time, taking into account inter-temporal ramp rates of generators

of different technologies. In this subsection, an attack strategy is demonstrated, in which the attacker could withhold generation capacity for financial gain by stealthily manipulating the ramp constraint limits of generators in look ahead dispatch. It should be noted that the proposed attack strategy is different from the capacity withholding methods used for a generation company to report capacity noticeably lower than its maximum capacity based on learning algorithm (e.g., SA-Q-Learning algorithm) [50], [51].

3.5.1 Problem Formulation

The i th unit's initial generation power $P_{g_i}[0]$ embedded in (3.19) is replaced, at every dispatch interval, by its corresponding estimate $\hat{P}_{g_i}(\mathbf{z})$, which is processed and delivered by the state estimator. Therefore, in static dispatch the generation power of unit i at $k = 1$ becomes bounded by

$$P_{g_i}^{\max}[1] = \min\{P_{g_i}^{\max}, P_{g_{i,R}}^{\max}(\mathbf{z})\} \quad (3.51)$$

$$P_{g_i}^{\min}[1] = \max\{P_{g_i}^{\min}, P_{g_{i,R}}^{\min}(\mathbf{z})\}, \quad (3.52)$$

where the maximum and minimum limits of the ramp constraints, $P_{g_{i,R}}^{\max}(\mathbf{z})$ and $P_{g_{i,R}}^{\min}(\mathbf{z})$, are

$$P_{g_{i,R}}^{\max}(\mathbf{z}) = \hat{P}_{g_i}(\mathbf{z}) + R_i\Delta T, \quad P_{g_{i,R}}^{\min}(\mathbf{z}) = \hat{P}_{g_i}(\mathbf{z}) - R_i\Delta T. \quad (3.53)$$

If the attacker manipulates the estimate $\hat{P}_{g_i}(\mathbf{z})$ by injecting false data into \mathbf{z} so that the capacity limits of unit i at $k = 1$ are binding to stealthily changed ramp constraint limits, the optimal generation dispatch and nodal price might be miscalculated by RTOs. In this paper we define this type of attack as a ramp-induced data (RID) attack in a potential class of malicious inter-temporal data attacks.

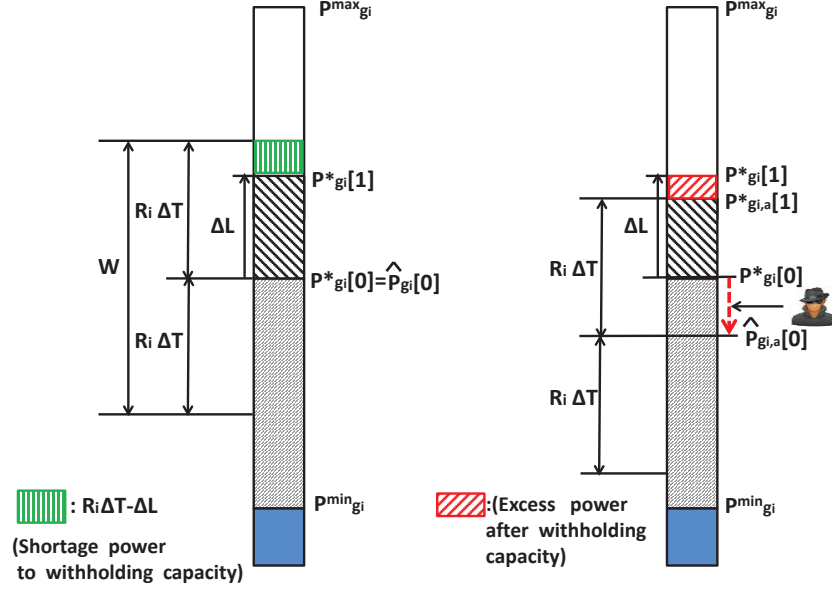


Figure 3.4: Conceptual diagrams illustrating a ramp-induced data attack.

Figure 3.4 illustrates the RID attack, which withholds capacity of a marginal unit (a part-loaded generator). Left and right diagrams describe the generation characteristics of the marginal unit without and with the attack, respectively. W is the feasible range of generation limited by the ramp rate of the marginal unit, and ΔL is an incremental (in this figure) or decremental system load from $k = 0$ to $k = 1$. We note that as $\hat{P}_{gi}[0]$ (for simplicity, we omit \mathbf{z} , instead emphasize the time) is manipulated by the attacker, ΔL can deviate, upwards or downwards, from the range of W , leading to capacity withholding or capacity withdrawing, respectively. The right diagram in Figure 3.4 shows that if $\hat{P}_{gi}[0]$ is decreased to $\hat{P}_{gi,a}[0]$ by the attacker at $k = 0$ so that ΔL deviates upwards from the range of W , the attacker succeeds in withholding capacity, resulting in a new dispatch output $\hat{P}^*_{gi,a}[1]$ at $k = 1$. As a result, the infra-marginal unit (the unit with the next higher marginal cost) is dispatched to supply the excess demand, consequently leading to a uniformly higher market price.

Remark 2. Define $\hat{P}_{g_i, \mathbf{a}}[0] - P_{g_i}^*[0]$ as the contribution of the attacker to changing the nodal price. The RID attack fails (i.e., the nodal price remains unchanged) if the value of this contribution belongs to the following interval:

$$\Delta L - R_i \Delta T \leq \hat{P}_{g_i, \mathbf{a}}[0] - P_{g_i}^*[0] \leq \Delta L + R_i \Delta T. \quad (3.54)$$

The feasible region of $\hat{P}_{g_i}[0]$ based on constraint (3.54) is defined as the price-invulnerable region.

3.5.2 Attack Strategy

In this subsection we formulate a ramp-induced data attack strategy. The power system is assumed to have sufficient transmission capacity. As the first step toward understanding the impact of cyber attack on *temporal* ramp-constrained economic dispatch, we exclude the impact of *spatial* transmission congestion on the market clearing prices. In practice, temporal ramp constraints are coexisting with spatial transmission flow constraints. Therefore, for a successful RID attack in congested networks the attacker should know the targeted power system very well and as much as the system operator knows, however this scenario is unrealistic. Developing a feasible RID attack strategy in congested networks is beyond the scope of this paper and referred to as a future work.

- *Marginal unit attack*: a injection measurement sensor associated with the marginal unit is compromised.
- *Binding unit attack*: injection measurement sensors associated with the binding units are compromised.

- *Coordinated attack*: injection measurement sensors associated with the binding units as well as the marginal unit are compromised.

Here a binding unit represents two types of units: an intra-marginal unit with the lower marginal cost or an infra-marginal unit with the higher marginal cost than a marginal unit. The following proposed attack strategy and simulation results focus on intra-marginal unit attack belonging to binding unit attack.

Remark 3. *When there is no network transmission congestion, it is well acknowledged that static dispatch involves a single marginal unit and multiple binding units that produce their minimum or maximum outputs. On the other hand, look-ahead dispatch may involve multiple marginal units even if there is no congestion in the transmission network. In this paper the marginal unit attack is associated with the marginal unit in static dispatch.*

For achieving undetectability and profitability, the attacker computes the attack vector \mathbf{a} by compromising sensors $i \in G_M$ or $j \in \underline{G}_M^c$, which is the solution of the following optimization problem:

$$\max_{\mathbf{a} \in \text{span}(\mathcal{A})} \delta \quad (3.55)$$

s.t.

$$\|(\mathbf{I} - \mathbf{HB})\mathbf{a}\|_2 \leq \epsilon \quad (3.56)$$

$$\alpha \mathcal{C}_M(\mathbf{a}) + \beta \mathcal{C}_B(\mathbf{a}) \leq \Delta L - R_i \Delta T - \delta \quad (3.57)$$

$$\delta > 0 \quad (3.58)$$

where

$$\mathcal{C}_M(\mathbf{a}) = \mathbf{B}_i \mathbf{a}, \quad \mathcal{C}_B(\mathbf{a}) = \sum_{j \in \underline{G}_M^c} [\mathbf{B}_j \mathbf{a} + R_j \Delta T].$$

$\mathcal{C}_M(\mathbf{a})$ and $\mathcal{C}_B(\mathbf{a})$ are the contributions of the attacker to changing the nodal price, corresponding to the marginal unit and binding unit attacks, respectively. The derivations of these contribution terms are referred to in Section 3.7. The set \mathcal{A} represents the attack vector space, which describes the attack pattern related to the type and number of compromised sensors. $\Delta L - R_i \Delta T$ is the minimum amount of power which the attacker should reduce at $k = 0$ in order to withhold the capacity of unit i at $k = 1$. Constraint (3.56) assures undetectability as the parameter ϵ is tuned with an appropriate value. Constraint (3.57) assures profitability since it enables unit i to bind at the limit of the up-ramp constraint, leading to the increasing nodal price. Therefore, the attacker aims to maximize the margin δ in order to make a financial gain via capacity withholding with a high probability. The binary values of α and β in (3.57) determine the following three types of attacks:

1. $\alpha = 1, \beta = 0$: Marginal unit attack
2. $\alpha = 0, \beta = 1$: Binding unit attack
3. $\alpha = 1, \beta = 1$: Coordinated attack.

Remark 4. *Compared to the capacity withholding mentioned above, capacity withdrawing can benefit a load serving entity (LSE) by manipulating the down-ramp constraint limit. This type of the attack is feasible when constraint (3.57) is replaced with*

$$\alpha \mathcal{C}_M(\mathbf{a}) + \beta \mathcal{C}_B(\mathbf{a}) \geq \Delta L + R_i \Delta T + \delta \quad (3.59)$$

where

$$\mathcal{C}_M(\mathbf{a}) = \mathbf{B}_i \mathbf{a}, \quad \mathcal{C}_B(\mathbf{a}) = \sum_{j \in \overline{G}_M^c} [\mathbf{B}_j \mathbf{a} - R_j \Delta T].$$

3.5.3 Attack Performance Metrics

The performance of the proposed RID attack is evaluated using the following three performance metrics.

- **Attack Profitability:** Assuming that the power injection measurement sensor at generator i is compromised, we define the attack profit efficiency (PE) of generator i as the ratio of the profit with attack to without attack:

$$\text{PE}(i) = \frac{P_{g_i, \mathbf{a}}^*[1](\lambda_i^{(a)} - c_i)}{P_{g_i}^*[1](\lambda_i^{(b)} - c_i)} \times 100 \text{ (\%)}. \quad (3.60)$$

Here, $(\lambda_i^{(a)}, P_{g_i, \mathbf{a}}^*[1])$ and $(\lambda_i^{(b)}, P_{g_i}^*[1])$ are two pairs of the nodal price and optimal generation dispatch with and without attack, respectively. c_i is the marginal cost for generator i .

- **Attack Undetectability:** The system operator normally performs the Chi-squares test [52] for detecting bad data in the measurements. Bad (or malicious) data will bypass if

$$J(\hat{\mathbf{x}}) \leq \chi_{(m-s), p}^2 := \eta_\chi, \quad (3.61)$$

where p is the detection confidence probability, and m and s represent the number of measurements and state variables, respectively.

- **Attack Vulnerability:** Since the measurement noise follows a Gaussian distribution, the manipulated estimate of the state at generator i is also a Gaussian random variable

$$\hat{\mathbf{x}}_i(\mathbf{z}_a) \sim \mathcal{N}(\mathbf{P}_i^*[\mathbf{0}] + \mathbf{B}_i \mathbf{a}, \mathbf{B}_i \mathbf{R} \mathbf{B}_i^T). \quad (3.62)$$

The probability of the distorted estimate $\hat{\mathbf{x}}_i(\mathbf{z}_a)$ being within the price-invulnerable region defined in Remark 2 is expressed as in terms of $Q(\cdot)$ functions

$$\mathbb{P}_i(\mathbf{a}) = \mathbb{P}(\mathbf{l}(i) \leq \hat{\mathbf{x}}_i(\mathbf{z}_a) \leq \mathbf{u}(i)) \quad (3.63)$$

$$= Q(\mathbf{l}(i)) - Q(\mathbf{u}(i)), \quad (3.64)$$

where the complementary Gaussian cumulative distribution function $Q(x)$ is defined as

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\xi^2}{2}\right) d\xi \quad (3.65)$$

and

$$\mathbf{l}(i) = \frac{\Delta L - R_i \Delta T - \mathbf{B}_i \mathbf{a}}{\sqrt{\mathbf{B}_i \mathbf{R} \mathbf{B}_i^T}} \quad (3.66)$$

$$\mathbf{u}(i) = \frac{\Delta L + R_i \Delta T - \mathbf{B}_i \mathbf{a}}{\sqrt{\mathbf{B}_i \mathbf{R} \mathbf{B}_i^T}}. \quad (3.67)$$

We define $\mathbb{P}_i(\mathbf{a})$ as the price-invulnerable probability (PIP) with respect to generator i . From (3.63), (3.65), (3.66) and (3.67), we specify the relationship among the ramp rate $R_i \Delta T$, the diagonal measurement covariance matrix \mathbf{R} , and the PIP as follows:

1. The increase of the $R_i \Delta T$ leads to the increase of the PIP.
2. The decrease of the values of the diagonal elements in \mathbf{R} leads to the increase of the PIP.

In other words, the deployment of more accurate sensors and generators with a faster ramp rate enables the power system to become more robust to the RID attack.

3.5.4 Simulation Studies

In this subsection the economic impact of the proposed RID attack on the real-time electricity market operation is illustrated in the IEEE 14-bus system as shown in Figure 3.5. Measurement configuration includes nodal power injection measurements at all generation and load buses, and power flow measurements at one end of each transmission line. This system has a total of 34 measurements including 14 power injection and 20 power flow measurements, which assure the system observability. Table 3.4 shows the five generators' operating characteristics, including unit type (generation bus number), physical capacity limit, ramp rate and marginal cost (MC).

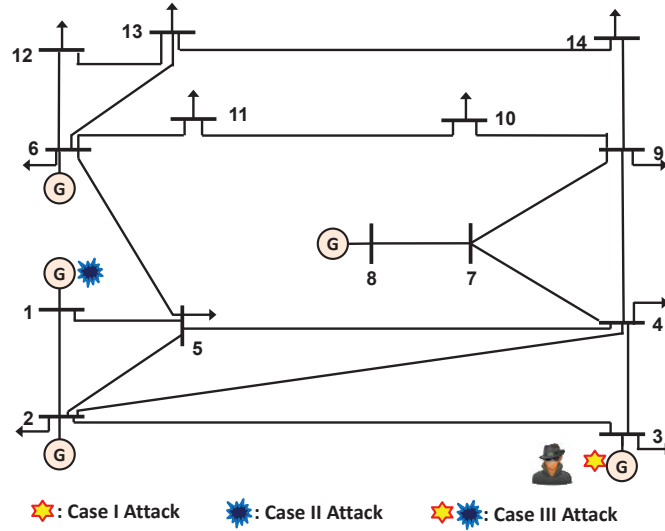


Figure 3.5: IEEE 14-bus Test system.

In this section, three cases are simulated in the IEEE-14 bus system:

- Case I: Marginal unit attack.
- Case II: Binding unit attack.

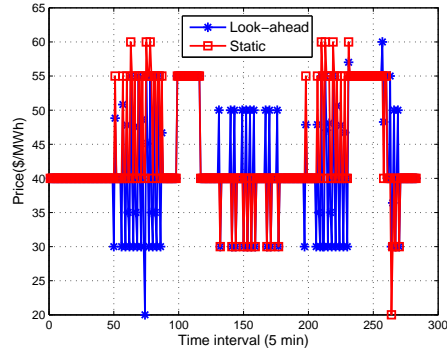
Table 3.4: Generator Parameters of the IEEE 14-bus Test System.

Unit Type	P_{\min}	P_{\max}	Ramp Rate	MC
Coal(1)	0MW	200MW	10MW/5min	30\$/MWh
Wind(2)	0MW	300MW	150MW/5min	20\$/MWh
Nuclear(3)	0MW	300MW	8MW/5min	40\$/MWh
Coal(6)	50MW	250MW	15 MW/5min	55\$/MWh
Oil(8)	60MW	150MW	60 MW/5min	60\$/MWh

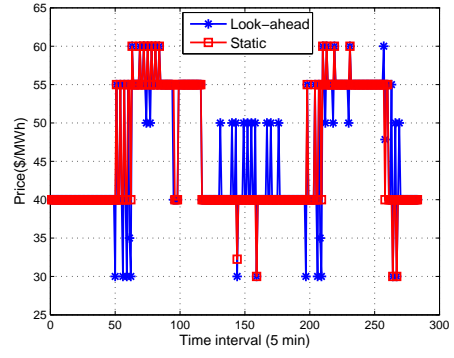
- Case III: Coordinated attack.

The performance of the proposed RID attack is evaluated based on the one day load profile with a 5-min resolution. This load profile is obtained by interpolating a 15-min daily data in the ERCOT website. The load is scaled down to be consistent with the IEEE 14-bus test system’s peak load data. The common goal of all three cases is to withhold the capacity of generator 3 for the purpose of making a profit. A power injection sensor at generation bus 3 is compromised in Case I whereas a power injection sensor at generation 1 is compromised in Case II. Case III represents the coordinated attack, which compromises both sensors targeted in Case I and Case II.

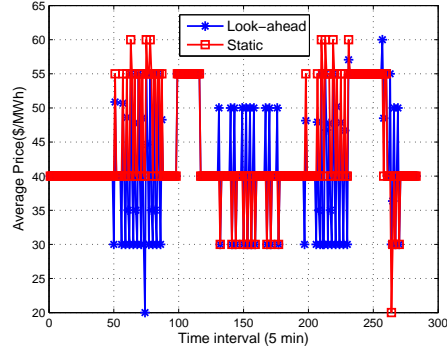
Figures 3.6 show the comparison of the LMPs between static ($K = 1$) and look-ahead dispatch ($K = 6$) without attack and with attack in Cases I, II and III. Due to no network transmission congestion, the prices in these figures denote the uniform LMPs for all the buses at every dispatch interval. In Figure 3.6(a), the LMPs in look-ahead dispatch are oscillating around 40\$/MWh more than the ones in static dispatch. This phenomenon is due to the fact that the binding of generator 3 at the up- or down-ramp constraints at time $k + 1$ makes its corresponding Lagrangian multiplier, $\omega_{3,\max}[k + 1]$ or $\omega_{3,\min}[k + 1]$, become positive. As shown



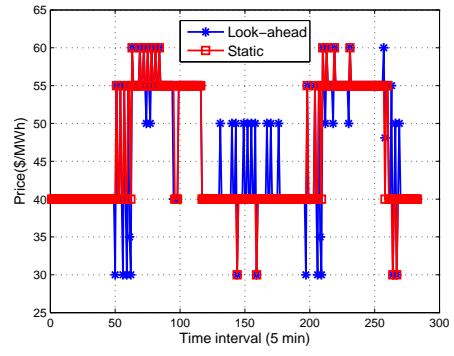
(a) Without attack



(b) Case I attack



(c) Case II attack



(d) Case III attack

Figure 3.6: LMP of static and look-ahead dispatch without attack and with Case I,II and III attacks.

in equation (3.23), this leads to different LMPs at time k than the ones from static dispatch. We observe from Figures 3.6(b),(c),(d) that the LMPs in both dispatch models tend to increase with attack. This observation implies that the attacker successfully withholds the capacity of generator 3 by lowering its up-ramp constraint limit through the reduction of the initial estimate $\hat{P}_{g3,a}[0]$. Consequently, this leads to the shift of the marginal unit to another one with a more expensive marginal cost.

Table 3.5: Attack Performance in Static and Look-ahead Dispatch.

Case	Static (PE(3))	Look-ahead (PE(3))	$J(\eta_x = 37.6)$
I	131.9	148.9	28.2
II	101.2	102.6	35.5
III	108.9	113.8	31.5

Table 3.5 shows the attack performance of Cases I, II and III in both static and look-ahead dispatch. The second and third columns of this table indicate the attack profit efficiency at generation bus 3. We can observe from the comparison of these two columns several facts. First, the PE values in all three cases of both dispatch models are larger than 100. It indicates that the attacker makes an additional profit using the proposed attack strategy. Second, for all three cases, the PE in look-ahead dispatch is higher than in static dispatch. This observation might result from the fact that the attack leads to more increase of the nodal price in look-ahead dispatch than in static dispatch. Lastly, among three cases, Case I and Case II attacks yield the largest and smallest PE, respectively. The PE in Case III is between Case I and Case II. This result is natural since Case II and Case III attacks require an extra effort for withholding the binding unit's capacity as well as the marginal unit's capacity so that both attacks fail with a higher probability than Case I attack. Figure 3.7 shows the amount of generator 3's capacity which all three attacks withhold between 80 and 90 time intervals. As expected, it is

verified that Case I, Case III, and Case II attacks withhold capacity the most in a descending order. This fact also justifies the third observation mentioned above. The values of the estimated objective functions for all three cases are shown in the last column of Table 3.5. Based on the measurement configuration with $m=34$ and $s=14$, the threshold (η_χ) of the Chi-squares test with a 99% confidence level is set to 37.6. For undetectability, the parameter ϵ in (3.56) is set to 3. Therefore, all three attacks in both dispatch models succeed in avoiding the Chi-squares bad data detection.

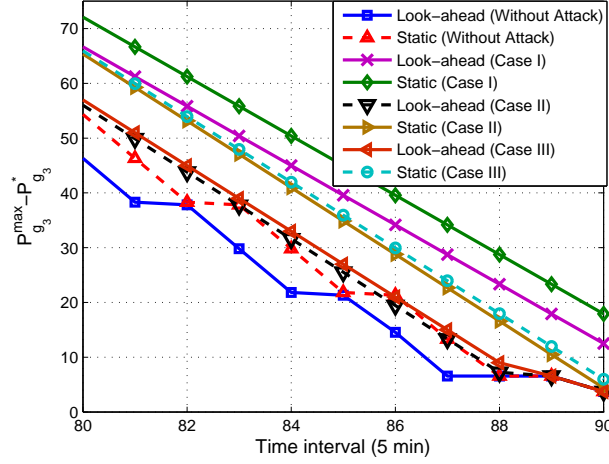


Figure 3.7: $P_{g_3}^{max} - P_{g_3}^*$ of static and look-ahead dispatch without attack and with Case I,II and III attacks.

Table 3.6: Attack Performance with Varying Attack Magnitude in Case I.

Attack Relative Magnitude (ARM %)	0.25	0.5	0.75	1
Static (PE(3))	111.8	120.8	126.4	126.9
Look-ahead (PE(3))	112.2	125.8	127.6	137.7
J	21.1	25.4	29.2	33.1
PIP	0.433	0.344	0.259	0.188

Table 3.6 shows the sensitivity of Case I attack performance with respect to the attack magnitude. In this table, the attack relative magnitude (ARM) is defined as $\frac{\|\mathbf{a}\|_\infty}{\|\mathbf{z}\|_\infty} \times 100$ where $\|\cdot\|_\infty$ denotes an infinity norm. We observe from this table that

the increase of the ARM leads to more profit (the third and fourth rows) in both dispatch models. However, the estimated objective function J (the fifth row) used for the Chi-squares bad data test increases and the PIP (the last row) decreases. This implies that as the ARM increases the attack becomes more vulnerable to the bad data detection and fails with an increasing probability. Tables 3.7 and 3.8 show Case I attack performance with the varying ramp rate of generator 3 and measurement variance of sensors. We first observe from Table 3.7 that as the ramp rate of generator 3 increases the PE in both dispatch models decreases. Another observation from Table 3.8 is that the decrease of measurement variance leads to the decrease of the attack profit. These observations imply that the nodal prices become less manipulable, which is verified with the increasing PIP in Tables 3.7 and 3.8.

Table 3.7: Impact of Ramp Rate on the Attack Performance in Case I.

Ramp Rate (MW/5min)	8	10	12	14
Static (PE(3))	131.9	119.7	106.4	100.5
Look-ahead (PE(3))	148.9	123.5	108.5	103.1
PIP	0.017	0.021	0.037	0.044

Table 3.8: Impact of Measurement Variance on the Attack Performance in Case I.

Measurement Variance (σ^2)	0.0005	0.005	0.05	0.5
Static (PE(3))	123.2	129.1	130.3	136.9
Look-ahead (PE(3))	143.5	144.8	146.1	152.8
PIP	0.056	0.041	0.034	0.021

3.6 Conclusions

In this chapter we examine the possible economic impact of two types of undetectable cyber data attacks against state estimation on real-time electric power market operations: (1) spatial data attack on static dispatch; and (2) temporal data attack on look-ahead dispatch.

In spatial attack, we show how an attacker can manipulate the nodal price of ex-post real-time market without being detected by the state estimators. In conjunction with virtual bidding, these integrity attacks can lead to consistent financial profit for the attacker. A heuristic is developed to compute the optimal injection of false data from the attackers perspective. False data injection attacks with a limited number of sensors are formulated as a convex optimization problem and thus solved efficiently by the attacker. Illustrative examples in IEEE 14-bus system show that the potential economic gain for the attackers are significant even with small number of sensors being compromised by the attackers.

In temporal attack, we propose a novel attack strategy with which the attacker can manipulate, in look-ahead dispatch, the limits of ramp constraints of generators. It is demonstrated that the proposed attack may lead to financial profits via malicious capacity withholding of selected generators, while being undetected by the existing bad data detection algorithm embedded in the state estimator. Numerical examples simulated in the IEEE 14-bus system demonstrate the undetectability and profitability of the proposed cyber data attack.

In future work, a system-theoretical framework to analyze the effect of various

types of spatial and temporal data attacks on real-time electricity market operations will be developed. The key challenge lies in how to analytically quantify the impact of manipulated sensors measurement on the nodal price in space-time coupled optimization problem. Another important future direction is to design the robust real-time pricing model as countermeasures to mitigate the financial risks of a variety of cyber data attacks.

3.7 Appendix

In this appendix, we derive the two types of the attack contribution terms in the second inequality constraint of the attack formulation described in Section 3.5.2. We define the contributions of the marginal unit and binding unit attacks in the expected sense as

$$\mathcal{C}_M(\mathbf{a}) = E[d_i^M(\mathbf{a})] \quad (3.68)$$

$$\mathcal{C}_B(\mathbf{a}) = E[d^B(\mathbf{a})] \quad (3.69)$$

where

$$d_i^{(M)}(\mathbf{a}) = \hat{P}_{g_i, \mathbf{a}}[0] - P_{g_i}^*[0] \quad (3.70)$$

$$d^{(B)}(\mathbf{a}) = \sum_{j \in \underline{G}_M^c} (\hat{P}_{g_j, \mathbf{a}}[0] + R_j \Delta T - P_{g_j}^{\max}[0]) \quad (3.71)$$

Here, $\hat{P}_{g_i, \mathbf{a}}[0]$ is the manipulated estimate of generation power at generation bus i .

Then,

$$\mathcal{C}_M(\mathbf{a}) = E[d_i^{(M)}(\mathbf{a})] = E[\hat{P}_{g_i, \mathbf{a}}[0]] - P_{g_i}^*[0] \quad (3.72)$$

$$\stackrel{(a)}{=} E[\mathbf{B}_i(\mathbf{H}\mathbf{x} + \mathbf{e} + \mathbf{a})] - P_{g_i}^*[0] \stackrel{(b)}{=} \mathbf{B}_i \mathbf{a} \quad (3.73)$$

where \mathbf{B}_i is the row vector of matrix \mathbf{B} , which corresponds to the injection measurement sensor of generator i . (a) follows from $\hat{P}_{g_i, \mathbf{a}}[0] = \mathbf{B}_i \mathbf{z}$. (b) follows from $\mathbf{B}_i \mathbf{H} = [0 \dots 0 \ 1 \ 0 \dots 0]$ where 1 is the i th element of vector $\mathbf{B}_i \mathbf{H}$ and $E[\mathbf{x}_i] \approx P_{g_i}^*[0]$ together with $E[\mathbf{e}] = 0$. Similarly,

$$\mathcal{C}_B(\mathbf{a}) = E[d^{(B)}(\mathbf{a})] = \sum_{j \in \underline{\mathcal{G}}_M^c} [E[\hat{P}_{g_j, \mathbf{a}}[0]] + R_j \Delta T - P_{g_j}^{\max}[0]] \quad (3.74)$$

$$= \sum_{j \in \underline{\mathcal{G}}_M^c} [\mathbf{B}_j \mathbf{a} + P_{g_j}^*[0] + R_j \Delta T - P_{g_j}^{\max}[0]] \quad (3.75)$$

$$\stackrel{(c)}{=} \sum_{j \in \underline{\mathcal{G}}_M^c} [\mathbf{B}_j \mathbf{a} + R_j \Delta T] \quad (3.76)$$

where (c) follows from $P_{g_j}^*[0] = P_{g_j}^{\max}[0]$.

CHAPTER 4

LMP SENSITIVITY ANALYSIS TO DATA
CORRUPTION-INDUCED ESTIMATION ERROR

4.1 Introduction

State estimation is one of the key applications for power system energy management systems (EMSs). The impact of bad data on power systems has been intensively investigated in recent decades in power system state estimation literature. Measurement noise and/or manipulated sensor errors in a supervisory control and data acquisition (SCADA) system may mislead system operators about real-time conditions in a power system, which in turn may impact the price signals in real-time power markets. This chapter attempts to provide a novel analytical framework with which to investigate the impact of bad sensor data on electric power market operations. In future power system operations, which will probably involve many more sensors, the impact of sensor data quality on grid operations will become increasingly important.

In this chapter, we investigate the sensitivity of real-time LMP with respect to *continuous* (e.g., the power injection/flow and voltage magnitude) and *discrete* (e.g., the on/off status of a circuit breaker) data corruption due to state estimation error. Fig. 4.1 illustrates how the corrupted SCADA sensor data impact the state estimation as well as the security constrained economic dispatch in energy management systems (EMSs) and market management systems (MMSs). The two lines (a) and (b) in Fig. 4.1 represent the flow of manipulated network topology and

power flow estimates, corresponding to the corruption of discrete and continuous data, respectively. The impacts of (b) and (a) on LMP are analyzed in Section 4.3 and Section 4.4, respectively.

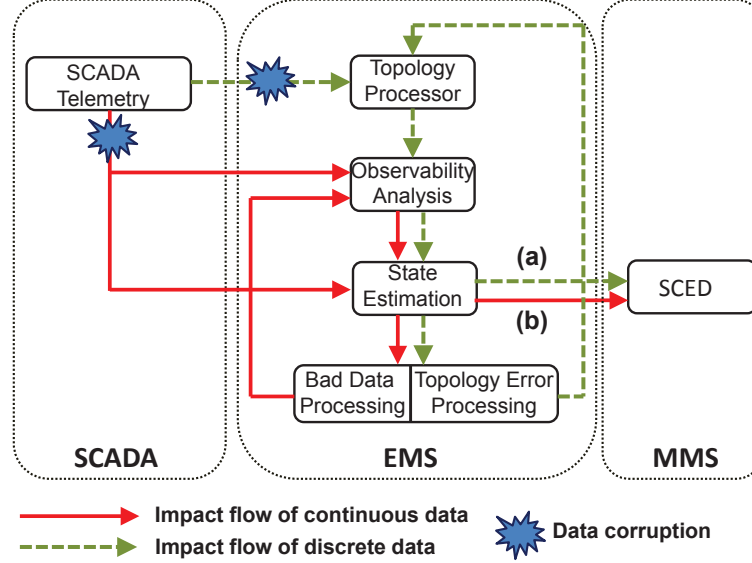


Figure 4.1: Illustrating the impact of corrupted continuous and discrete SCADA sensor data on state estimation and SCED.

4.1.1 Literature Review

Real-time market LMPs are primarily affected by a system's physical conditions, which are the results of state estimation routine. A study of LMP sensitivity with respect to system physical conditions was first conducted by Conejo et al. [53]. In this work, the LMP sensitivity problem was formulated in nonlinear programming based on the AC optimal power flow (ACOPF) model. It provided a generalized platform for calculating the sensitivity of LMP with respect to changes in various parameters such as load, generator cost, voltage limit, generation power limit, and network topology. Sensitivity studies have also been conducted with

linear programming based on the DC optimal power flow (DCOPF) model with a DCOPF-based algorithm [43], the probabilistic model [54], and the continuous locational marginal pricing approach [55]. All previous work has focused mainly on the impact of physical load variations on LMP sensitivity. More recently, some work has proposed cyber data attacks which stealthily change power flow estimate and network topology estimate through the corruption of continuous [40] and discrete data [56], [57], and quantify the economic impact of such attacks on real-time power market operations. However, no analytic study for quantifying the impact of such estimation errors on LMP sensitivity has been done yet.

4.1.2 Report Organization

The remainder of this chapter is organized as follows. We briefly review AC state estimation and two representative real-time pricing models in Section 4.2. In Section 4.3, we formulate the problem, derive the quantifying sensitivity of LMP subject to corrupted continuous data and provide numerical examples that illustrate the impact of different SCADA sensors on LMP in IEEE 14-bus and 118-bus systems with both the Ex-ante and Ex-post pricing models. In Section 4.4, a LMP sensitivity index with respect to topology error due to discrete data corruption is derived and the derived sensitivity index is verified and illustrated in the IEEE 14-bus system. We make concluding remarks and suggest future work in Section 4.5.

4.2 Preliminaries

The notations used in this section are summarized in Table 4.1.

Table 4.1: Notations.

a_i	Linear cost coefficient for generator i
b_i	Quadratic cost coefficient for generator i
$C_i(\cdot)$	Energy cost for generator i
P_{g_i}	Scheduled generator power output for generator i
L_{d_i}	Fixed demand at bus i
$P_{g_i}^{\min}, P_{g_i}^{\max}$	Min/max generation limits for generator i at Ex-ante dispatch
F_l^{\min}, F_l^{\max}	Min/max flow limits for transmission line l at Ex-ante dispatch
S_{li}	Generation shift factor of transmission line l to bus i
$\Delta P_{g_i}^{\max}, \Delta P_{g_i}^{\min}$	Min/max incremental generation limits for generator i at Ex-post dispatch
R_i	Ramp rate of generator i
ΔT	Dispatch interval
π_i	Locational marginal price at bus i
λ	Shadow price of the system energy balance equation
τ_i	Shadow price of the capacity constraint for generator i
μ_l	Shadow price of the transmission line constraint for transmission line l
N_b	Total number of buses
N_m	Total number of sensor measurements
N_l	Total number of transmission lines
$\mathcal{CL}_+, \mathcal{CL}_-$	Sets of positively and negatively congested lines at Ex-ante dispatch
\mathcal{S}_v	Set of voltage magnitude measurements
\mathcal{S}_{ri}	Set of real power injection measurements
\mathcal{S}_{ai}	Set of reactive power injection measurements
\mathcal{S}_{rf}	Set of real power flow measurements
\mathcal{S}_{af}	Set of reactive power flow measurements
\mathbf{I}_k	$k \times k$ identity matrix
$\mathbf{1}_k, \mathbf{0}_k$	$k \times 1$ column vectors with all ones and all zeros, respectively

4.2.1 AC State Estimation Model

The measurement model for AC state estimation is formulated as

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}. \quad (4.1)$$

Here $\mathbf{z} = [\mathbf{z}_r^T \ \mathbf{z}_a^T \ \mathbf{z}_v^T]^T$ is the $N_m \times 1$ measurement vector that consists of real power injection and the flow vector $\mathbf{z}_r = [\mathbf{z}_{ri}^T \ \mathbf{z}_{rf}^T]^T$, the reactive power injection and flow vector $\mathbf{z}_a = [\mathbf{z}_{ai}^T \ \mathbf{z}_{af}^T]^T$, and the bus voltage magnitude vector \mathbf{z}_v . $\mathbf{x} = [\boldsymbol{\theta}^T \ \mathbf{V}^T]^T$ is the state vector that consists of the $(N_b - 1) \times 1$ bus voltage phase angle vector $\boldsymbol{\theta}$ excluding a slack bus and the $N_b \times 1$ voltage magnitude vector \mathbf{V} . $\mathbf{h}(\mathbf{x})$ is the $N_m \times 1$ nonlinear vector valued measurement function relating measurements to states, and \mathbf{e} is the $N_m \times 1$ independent identically distributed (i.i.d.) Gaussian measurement error vector with zero mean and diagonal covariance matrix \mathbf{R} . The state estimator computes the optimal estimate of \mathbf{x} by minimizing the weighted least squares of measurement error:

$$\text{minimize} \quad J(\mathbf{x}) = \mathbf{r}^T \mathbf{R}^{-1} \mathbf{r} \quad (4.2)$$

$$\text{s.t.} \quad \mathbf{r} = \mathbf{z} - \mathbf{h}(\mathbf{x}). \quad (4.3)$$

Using the Gauss-Newton method, the weighted least squares estimate vector $\hat{\mathbf{x}}$ is computed by the following iterative procedure [52]:

$$\Delta \hat{\mathbf{x}}^{k+1} = [\mathbf{G}(\hat{\mathbf{x}}^k)]^{-1} \mathbf{H}^T(\hat{\mathbf{x}}^k) \mathbf{R}^{-1} \Delta \mathbf{z}^k \quad (4.4)$$

where $\mathbf{H}(\hat{\mathbf{x}}^k) = \left[\frac{\partial \mathbf{h}(\hat{\mathbf{x}}^k)}{\partial \hat{\mathbf{x}}^k} \right]$ is the $N_m \times (2N_b - 1)$ Jacobian matrix at k -th iteration, and

$$\Delta \hat{\mathbf{x}}^{k+1} = \hat{\mathbf{x}}^{k+1} - \hat{\mathbf{x}}^k \quad (4.5)$$

$$\Delta \mathbf{z}^k = \mathbf{z} - \mathbf{h}(\hat{\mathbf{x}}^k) \quad (4.6)$$

$$\mathbf{G}(\hat{\mathbf{x}}^k) = \mathbf{H}^T(\hat{\mathbf{x}}^k) \mathbf{R}^{-1} \mathbf{H}(\hat{\mathbf{x}}^k). \quad (4.7)$$

The iteration process in (4.4) continues until the maximum of $|\Delta \hat{\mathbf{x}}^k|$ is less than a predetermined threshold, otherwise stops and yields the ultimate estimates.

4.2.2 Real-time Electricity Pricing Model

Locational marginal price (LMP) is the core variable in market operations [58]. In real-time power markets, LMP is obtained as the by-product of security constrained economic dispatch (SCED) in either of the two main pricing models: Ex-ante (e.g. in ERCOT, NY ISO) and Ex-post (e.g. in ISO New England, PJM, and Midwest ISO) [42]. Both pricing models are built on the power flow and network topology results given by the state estimator, which uses two types of sensor data: 1) continuous (e.g., the power injection/flow and voltage magnitude); and 2) discrete (e.g., the on/off status of a circuit breaker).

The Ex-ante Model: In ex-ante real-time market models, LMPs are computed before the actual deployment of dispatch orders. For the system operator, the Ex-ante dispatch is formulated as follows [43]:

$$\min_{P_{g_i}} \sum_{i=1}^{N_b} C_i(P_{g_i}) \quad (4.8)$$

s.t.

$$\lambda : \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} L_{d_i} \quad (4.9)$$

$$\boldsymbol{\tau} : \hat{P}_{g_i}^{\min} \leq P_{g_i} \leq \hat{P}_{g_i}^{\max} \quad \forall i = 1, \dots, N_b \quad (4.10)$$

$$\boldsymbol{\mu} : F_l^{\min} \leq \sum_{i=1}^{N_b} S_{li}(P_{g_i} - L_{d_i}) \leq F_l^{\max} \quad \forall l = 1, \dots, N_l \quad (4.11)$$

where

$$\begin{aligned}\hat{P}_{g_i}^{\max} &= \min\{P_{g_i}^{\max}, \hat{P}_{g_i}(\mathbf{z}) + R_i\Delta T\} \\ \hat{P}_{g_i}^{\min} &= \max\{P_{g_i}^{\min}, \hat{P}_{g_i}(\mathbf{z}) - R_i\Delta T\}.\end{aligned}$$

In this formulation, the objective function is to minimize the total generation costs in (4.8). (4.9) is the system-wide energy balance equation. (4.10) is the physical capacity constraints of each generator embedded with its ramp constraints. (4.11) is the transmission line constraints.

The Ex-post Model: In ex-post real-time market models, LMPs are computed after the fact using real-time estimates for settlement purposes. Assuming no demand elasticity, the Ex-post dispatch is written as [44]:

$$\min_{P_{g_i}} \sum_{i=1}^{N_b} C_i(P_{g_i}) \quad (4.12)$$

s.t.

$$\lambda : \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} \hat{P}_{g_i}(\mathbf{z}) \quad (4.13)$$

$$\boldsymbol{\tau} : \hat{P}_{g_i}^{\min} \leq P_{g_i} \leq \hat{P}_{g_i}^{\max} \quad \forall i = 1, \dots, N_b \quad (4.14)$$

$$\boldsymbol{\mu}_{\max} : \sum_{i=1}^{N_b} S_{li}(P_{g_i} - L_{d_i}) \leq \hat{F}_l(\mathbf{z}) \quad \forall l \in \mathcal{CL}_+ \quad (4.15)$$

$$\boldsymbol{\mu}_{\min} : \sum_{i=1}^{N_b} S_{li}(P_{g_i} - L_{d_i}) \geq \hat{F}_l(\mathbf{z}) \quad \forall l \in \mathcal{CL}_- \quad (4.16)$$

where

$$\hat{P}_{g_i}^{\max} = \hat{P}_{g_i}(\mathbf{z}) + \Delta P_{g_i}^{\max}, \quad \hat{P}_{g_i}^{\min} = \hat{P}_{g_i}(\mathbf{z}) + \Delta P_{g_i}^{\min}.$$

The above formulation is expressed with different notation than the Ex-post model formulated in [44] in order to emphasize that the state estimation solution has a direct impact on the Ex-post model.

4.3 Impact Analysis of LMP Subject to Power Flow Estimate Errors

In this subsection, we focus on a sensitivity analysis of real-time LMP subject to corrupted *continuous* data fed into the state estimator. Fig. 4.2 illustrates that via state estimation, SCADA measurement \mathbf{z} may impact the results of a pair of Ex-ante nodal price and optimal generation dispatch $\{\pi(\hat{\mathbf{x}}_A(\mathbf{z})), P_g^*(\hat{\mathbf{x}}_A(\mathbf{z}))\}$ and the Ex-post price $\pi(\hat{\mathbf{x}}_P(\mathbf{z}))$.

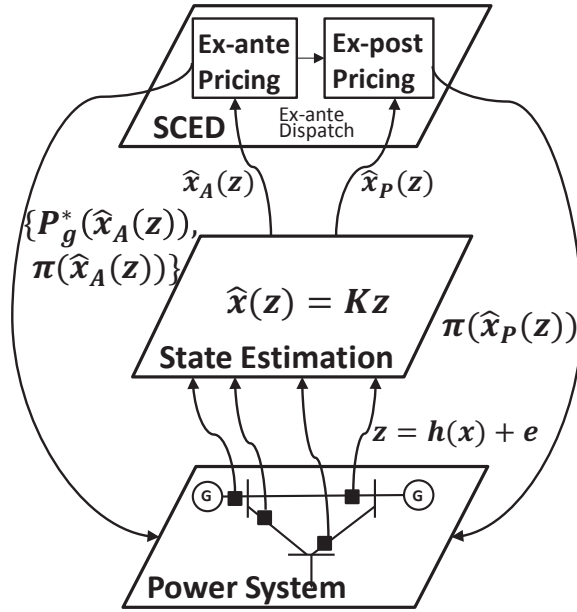


Figure 4.2: A three-layered framework illustrating the coupling of the physical power system, state estimation, and SCED.

4.3.1 Problem Formulation

Referring to Fig. 4.2, for all buses ($i = 1, \dots, N_b$) and measurements ($j = 1, \dots, N_m$), the $N_b \times 1$ vector of LMPs can be expressed in a composite function

form:

$$\mathbf{LMP} = \boldsymbol{\pi}(\hat{\mathbf{x}}(\mathbf{z}))$$

where

$$\boldsymbol{\pi} = [\pi_1, \pi_2, \dots, \pi_{N_b}]^T \quad (4.17)$$

$$\pi_i = f_i(\hat{x}_1, \hat{x}_2, \dots, \hat{x}_{N_m}) \quad (4.18)$$

$$\hat{x}_j = g_j(z_1, z_2, \dots, z_{N_m}). \quad (4.19)$$

π_i represents the LMP at bus i . z_j and \hat{x}_j are the measurement and its corresponding estimate at sensor j , respectively. $f_i(\cdot)$ is the vector function that describes the relationship between any estimate and LMP at bus i . $g_j(\cdot)$ is the vector function that describes the relationship between any measurement and estimate at sensor j .

The primary goal of this paper is to compute LMP sensitivity at any bus i subject to a measurement change at any sensor j throughout the entire transmission network.

$$\frac{\partial \pi_i}{\partial z_j} = \boldsymbol{\Lambda}_{(i,j)}. \quad (4.20)$$

By chain rule, for all i and j , (4.20) is written as

$$\frac{\partial \pi_i}{\partial z_j} = \frac{\partial \pi_i}{\partial \hat{x}_1} \frac{\partial \hat{x}_1}{\partial z_j} + \frac{\partial \pi_i}{\partial \hat{x}_2} \frac{\partial \hat{x}_2}{\partial z_j} + \dots + \frac{\partial \pi_i}{\partial \hat{x}_{N_m}} \frac{\partial \hat{x}_{N_m}}{\partial z_j}. \quad (4.21)$$

In (4.21), the estimate \hat{x}_j is chosen as an intermediate variable for computing the partial derivative of π_i with respect to z_j . This variable is used to set the bounds for: 1) minimum and maximum generation capacity in (4.10), (4.14); 2) the system balance equation in (4.13); and 3) the positive and negative transmission line capacity in (4.15), (4.16). Equation (4.21) can be expressed in matrix form as

shown in (4.22).

$$\begin{aligned}
\mathbf{\Lambda}_{(N_b \times N_m)} &= \frac{\partial \boldsymbol{\pi}}{\partial \mathbf{z}} = \frac{\partial \boldsymbol{\pi}}{\partial \hat{\mathbf{x}}} \frac{\partial \hat{\mathbf{x}}}{\partial \mathbf{z}} \\
&= \underbrace{\begin{bmatrix} \frac{\partial \pi_1}{\partial \hat{x}_1} & \frac{\partial \pi_1}{\partial \hat{x}_2} & \cdots & \frac{\partial \pi_1}{\partial \hat{x}_{N_m}} \\ \frac{\partial \pi_2}{\partial \hat{x}_1} & \frac{\partial \pi_2}{\partial \hat{x}_2} & \cdots & \frac{\partial \pi_2}{\partial \hat{x}_{N_m}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \pi_{N_b}}{\partial \hat{x}_1} & \frac{\partial \pi_{N_b}}{\partial \hat{x}_2} & \cdots & \frac{\partial \pi_{N_b}}{\partial \hat{x}_{N_m}} \end{bmatrix}}_{\mathbf{\Lambda}_A} \underbrace{\begin{bmatrix} \frac{\partial \hat{x}_1}{\partial z_1} & \frac{\partial \hat{x}_1}{\partial z_2} & \cdots & \frac{\partial \hat{x}_1}{\partial z_{N_m}} \\ \frac{\partial \hat{x}_2}{\partial z_1} & \frac{\partial \hat{x}_2}{\partial z_2} & \cdots & \frac{\partial \hat{x}_2}{\partial z_{N_m}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \hat{x}_{N_m}}{\partial z_1} & \frac{\partial \hat{x}_{N_m}}{\partial z_2} & \cdots & \frac{\partial \hat{x}_{N_m}}{\partial z_{N_m}} \end{bmatrix}}_{\mathbf{\Lambda}_B}.
\end{aligned} \tag{4.22}$$

The sensitivity $\mathbf{\Lambda}_{(i,j)}$ in (4.20) is the element at the i th row and j th column of the $N_b \times N_m$ sensitivity matrix $\mathbf{\Lambda}$. The matrix $\mathbf{\Lambda}$ is written as the multiplication form of two matrices with different types of sensitivities: the $N_b \times N_m$ matrix $\mathbf{\Lambda}_A = \frac{\partial \boldsymbol{\pi}}{\partial \hat{\mathbf{x}}}$ quantifies the *economic* impact of any estimate on any LMP, and the $N_m \times N_m$ matrix $\mathbf{\Lambda}_B = \frac{\partial \hat{\mathbf{x}}}{\partial \mathbf{z}}$ quantifies the *cyber* impact of any sensor measurement on any estimate. The derivations of $\mathbf{\Lambda}_A$ and $\mathbf{\Lambda}_B$ are described in more detail in the next section.

4.3.2 Derivation of the Proposed LMP Sensitivity Index

• Sensitivity of LMPs to Estimated States

We first derive the sensitivity matrix $\mathbf{\Lambda}_A$ using the Ex-ante model. To this end, the perturbation approach developed in [53] is applied to the Ex-ante model in

Subsection 4.2.2. The Lagrangian function of the Ex-ante dispatch is written as

$$\begin{aligned}\mathcal{L} = & \sum_{i=1}^{N_b} C_i(P_{g_i}) - \lambda \left(\sum_{i=1}^{N_b} [P_{g_i} - L_{d_i}] \right) + \sum_{j=1}^{2N_b} \tau_j \left(\sum_{i=1}^{N_b} A_{ji} P_{g_i} - \hat{C}_j \right) \\ & + \sum_{l=1}^{2N_l} \mu_l \left(\sum_{i=1}^{N_b} S_{li} [P_{g_i} - L_{d_i}] - D_l \right)\end{aligned}$$

where A_{ji} , S_{li} , \hat{C}_j and D_l are the elements of the following matrices

$$\mathbf{A}_{(2N_b \times N_b)} = \begin{bmatrix} A_{ji} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_{N_b} \\ -\mathbf{I}_{N_b} \end{bmatrix}, \quad \mathbf{B}_{(2N_l \times N_b)} = \begin{bmatrix} S_{li} \end{bmatrix} = \begin{bmatrix} \mathbf{S} \\ -\mathbf{S} \end{bmatrix} \quad (4.23)$$

$$\hat{\mathbf{C}}_{(2N_b \times 1)} = \begin{bmatrix} \hat{C}_j \end{bmatrix} = \begin{bmatrix} \hat{\mathbf{P}}_g^{\max} \\ -\hat{\mathbf{P}}_g^{\min} \end{bmatrix}, \quad \mathbf{D}_{(2N_l \times 1)} = \begin{bmatrix} D_l \end{bmatrix} = \begin{bmatrix} \mathbf{F}^{\max} \\ -\mathbf{F}^{\min} \end{bmatrix} \quad (4.24)$$

Here, \mathbf{S} is the generation shift factor matrix, and

$$\hat{\mathbf{P}}_g^{\max(\min)} = [\hat{P}_{g_1}^{\max(\min)}, \dots, \hat{P}_{g_{N_b}}^{\max(\min)}]^T, \quad \mathbf{F}^{\max(\min)} = [F_1^{\max(\min)}, \dots, F_{N_l}^{\max(\min)}]^T. \quad (4.25)$$

As in [53], unbinding inequality constraints are excluded in our sensitivity analysis. Let us define B_g and B_f as the number of binding constraints associated with generation capacity and line capacity, respectively. Then, the KKT conditions of the Ex-ante problem are written as

$$\begin{aligned} \text{(i)} \quad & \frac{\partial C_i(P_{g_i})}{\partial P_{g_i}} - \lambda + \sum_{j=1}^{B_g} \tau_j A_{ji} + \sum_{l=1}^{B_f} \mu_l S_{li} = 0 & \forall i = 1, \dots, N_b \\ \text{(ii)} \quad & \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} L_{d_i} \\ \text{(iii)} \quad & \sum_{i=1}^{N_b} A_{ji} P_{g_i} = \hat{C}_j & \forall j = 1, \dots, B_g \\ \text{(iv)} \quad & \sum_{i=1}^{N_b} S_{li} [P_{g_i} - L_{d_i}] = D_l & \forall l = 1, \dots, B_f. \end{aligned}$$

after which the above KKT equations are perturbed with respect to P_{g_i} , L_{d_i} , \hat{C}_j , λ , τ_j , and μ_j as follows:

$$\begin{aligned}
\text{(i)} \quad & \underbrace{\frac{\partial}{\partial P_{g_i}} \left(\frac{\partial C_i(P_{g_i})}{\partial P_{g_i}} \right)}_{M_i} dP_{g_i} - d\lambda + \sum_{j=1}^{B_g} A_{ji} d\tau_j + \sum_{l=1}^{B_f} S_{li} d\mu_l = 0 \quad \forall i = 1, \dots, N_b \\
\text{(ii)} \quad & \sum_{i=1}^{N_b} dP_{g_i} = \sum_{i=1}^{N_b} dL_{d_i} \\
\text{(iii)} \quad & \sum_{i=1}^{N_b} A_{ji} dP_{g_i} = d\hat{C}_j \quad \forall j = 1, \dots, B_g \\
\text{(iv)} \quad & \sum_{i=1}^{N_b} S_{li} dP_{g_i} = \sum_{i=1}^{N_b} S_{li} dL_{d_i} \quad \forall l = 1, \dots, B_f.
\end{aligned}$$

It should be noted that the variables D_l , A_{ji} , and S_{li} in the KKT equations are not perturbed. This is due to the fact that 1) the limits of line flow constraint limits in the Ex-ante model are not updated by the state estimator, and 2) the network topology is not affected by corrupted analog data. These perturbation equations can be expressed in matrix form:

$$\underbrace{\begin{bmatrix} \mathbf{M} & -\mathbf{1}_{N_b} & \Upsilon \\ \mathbf{1}_{N_b}^T & \mathbf{0} & \mathbf{0} \\ \Upsilon^T & \mathbf{0} & \mathbf{0} \end{bmatrix}}_{\Xi} \begin{bmatrix} d\mathbf{P}_g \\ d\lambda \\ d\boldsymbol{\tau}_s \\ d\boldsymbol{\mu}_s \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{U}_1^T & \mathbf{U}_2^T \end{bmatrix}}_{\Phi} \begin{bmatrix} d\mathbf{L}_d \\ d\hat{\mathbf{C}}_s \end{bmatrix} \quad (4.26)$$

where

$$\mathbf{M}_{(N_b \times N_b)} = \text{diag}(M_1, \dots, M_{N_b}) \quad (4.27)$$

$$\Upsilon_{(N_b \times [B_g + B_f])} = \begin{bmatrix} \mathbf{A}_s^T & \mathbf{B}_s^T \end{bmatrix} \quad (4.28)$$

$$\mathbf{U}_1_{(N_b \times [N_b + 1 + B_g + B_f])} = \begin{bmatrix} \mathbf{0} & \mathbf{1}_{N_b} & \mathbf{0} & \mathbf{B}_s^T \end{bmatrix} \quad (4.29)$$

$$\mathbf{U}_2_{(B_g \times [N_b + 1 + B_g + B_f])} = \begin{bmatrix} \mathbf{0} & \mathbf{0}_{B_g} & \mathbf{I}_{B_g} & \mathbf{0} \end{bmatrix}. \quad (4.30)$$

Taking the inverse of Ξ on both sides of (4.26),

$$\begin{bmatrix} d\mathbf{P}_g \\ d\lambda \\ d\boldsymbol{\tau}_s \\ d\boldsymbol{\mu}_s \end{bmatrix} = \underbrace{\Xi^{-1}\Phi}_{\Lambda_p} \begin{bmatrix} d\mathbf{L}_d \\ d\hat{\mathbf{C}}_s \end{bmatrix}. \quad (4.31)$$

The subscript s of the variables in (4.26), (4.28), and (4.29) represents the subvector (submatrix) of the original vector (matrix) that corresponds to the binding constraints. The matrix Λ_p in (4.31) is partitioned into two sensitivity matrices— $\Lambda_{\mathbf{L}_d}$ and $\Lambda_{\hat{\mathbf{C}}_s}$:

$$\Lambda_p = \left[\Lambda_{\mathbf{L}_d} \mid \Lambda_{\hat{\mathbf{C}}_s} \right] = \begin{bmatrix} \frac{\partial \mathbf{P}_g}{\partial \mathbf{L}_d} & \frac{\partial \mathbf{P}_g}{\partial \hat{\mathbf{C}}_s} \\ \frac{\partial \lambda}{\partial \mathbf{L}_d} & \frac{\partial \lambda}{\partial \hat{\mathbf{C}}_s} \\ \frac{\partial \boldsymbol{\tau}_s}{\partial \mathbf{L}_d} & \frac{\partial \boldsymbol{\tau}_s}{\partial \hat{\mathbf{C}}_s} \\ \frac{\partial \boldsymbol{\mu}_s}{\partial \mathbf{L}_d} & \frac{\partial \boldsymbol{\mu}_s}{\partial \hat{\mathbf{C}}_s} \end{bmatrix}. \quad (4.32)$$

Using the sensitivities of two shadow prices with respect to $\hat{\mathbf{C}}_s \left(\frac{\partial \lambda}{\partial \hat{\mathbf{C}}_s}, \frac{\partial \boldsymbol{\mu}_s}{\partial \hat{\mathbf{C}}_s} \right)$ in $\Lambda_{\hat{\mathbf{C}}_s}$ and according to the definition of LMP [46], we finally construct the matrix Λ_A .

On the other hand, in the Ex-post model, (4.26) can be extended as follows:

$$\begin{bmatrix} \mathbf{M} & -\mathbf{1}_{N_b} & \Upsilon \\ \mathbf{1}_{N_b}^T & 0 & \mathbf{0} \\ \Upsilon^T & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} d\mathbf{P}_g \\ d\lambda \\ d\boldsymbol{\tau}_s \\ d\boldsymbol{\mu}_s \end{bmatrix} = \begin{bmatrix} \mathbf{U}_1^T & \mathbf{U}_2^T & \mathbf{U}_3^T \end{bmatrix} \begin{bmatrix} d\hat{\mathbf{P}}_g \\ d\hat{\mathbf{C}}_s \\ d\hat{\mathbf{D}}_s \end{bmatrix}. \quad (4.33)$$

$\hat{\mathbf{D}}_s$ is the subvector of $\hat{\mathbf{D}}$ (the real power flow estimate vector) that corresponds to the binding constraints, and

$$\mathbf{U}_{\mathbf{3}(B_f \times [N_b+1+B_g+B_f])} = \begin{bmatrix} \mathbf{0} & \mathbf{0}_{B_f} & \mathbf{0} & \mathbf{I}_{B_f} \end{bmatrix}. \quad (4.34)$$

Compared to (4.32), Λ_p in the Ex-post model is written as

$$\Lambda_p = \left[\Lambda_{\hat{\mathbf{P}}_g} \mid \Lambda_{\hat{\mathbf{C}}_s} \mid \Lambda_{\hat{\mathbf{D}}_s} \right] = \begin{bmatrix} \frac{\partial \mathbf{P}_g}{\partial \hat{\mathbf{P}}_g} & \frac{\partial \mathbf{P}_g}{\partial \hat{\mathbf{C}}_s} & \frac{\partial \mathbf{P}_g}{\partial \hat{\mathbf{D}}_s} \\ \frac{\partial \lambda}{\partial \hat{\mathbf{P}}_g} & \frac{\partial \lambda}{\partial \hat{\mathbf{C}}_s} & \frac{\partial \lambda}{\partial \hat{\mathbf{D}}_s} \\ \frac{\partial \tau}{\partial \hat{\mathbf{P}}_g} & \frac{\partial \tau}{\partial \hat{\mathbf{C}}_s} & \frac{\partial \tau}{\partial \hat{\mathbf{D}}_s} \\ \frac{\partial \mu}{\partial \hat{\mathbf{P}}_g} & \frac{\partial \mu}{\partial \hat{\mathbf{C}}_s} & \frac{\partial \mu}{\partial \hat{\mathbf{D}}_s} \end{bmatrix}. \quad (4.35)$$

• Sensitivity of State Estimation to SCADA Data

Sensitivity analysis of state estimation subject to SCADA measurements was pioneered by Stuart and Herget [59], who investigated the effect of power system modeling errors on weighted least squares (WLS) state estimation. A more rigorous sensitivity analysis method, based on the same perturbation approach illustrated in [53], has been proposed by Mínguez and Conejo [60]. This method has been formulated in a general optimization problem that allows for the sensitivity analysis of alternative state estimation methods with different objective functions, such as the least absolute value (LAV) from the weighted least squares. It should be noted that, in this paper, the sensitivity analysis is based on WLS state estimation. However, one can apply it to various state estimation methods by using the method proposed in [60].

In this subsection, we first derive the matrix Λ_B that illustrates the sensitivities of the real power injection and real flow measurement estimates with respect to the changes in all types of measurements. In equation (4.4), the matrix $\Psi(\hat{\mathbf{x}}^k)$ is defined and partitioned as

$$\Psi(\hat{\mathbf{x}}^k) = [\mathbf{G}(\hat{\mathbf{x}}^k)]^{-1} \mathbf{H}^T(\hat{\mathbf{x}}^k) \mathbf{R}^{-1} = \begin{bmatrix} \Psi_{\hat{\boldsymbol{\theta}}}(\hat{\mathbf{x}}^k) \\ \Psi_{\hat{\mathbf{V}}}(\hat{\mathbf{x}}^k) \end{bmatrix} \quad (4.36)$$

where $\Psi_{\hat{\boldsymbol{\theta}}}(\hat{\mathbf{x}}^k)$ and $\Psi_{\hat{\mathbf{V}}}(\hat{\mathbf{x}}^k)$ represent the sensitivities of the voltage phase angle estimates and the magnitudes with respect to all perturbed measurements at the

k -th iteration, respectively. Therefore, (4.4) can be rewritten as

$$\left[\frac{d\hat{\boldsymbol{\theta}}^{k+1}}{d\hat{\mathbf{V}}^{k+1}} \right] = \left[\frac{\boldsymbol{\Psi}_{\hat{\boldsymbol{\theta}}(\hat{\mathbf{x}}^k)}}{\boldsymbol{\Psi}_{\hat{\mathbf{V}}(\hat{\mathbf{x}}^k)}} \right] d\mathbf{z}. \quad (4.37)$$

It should be noted that the DCOPF-based SCED is formulated with linearized real power injection and a flow estimation solution [61]. Using the linear equations in the upper partition of equation (4.37) and the matrix $\boldsymbol{\Psi}_{\hat{\boldsymbol{\theta}}}$ computed with the converged estimate $\hat{\mathbf{x}}$, we have the following sensitivity equation:

$$d\hat{\mathbf{z}}_r = \begin{bmatrix} \mathbf{B}_{P\theta}^S \\ \mathbf{B}_{P\theta} \\ \mathbf{B}_{F\theta} \end{bmatrix} d\hat{\boldsymbol{\theta}} = \begin{bmatrix} \mathbf{B}_{P\theta}^S \\ \mathbf{B}_{P\theta} \\ \mathbf{B}_{F\theta} \end{bmatrix} \boldsymbol{\Psi}_{\hat{\boldsymbol{\theta}}} d\mathbf{z} = \mathbf{K} d\mathbf{z} \quad (4.38)$$

where

$$\mathbf{K} = \begin{bmatrix} \mathbf{B}_{P\theta}^S \\ \mathbf{B}_{P\theta} \\ \mathbf{B}_{F\theta} \end{bmatrix} \boldsymbol{\Psi}_{\hat{\boldsymbol{\theta}}}. \quad (4.39)$$

$d\hat{\mathbf{z}}_r$ is the perturbed estimate vector of the real power injection and the flow measurements. The matrix $\mathbf{B}_{P\theta} = \mathbf{A}_r \mathbf{B}_d \mathbf{A}_r^T$ is defined as the $(N_b - 1) \times (N_b - 1)$ reduced node-to-node susceptance matrix that explains the relationship between real power injections at any bus except the slack bus and the phase angles. Here $\mathbf{B}_d = \text{diag}(s_1, s_2, \dots, s_{N_l})$ is the $N_l \times N_l$ diagonal branch susceptance matrix and \mathbf{A}_r is the $(N_b - 1) \times N_l$ reduced node-to-branch incidence matrix without a slack bus. According to the law of conservation of power, the $1 \times (N_b - 1)$ matrix $\mathbf{B}_{P\theta}^S = -\mathbf{1}_{(N_b-1)}^T \mathbf{B}_{P\theta}$ is derived, and it explains the relationship between real power injections at the slack bus and the phase angles. The matrix $\mathbf{B}_{F\theta} = \mathbf{B}_d \mathbf{A}_r^T$ specifies the relationship between real power flows and the phase angles. Using (4.39), we compute the matrix $\boldsymbol{\Lambda}_B = \mathbf{K}$.

4.3.3 Simulation Studies

In this section, we illustrate and verify the proposed approach to quantifying the sensitivities of real-time LMP with respect to changes in sensor data. The proposed sensitivity analysis is applied to IEEE 14-bus and 118-bus systems. System data for the IEEE 14-bus system are taken from the MATPOWER 4.0 IEEE 14-bus test case file. Table 4.2 shows the generator parameters in the IEEE 14-bus system.

Table 4.2: Generator Parameters in the IEEE 14-bus System.

Bus	$P_{g_i}^{\min}$	$P_{g_i}^{\max}$	a_i (\$/MWh)	b_i (\$/(MW) ² h)
1	0MW	332.4MW	20	0.043
2	0MW	140MW	20	0.25
3	0MW	100MW	40	0.01
6	0MW	100MW	40	0.01
8	0MW	100MW	40	0.01

In this simulation, the measurement configuration consists of 8 voltage magnitude measurements, 8 pairs of real and reactive power injection measurements, and 12 pairs of real and reactive power flow measurements. V_i is the measurement of voltage magnitude at bus i , P_i and Q_i are the measurements of real and reactive power injection at bus i , respectively, and $P_{i,j}$ and $Q_{i,j}$ are the measurements of real and reactive power flow from bus i to bus j , respectively. Fig. 4.3 shows the IEEE 14-bus system with a measurement configuration that consists of the following five measurement sets:

$$\mathcal{S}_v = \{V_2, V_3, V_7, V_8, V_{10}, V_{11}, V_{12}, V_{14}\}$$

$$\mathcal{S}_{ri} = \{P_2, P_3, P_7, P_8, P_{10}, P_{11}, P_{12}, P_{14}\}$$

$$\mathcal{S}_{ai} = \{Q_2, Q_3, Q_7, Q_8, Q_{10}, Q_{11}, Q_{12}, Q_{14}\}$$

$$\mathcal{S}_{rf} = \{P_{1,2}, P_{2,3}, P_{4,2}, P_{4,7}, P_{4,9}, P_{5,2}, P_{5,4}, P_{5,6}, P_{6,13}, P_{7,9}, P_{11,6}, P_{12,13}\}$$

$$\mathcal{S}_{af} = \{Q_{1,2}, Q_{2,3}, Q_{4,2}, Q_{4,7}, Q_{4,9}, Q_{5,2}, Q_{5,4}, Q_{5,6}, Q_{6,13}, Q_{7,9}, Q_{11,6}, Q_{12,13}\}.$$

In this measurement configuration, the locations of the voltage magnitude measurements are consistent with those of the real and reactive power injection measurements. For each measurement set, the measurement index is numbered from one to the total number of measurements in each set. We assume that all measure-

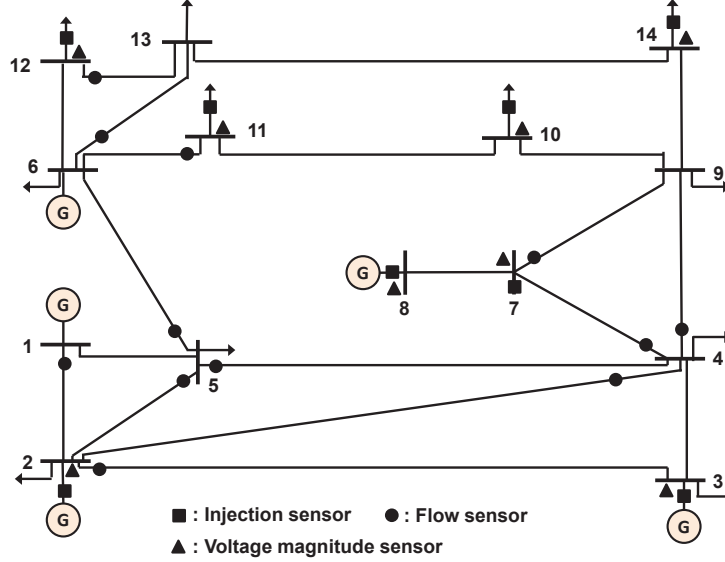


Figure 4.3: IEEE 14-bus system with a given measurement configuration.

ments are corrupted by additive Gaussian noises with equal variances $\sigma^2=0.00001$. Finally, for all buses i , j , and k , we compute LMP sensitivities with respect to the five types of measurements—real/reactive power injection, real/reactive power

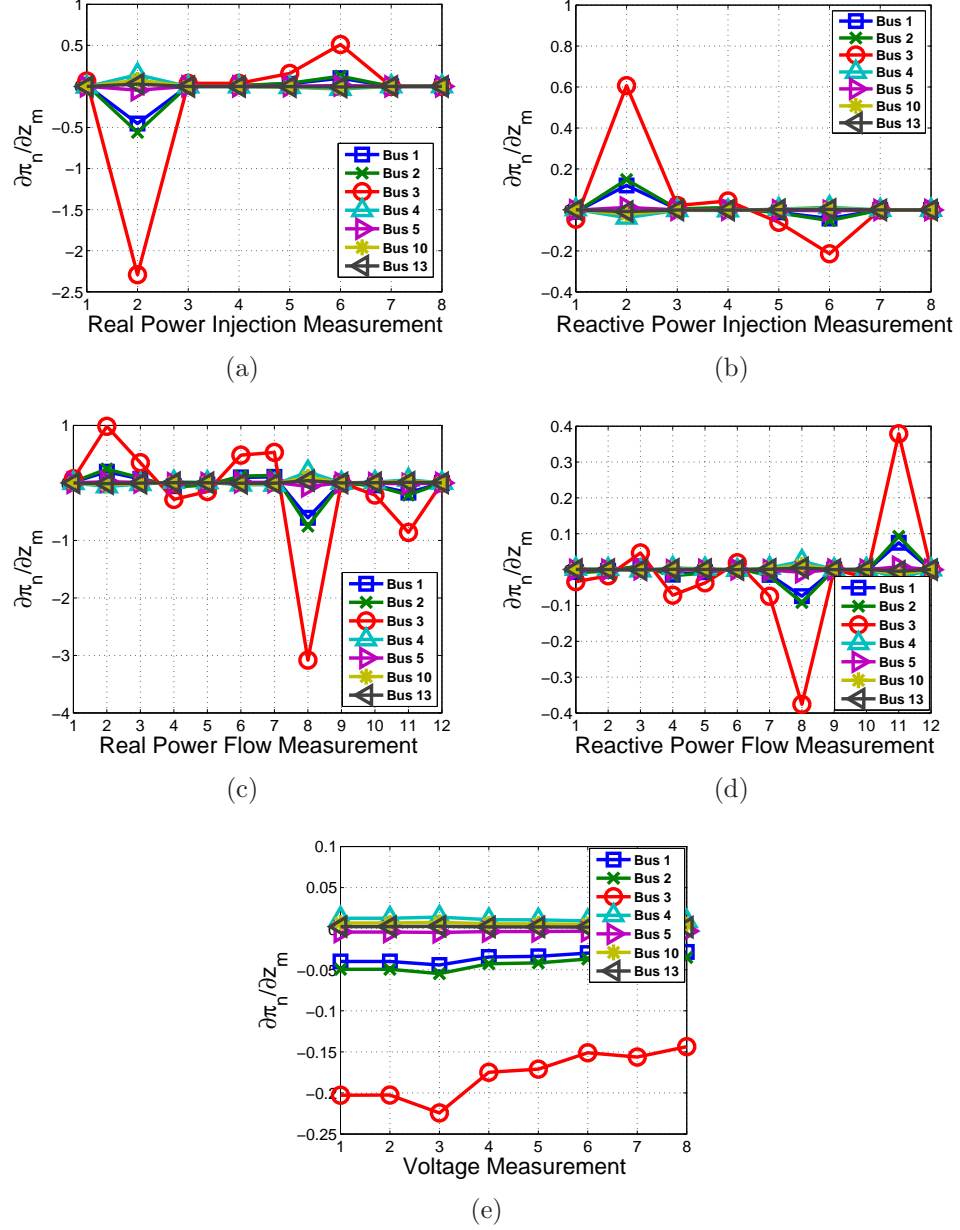


Figure 4.4: Sensitivities of Ex-ante prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 3-4 is congested and P_{g_3} is binding at $\hat{P}_{g_3}^{\min}$ in the IEEE 14-bus system.

flow, and voltage magnitude—as follows:

$$\frac{\partial \pi_i}{\partial P_j}, \quad \frac{\partial \pi_i}{\partial Q_j}, \quad \frac{\partial \pi_i}{\partial P_{j,k}}, \quad \frac{\partial \pi_i}{\partial Q_{j,k}}, \quad \frac{\partial \pi_i}{\partial V_j}. \quad (4.40)$$

Units for the sensitivities $\left\{ \frac{\partial \pi_i}{\partial P_j}, \frac{\partial \pi_i}{\partial P_{j,k}} \right\}$, $\left\{ \frac{\partial \pi_i}{\partial Q_j}, \frac{\partial \pi_i}{\partial Q_{j,k}} \right\}$, and $\left\{ \frac{\partial \pi_i}{\partial V_j} \right\}$ are $(\$/\text{MWh})/(\text{puMW})$, $(\$/\text{MWh})/(\text{puMVar})$, and $(\$/\text{MWh})/(\text{puV})$, respectively.

Fig. 4.4 provides snapshots of five different Ex-ante LMP sensitivities in (4.40) at some buses in the IEEE 14-bus system with line 3-4 congestion. These figures provide information about the directions of the post-corruption LMPs as well as their sensitivities with respect to each type of measurement at a given dispatch time. In this simulation, after the Ex-ante dispatch problem has been solved, there exist two binding generation capacity constraints: P_{g_3} and P_{g_8} are binding at $\hat{P}_{g_3}^{\min}$ and $\hat{P}_{g_8}^{\max}$, respectively. We assume that the corruption of the measurements impacts the binding constraint associated with P_{g_3} . In other words, the corrupted measurements affect $\hat{P}_{g_3}^{\min}$ (an intermediate variable in (4.21)), subsequently leading to changes in all the LMPs. We randomly choose seven buses (buses 1, 2, 3, 4, 5, 10, 13) out of the fourteen to differentiate clearly the LMP sensitivities among the various buses. The absolute values of the LMP sensitivities at buses 3 and 5 are the largest and smallest, setting the upper and lower bounds for sensitivity at the fourteen buses. We obtain from the simulation results the following observations:

- (O1) *Sensitivity grouping property*: all buses can be categorized into two sensitivity groups. In each group, buses obtain sensitivities with the same sign, but of different magnitude and subject to all types of measurements. Group I includes buses 1, 2, 3 and 5, and Group II buses 4, 10 and 13. For example, in Fig. 4.4(b) the corruption of z_2 yields positive sensitivities for Group I and negative sensitivities for Group II, whereas the corruption of z_6 yields the

reverse: negative sensitivities for Group I and positive sensitivities for Group II. This grouping property enables system operators to predict rapidly the direction of LMP's distortion in response to sensor data corruption.

(O2) *Identification of buses that are economically sensitive to data corruption:* buses incident to both ends of the congested line have the highest LMP sensitivities with respect to sensor data corruption. For example, bus 3 in Group I and bus 4 in Group II incident to congested line 3-4 have the largest absolute sensitivities in each group. In particular, it should be noted that the largest sensitivities are associated with bus 3. This implies that bus 3 is the most financially vulnerable to any corruption in sensor measurement.

(O3) *Identification of influential sensors on LMP:* the sensor most influential on LMP change is identified in each measurement group. In Fig. 4.4(a),(b), the sensors with z_2 (P_3 and Q_3) have the most significant impact on LMP. This is due to the fact that the change of the intermediate variable \hat{P}_{g3}^{\min} is dominantly affected by P_3 and Q_3 , subsequently leading to more change in LMP. This effect is also verified in Fig. 4.9(a),(b) based on the IEEE-118 bus system. In Fig. 4.4(c),(d) and (e), the sensors with z_8, z_{11} and z_3 ($P_{5,6}$, $Q_{11,6}$ and V_7) are the most influential, respectively. In addition, it should be noted that the localized effects on increasing sensitivity of measurements adjacent to the congested line and/or the intermediate variable do not always hold true. For example, z_{11} ($P_{11,6}$) is farther away from both the congested line and the intermediate variable than z_5 ($P_{4,9}$); however, in Fig. 4.4(c), data corruption in the former leads to a higher sensitivity than in the latter. This non-localized data effect motivates system operators to use our developed tool for identifying which sensors impact LMP sensitivity.

(O4) *Impact of different types of sensor data on LMP:* through a comparison of all

the figures, LMP appears to be more sensitive to real power injection/flow measurements than to reactive power injection/flow and voltage magnitude measurements. In order to compare the sensitivities of different units fairly, a normalized LMP sensitivity $|z_j| \frac{\partial \pi_i}{\partial z_j}$ is defined, which is incorporated into the following proposed metric:

$$\Omega_k^i = \sum_{j=1}^{|\mathcal{S}_k|} \left| |z_j| \frac{\partial \pi_i}{\partial z_j} \right| / |\mathcal{S}_k| \quad (4.41)$$

where Ω_k^i is the average of the absolute normalized sensitivities at bus i with respect to any measurement z_j in the set \mathcal{S}_k ($k = v, ri, ai, rf, af$). The cardinality of the set $|\mathcal{S}_k|$ means the number of elements in \mathcal{S}_k . For example, at bus 3, we compute $\Omega_{ri}^3 = 0.474$, $\Omega_{rf}^3 = 0.253$, $\Omega_v^3 = 0.175$, $\Omega_{af}^3 = 0.013$, and $\Omega_{ai}^3 = 0.012$, which is consistent with our expectation that real power injection and flow measurements have a more significant impact on LMP sensitivity than other measurements. This is due to the fact that DCOPF-based SCED is conducted based on a linearized state estimation solution that is more influenced by real power measurements than by reactive power and voltage magnitude measurements, as illustrated in (4.37) and (4.38).

- (O5) In Fig. 4.4(e), LMP sensitivities at all buses affected by corrupted voltage magnitude measurements fluctuate more smoothly than the ones affected by other types of corrupted measurements. In other words, all voltage magnitude measurements impact LMP variations almost evenly. In addition, the non-localized effect mentioned in (O3) is also verified between z_2 (V_3) and z_3 (V_7).

Fig. 4.5 provides snapshots of the Ex-post LMP sensitivities at arbitrarily chosen buses (buses 1, 6, 7, 9, 12, 13 and 14) with respect to the aforementioned

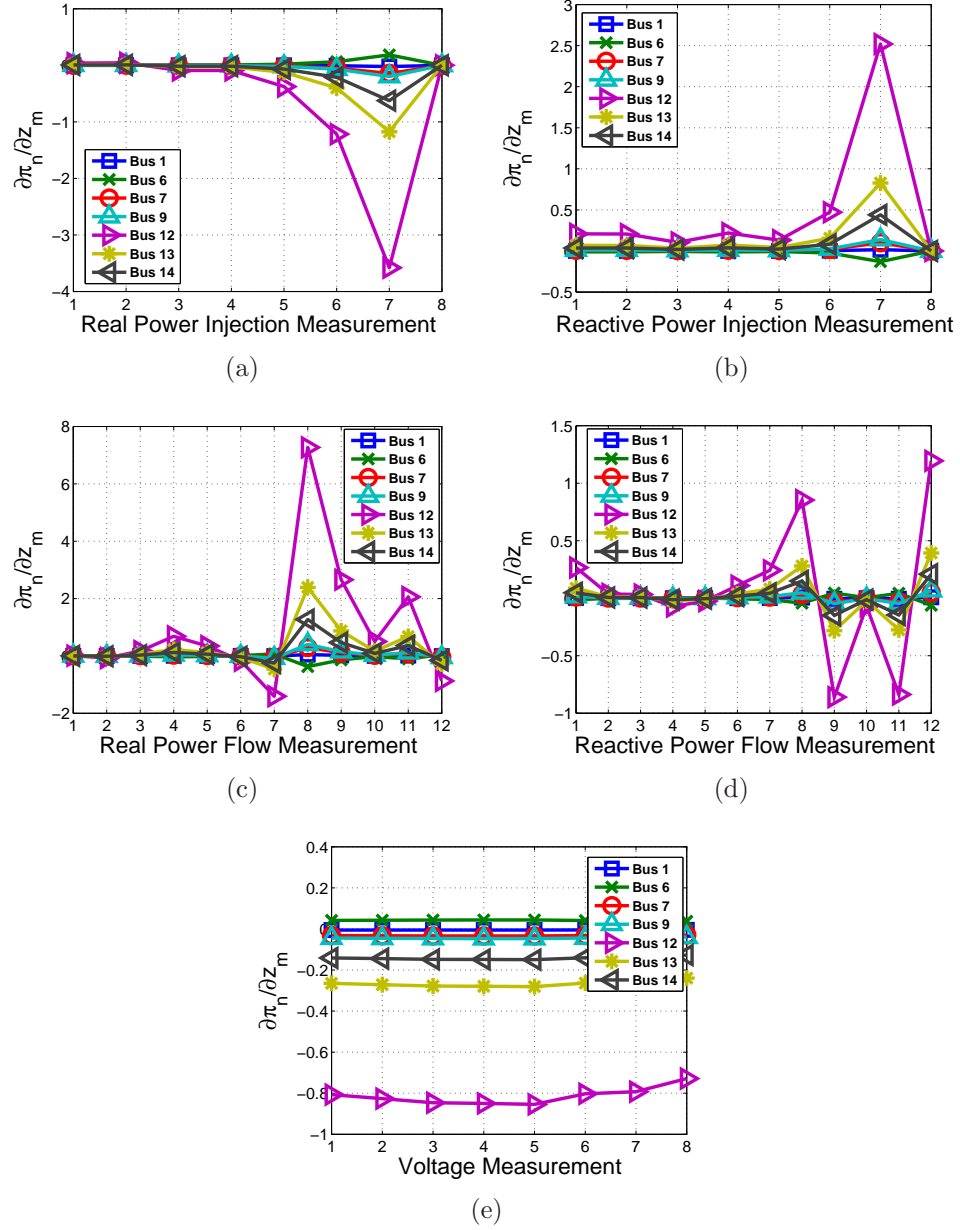


Figure 4.5: Sensitivities of Ex-post prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 6-12 is congested and the corresponding line flow is binding at the capacity limit of line 6-12 in the IEEE 14-bus system.

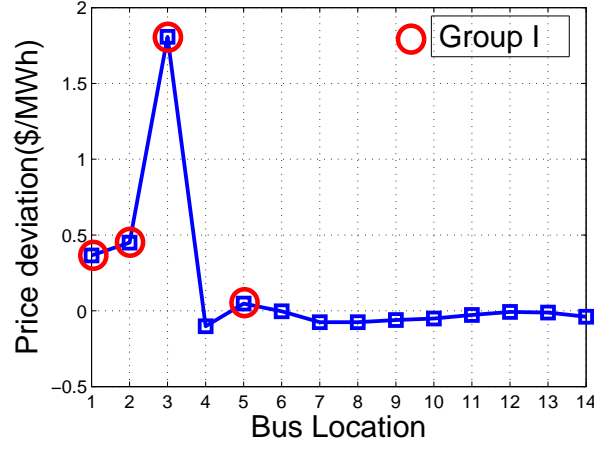


Figure 4.6: LMP differences between with and without corrupted data when z_8 is corrupted in Fig. 4.4(c).

five types of sensor measurements. In this simulation, line 6-12 is assumed to be congested at both Ex-ante dispatch and Ex-post dispatch. $\hat{P}_{6,12}$ is chosen as an intermediate variable to compute LMP sensitivity. We can observe from Fig. 4.5 the same phenomena as in Fig. 4.4: (O1) Group 1 for buses 1 and 6, and Group 2 for buses 7, 9, 12, 13 and 14; (O2) buses 6 and 12 incident to the congested line have the largest absolute value of LMP sensitivity in each group; (O3) in Fig. 4.5(a) and (b), the sensors with z_7 (P_{12} and Q_{12}) have the most significant impact on LMP, and in Fig. 4.5(c), (d) and (e), the sensors with z_8 , z_{12} and z_5 ($P_{5,6}$, $Q_{12,13}$ and V_{10}) are the most influential, respectively; and (O4) & (O5) real power measurements have a stronger impact on LMP sensitivity than the reactive power and voltage magnitude measurements, and the voltage magnitude measurements influence LMP sensitivity almost evenly.

Fig. 4.6 shows actual Ex-ante LMP and how they differ when they have or do not have corrupted data at all buses. It is assumed that the magnitude of z_8 is corrupted by 2% in Fig. 4.4(c). In the Chi-squares test [52] within a 99% confidence

level, the estimated objective functions and the bad data detection threshold are computed. $J(\hat{x}) = 15.69$ and $J^{(b)}(\hat{x}) = 30.17$ correspond to the values of the estimated objective functions without and with corrupted data, respectively, and $\chi^2 = 38.93$ is the value of the bad data detection threshold. It should be noted that since $J^{(b)}(\hat{x}) = 30.17 < \chi^2 = 38.93$, the corrupted measurement z_8 bypasses the bad data detection engine, which could then lead to LMP distortion. As expected, Fig. 4.6 justifies the result of our sensitivity analysis in two main ways. First, the prices at buses 1, 2, 3, and 5 in Group I change in a positive direction whereas the prices at the buses in Group II change in a negative direction. This observation explains the grouping property specified in (O1). Second, the descending order of the magnitudes of the actual price deviations is in accordance with that of sensitivity magnitudes. For example, Fig. 4.4(c) shows that buses 3, 2, 1 and 5 in Group I are in descending order of sensitivity magnitudes, which is consistent with the descending order of the actual price deviations at those same buses in Fig. 4.6.

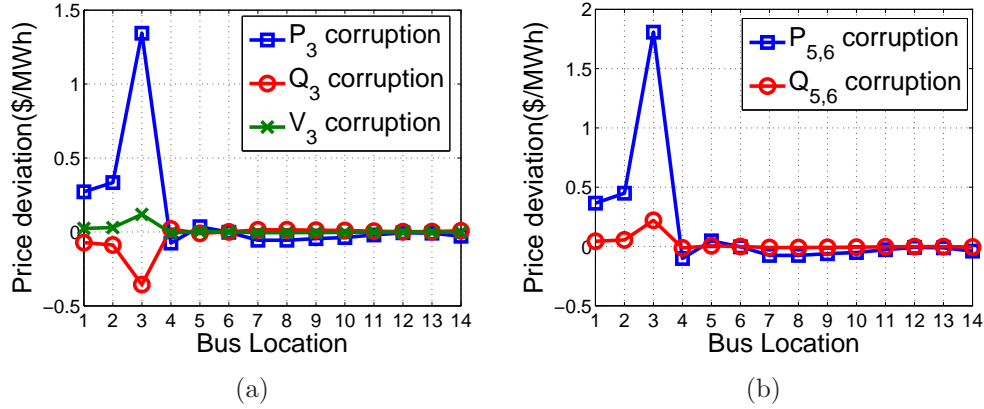


Figure 4.7: LMP differences between with and without corrupted data in Fig. 4.4 (a) P_3 , Q_3 , and V_3 corruptions (b) $P_{5,6}$ and $Q_{5,6}$ corruptions.

Fig. 4.7 shows the Ex-ante LMP deviations that are caused by the undetectable same amount of corruption in each measurement group $\{P_3, Q_3, V_3\}$ and $\{P_{5,6}, Q_{5,6}\}$. These figures show that real power injection and flow measurements have

a more significant impact on LMP than other measurements. This fact justifies observation (O4).

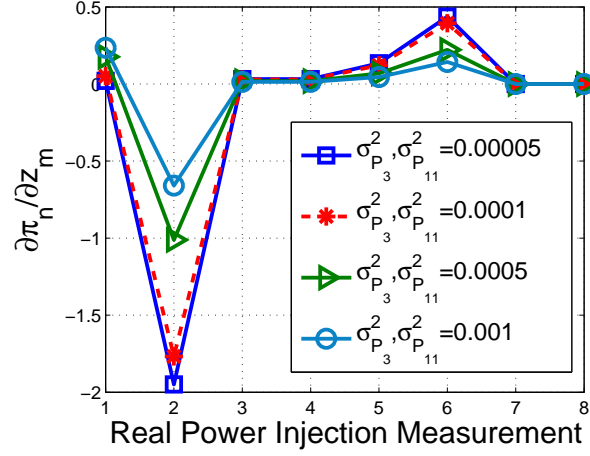


Figure 4.8: Comparison of LMP sensitivities at bus 3 in Fig. 4.4(a) with varying variances of injection measurements P_3 and P_{11} .

Fig. 4.8 shows the impact of sensor measurement accuracy on LMP sensitivity. In this figure, four plots represent LMP sensitivities at bus 3 in Fig. 4.4(a), with consistently varying variances of the two injection measurements z_2 (P_3) and z_6 (P_{11}). These sensitivities are measured at four different variance levels; $\sigma^2=0.00005$, 0.0001 , 0.0005 , and 0.001 . We can observe from Fig. 4.8 that, as the measurement variance decreases (i.e., the measurement accuracy increases), the corresponding LMP sensitivity increases. In other words, more accurate sensors lead to more change in LMP while sensor data remain corrupted. This shows the coupling between state estimation accuracy and LMP calculation. Based on this observation, one possible guideline for mitigating the financial risk from data corruption is to make it a high priority to protect accurate sensors.

For the IEEE 118-bus system, with 54 generation buses and 186 transmission lines as shown in Fig. 4.10, we assume that real and reactive power injection mea-

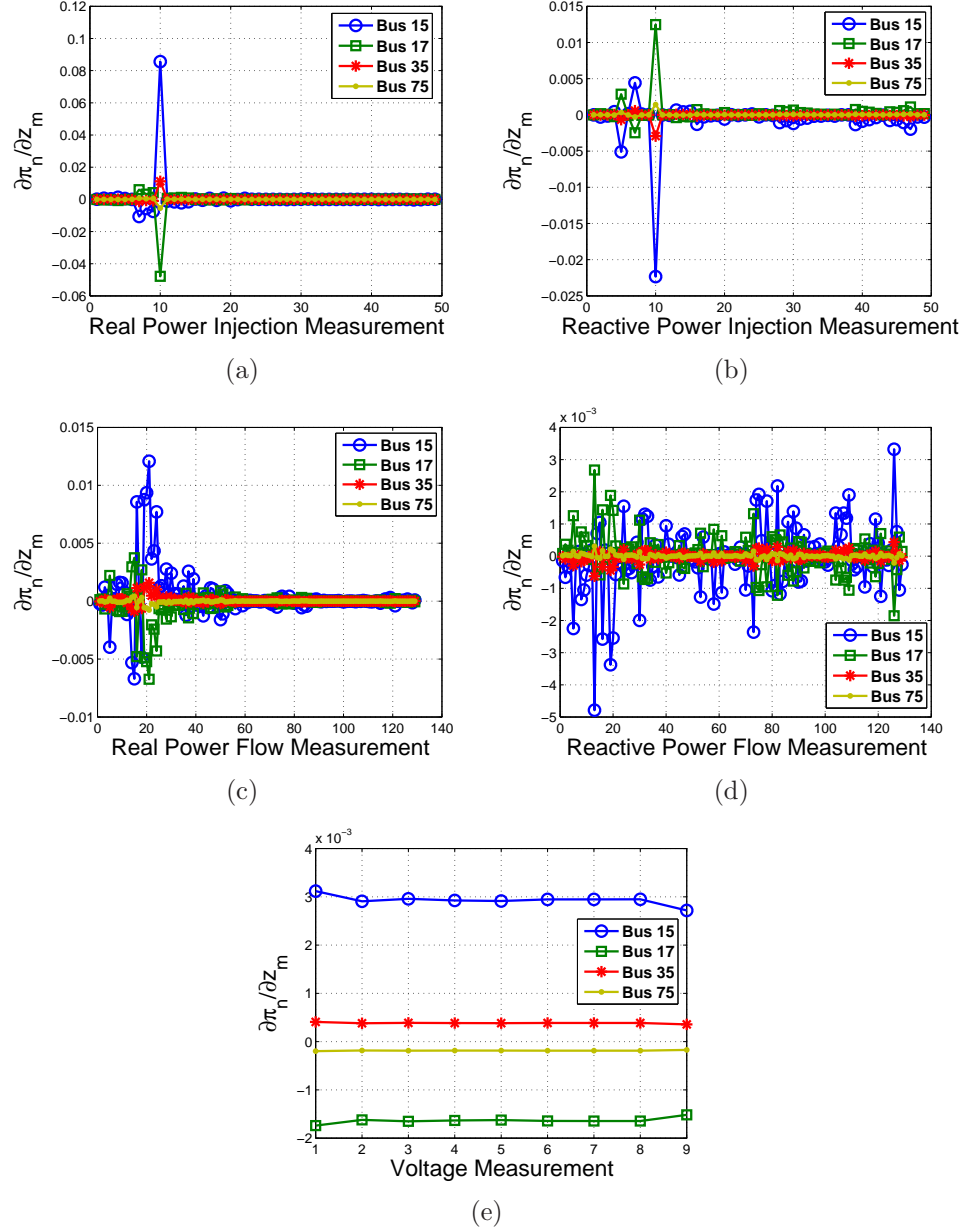


Figure 4.9: Sensitivities of Ex-ante prices with respect to (a) real power injection measurements, (b) reactive power injection measurements, (c) real power flow measurements, (d) reactive power flow measurements, and (e) voltage magnitude measurements. Line 15-17 is congested and $P_{g_{19}}$ is binding at $\hat{P}_{g_{19}}^{\max}$ in the IEEE 118-bus system.

measurements are placed at 49 generator buses, voltage magnitude measurements at 9 generator buses, and real and reactive flow measurements at 129 lines. Therefore, this system has a total of 365 measurements. System data for the IEEE 118-bus system are taken from the MATPOWER 4.0 IEEE 118-bus test case file.

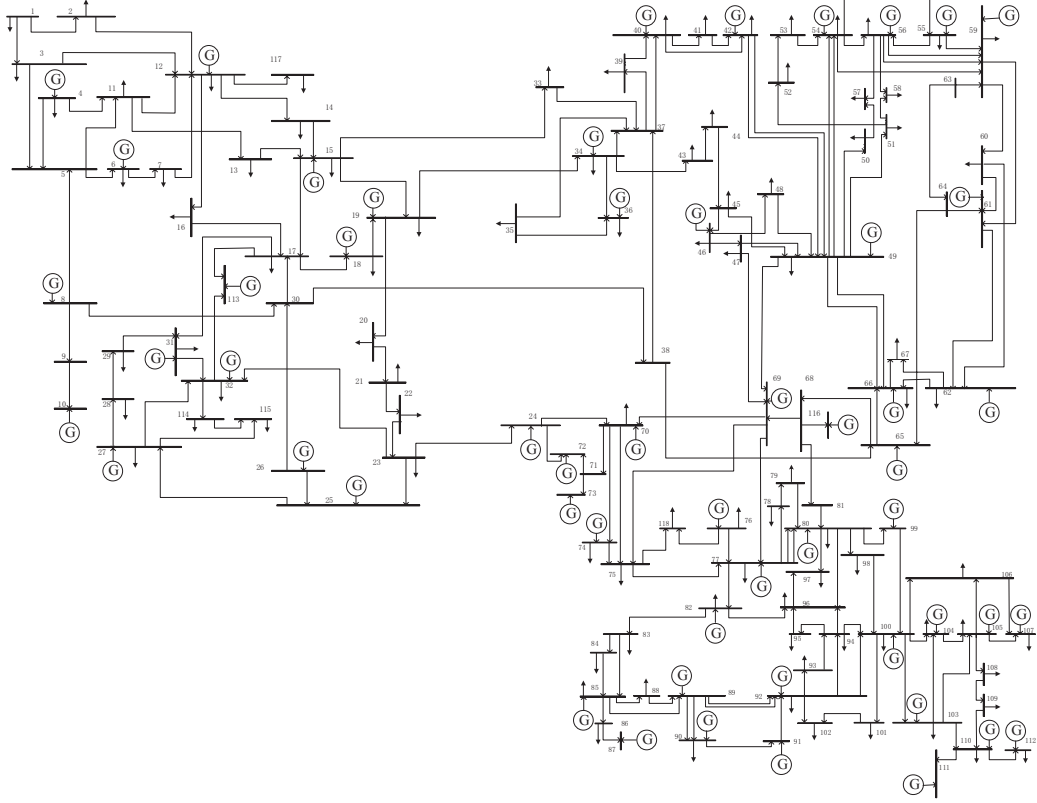


Figure 4.10: IEEE 118-bus system.

Fig. 4.9 show the Ex-ante LMP sensitivities at buses 15, 17, 35, and 75 in the IEEE 118-bus system with line 15-17 congestion with respect to the five different types of measurement. The magnitudes of the sensitivities at buses 15 and 17 are the highest in each sensitivity group. \hat{P}_{19}^{\max} is chosen as an intermediate variable to compute LMP sensitivity. As expected, all observations from Fig. 4.4 are also verified in the larger IEEE 118-bus system: 1) sensor grouping property (Group

1: buses 15 and 35, and Group 2: buses 17 and 75); 2) identification of the most economically sensitive buses in each group (buses 15 and 17) and the most influential sensors (e.g., z_{10} with P_{19} and Q_{19} in Fig. 4.9(a)(b)) on LMP change; and 3) the impact of different types of sensor data on LMP (e.g., the more significant impact of real power measurements than other types of measurements).

4.4 Impact Analysis of LMP Subject to Network Topology

Estimate Errors

4.4.1 Preliminaries

We consider a state estimation model based on a linearized DC power flow. The measurements taken by each sensor are written by

$$\mathbf{z} = \mathbf{J}\mathbf{x} + \mathbf{e} \quad (4.42)$$

where \mathbf{x} is the state vector of the entire power system, \mathbf{z} is measurement vector, \mathbf{e} is independent identically distributed (i.i.d.) Gaussian random measurement error vector with zero mean and covariance matrix \mathbf{R} , and \mathbf{J} is the *true* system Jacobian matrix of the state vector \mathbf{x} . Then, the weighted least squares estimate of \mathbf{x} is calculated by

$$\hat{\mathbf{x}}(\mathbf{z}) = (\mathbf{J}^T \mathbf{R}^{-1} \mathbf{J})^{-1} \mathbf{J}^T \mathbf{R}^{-1} \mathbf{z}. \quad (4.43)$$

Topology error processing detects and identifies topology errors based on measurement residuals. The wrongly reported circuit breaker status data generate two

types of topology errors: (i) line status error; and (ii) substation configuration error. The former represents an incorrect exclusion/inclusion of transmission lines from the network model whereas the latter a split/merging error of buses at the substation. In this section, we focus on line status error and substation configuration error is beyond the scope of this paper. For line status error, the measurement equation (4.42) is rewritten as

$$\mathbf{z} = \mathbf{J}_\mathbf{E}\mathbf{x} + \mathbf{E}\mathbf{x} + \mathbf{e}$$

where $\mathbf{J} = \mathbf{J}_\mathbf{E} + \mathbf{E}$. Here, $\mathbf{J}_\mathbf{E}$ is the incorrect system Jacobian matrix due to topology errors. \mathbf{E} is the system Jacobian error matrix. Then, topology error detection is performed using the normalized residual vector as follows:

$$E(\mathbf{r}^N) = \Omega^{-\frac{1}{2}}(\mathbf{I} - \mathbf{K}_\mathbf{E})\mathbf{M}\mathbf{f} = \mathbf{S}\mathbf{f} \underset{H_0}{\overset{H_1}{\geq}} \eta \quad (4.44)$$

where \mathbf{M} is the measurement-to-branch incidence matrix, \mathbf{f} is a vector of branch flow errors, $\mathbf{K}_\mathbf{E} = \mathbf{J}_\mathbf{E}(\mathbf{J}_\mathbf{E}^T\mathbf{R}^{-1}\mathbf{J}_\mathbf{E})^{-1}\mathbf{J}_\mathbf{E}^T\mathbf{R}^{-1}$, $\Omega = \text{diag}\{Cov(\mathbf{r})\}$, $\mathbf{S} = \Omega^{-\frac{1}{2}}(\mathbf{I} - \mathbf{K}_\mathbf{E})\mathbf{M}$ is the sensitivity matrix for \mathbf{r}^N with respect to branch flow errors \mathbf{f} , and η is the threshold of topology error detection. H_1 and H_0 correspond to the cases with and without topology error, respectively. In this section, we assume that the attack proposed in [56] successfully changes network topology estimate while bypassing topology error detection (4.44).

Ex-ante and Ex-post models rely on the network topology and the cost functions of generators. Therefore, our results illustrated in the next subsection are applicable to both models. In this section, we consider a real-time Ex-ante market model where LMPs are computed before the actual deployment of dispatch orders. For the system operator, the Ex-ante dispatch is formulated as follows,

$$\min_{p_i} \sum_{i \in G} C_i \cdot p_i \quad (4.45)$$

s.t.

$$\lambda : \sum_{n=1}^{N_b} P_{g_n} = \sum_{n=1}^{N_b} L_{d_n} \quad (4.46)$$

$$\boldsymbol{\tau} : p_i^{\min} \leq p_i \leq p_i^{\max} \quad \forall i \in G \quad (4.47)$$

$$\boldsymbol{\mu} : F_l^{\min} \leq \sum_{n=1}^{N_b} H_{l,n}(P_{g_n} - L_{d_n}) \leq F_l^{\max} \quad \forall l = 1, \dots, N_l \quad (4.48)$$

In this formulation, the objective function is to minimize the total generation costs in (4.45). (4.46) is the system-wide energy balance equation. (4.47) is the physical capacity constraints of each generator. (4.48) is the transmission line constraints. λ , $\boldsymbol{\tau}$, and $\boldsymbol{\mu}$ are the dual variables associated with the aforementioned equality and inequality constraints. $\boldsymbol{\tau}$ and $\boldsymbol{\mu}$ are expressed as $\boldsymbol{\tau} = [\boldsymbol{\tau}_{\max}^T, \boldsymbol{\tau}_{\min}^T]^T$ and $\boldsymbol{\mu} = [\boldsymbol{\mu}_{\max}^T, \boldsymbol{\mu}_{\min}^T]^T$ where subscript max(min) represents max(min) inequality constraint. $H_{l,n}$ is the element at the l th row and n th column of the $N_l \times N_b$ distribution factor matrix \mathbf{H} . This matrix explains the sensitivity of branch flows to nodal injection powers. The real-time LMP vector $\boldsymbol{\pi}$ is computed using the following equation [46]:

$$\boldsymbol{\pi} = \lambda \mathbf{1}_{N_b} - \mathbf{H}^T [\boldsymbol{\mu}_{\max} - \boldsymbol{\mu}_{\min}]. \quad (4.49)$$

4.4.2 Derivation of the Proposed LMP Sensitivity Index

In this subsection, we derive a simple sensitivity index to quantify the impact of network topology errors on LMP. This derivation is based on the following assumptions:

- (A1) Only one single transmission line is congested for both cases with and without topology error.

(A2) Network congestion patterns and marginal units remain unchanged with topology error.

(A3) The value of λ (LMP at slack bus) remains unchanged with topology error.

In (A2), a marginal unit is defined as a unit that generates power between its minimum and maximum capacity. The above assumptions would hold true under the situation in which other lines except a congested line have sufficient transmission capacity. It should be noted that these assumptions do not capture all the possible scenarios in actual operation. However, a large number of scenarios would fit into these assumptions under normal to light loading situations. Future work will expand the analysis to a broader set of scenarios.

We first present Proposition 1 where the shadow price associated with a congested line is expressed as the ratio of the gap of the energy costs of marginal units to the gap of distribution factors that correspond to the intersections of marginal units and the congested transmission line. It serves as the theoretical basis for the main result of this paper (equation (4.65)), which does not require extensive numerical simulations in order to determine the sensitivity of LMP to network topology errors.

Proposition 1. *Let i and j be two marginal units with $C_j > C_i$, belonging to different buses. Then, the shadow price for the congested transmission line l is expressed as*

$$\mu_l = \frac{\Delta C(j, i)}{\Delta H_l(i, j)} \quad (4.50)$$

where $\Delta C(j, i) = C_j - C_i$ and $\Delta H_l(i, j) = H_{l,i} - H_{l,j}$.

Proof. The shadow price of a congested transmission line is defined as the change of

total dispatch cost via relaxing the transmission constraint by one unit. Therefore, the shadow price for the congested transmission line l can be written as

$$\mu_l = - \sum_{i \in G} C_i \Delta p_i, \quad (4.51)$$

which satisfies the following two constraints:

$$\sum_{n=1}^{N_b} \Delta P_{g_n} = 0 \quad (4.52)$$

$$\sum_{n=1}^{N_b} H_{l,n} \Delta P_{g_n} = 1. \quad (4.53)$$

(4.51) is the increasing total generation cost. (4.52) represents that the overall demand still needs to be balanced. (4.53) is the line flow equation obtained by relaxing the constraint of the transmission line l by 1MW. Then, using (4.51) and (4.52),

$$\mu_l \stackrel{(a)}{=} -C_i \Delta P_{g_i} - C_j \Delta P_{g_j} \stackrel{(b)}{=} -C_i \Delta P_{g_i} + C_j \Delta P_{g_i} = (C_j - C_i) \Delta P_{g_i} \quad (4.54)$$

where (a) follows from the property that a single transmission line congestion yields two marginal units [62], thus setting the variable ΔP_i associated with any other unit to be zero, and (b) follows from (4.52). Similarly, (4.53) can be rewritten as

$$1 = H_{l,i} \Delta P_{g_i} + H_{l,j} \Delta P_{g_j} = H_{l,i} \Delta P_{g_i} - H_{l,j} \Delta P_{g_i} = (H_{l,i} - H_{l,j}) \Delta P_{g_i}. \quad (4.55)$$

Finally, the combination of (4.54) and (4.55) provides the following desired result,

$$\mu_l = \frac{[C_j - C_i]}{[H_{l,i} - H_{l,j}]} = \frac{\Delta C(j, i)}{\Delta H_l(i, j)}. \quad (4.56)$$

□

Proposition 1 together with (A1)-(A3) implies the following corollaries.

Corollary 4.4.0.1. *Consider the situation under (A1)-(A3). Suppose that the line l is congested. Then, the LMP sensitivity index with respect to the line k status error ($k \neq l$) is written as*

$$\Delta \boldsymbol{\pi}_l^k = \Delta C(j, i) \mathbf{v}_l^k \quad (4.57)$$

where

$$\Delta \boldsymbol{\pi}_l^k = [\Delta \pi_{l,1}^k, \dots, \Delta \pi_{l,N_b}^k]^T \quad (4.58)$$

$$\mathbf{v}_l^k = [v_{l,1}^k, \dots, v_{l,N_b}^k]^T \quad (4.59)$$

$$v_{l,n}^k = \frac{\tilde{H}_{l,n}^k}{\Delta \tilde{H}_l^k(i, j)} - \frac{H_{l,n}}{\Delta H_l(i, j)}. \quad (4.60)$$

Proof. For simplicity, the shadow price corresponding to only a positive line congestion is considered in (4.49). Under assumption (A1)-(A2), the LMPs vectors without and with the line k status error are written as

$$\boldsymbol{\pi}_l = \lambda \mathbf{1}_{N_b} - \mu_l \mathbf{H}_l^T \quad (4.61)$$

$$\tilde{\boldsymbol{\pi}}_l^k = \tilde{\lambda}^k \mathbf{1}_{N_b} - \tilde{\mu}_l^k \tilde{\mathbf{H}}_l^{kT} \quad (4.62)$$

where \mathbf{H}_l is the l th row vector of the distribution factor matrix \mathbf{H} . In (4.62), a tilde symbol over characters refers to topology error. Then, under assumption (A3) (i.e., $\lambda = \tilde{\lambda}^k$) the LMP sensitivity vector that illustrates the differences between LMPs without and with topology error is written as

$$\Delta \boldsymbol{\pi}_l^k = \boldsymbol{\pi}_l - \tilde{\boldsymbol{\pi}}_l^k = \tilde{\mu}_l^k \tilde{\mathbf{H}}_l^{kT} - \mu_l \mathbf{H}_l^T. \quad (4.63)$$

From Proposition 1, the shadow price corrupted by topology error is expressed as

$$\tilde{\mu}_l^k = \frac{[C_j - C_i]}{[\tilde{H}_{l,i}^k - \tilde{H}_{l,j}^k]} = \frac{\Delta C(j, i)}{\Delta \tilde{H}_l^k(i, j)}. \quad (4.64)$$

Finally, substituting (4.56) and (4.64) into (4.63),

$$\begin{aligned}
\Delta \boldsymbol{\pi}_l^k &= \left[\frac{\Delta C(j, i)}{\Delta \tilde{H}_l^k(i, j)} \right] \tilde{\mathbf{H}}_l^{kT} - \left[\frac{\Delta C(j, i)}{\Delta H_l(i, j)} \right] \mathbf{H}_l^T \\
&= \Delta C(j, i) \left[\frac{\tilde{\mathbf{H}}_l^{kT}}{\Delta \tilde{H}_l^k(i, j)} - \frac{\mathbf{H}_l^T}{\Delta H_l(i, j)} \right] \\
&= \Delta C(j, i) \mathbf{v}_l^k.
\end{aligned} \tag{4.65}$$

That is, the sensitivity of LMP at any bus to any line status error is written as the multiplication form of two independent functions which depend on: (i) the energy costs of marginal units; and (ii) congested line-related distribution factors at any bus and marginal units, respectively. \square

Corollary 4.4.0.2. *For any buses n and m ($n \neq m$),*

1. *If $v_{l,n}^k > 0$, LMP at bus n with topology error decreases, otherwise it remains the same or increases.*
2. *$|v_{l,n}^k| > |v_{l,m}^k|$ implies that LMP sensitivity at bus n is higher than at bus m .*
3. *The increase (decrease) of $\Delta C(j, i)$ leads to the increase (decrease) of LMP sensitivity at any bus.*

By Corollary 4.4.0.2(a), buses can be categorized into three groups with positive, negative and zero sensitivities. This grouping property enables system operators to make a quick prediction for the direction of post-LMPs by topology error. By Corollary 4.4.0.2(b), economically sensitive buses to topology error can be identified through the comparison of $|v_{l,n}^k|$. Corollary 4.4.0.2(c) allows system operators to assess the impact of the energy costs of marginal units on LMP sensitivity. Furthermore, it may provide guidelines for making a bidding strategy of

market participants such as generation company. Fig. 4.11 illustrates a linear relationship scaled by $\Delta C(j, i)$ between $\Delta \pi_l^k$ and \mathbf{v}_l^k , as well as sensitivity grouping, identification of economically sensitive buses and impact of varying $\Delta C(j, i)$ on LMP sensitivity, all of which are mentioned in Corollary 4.4.0.2.

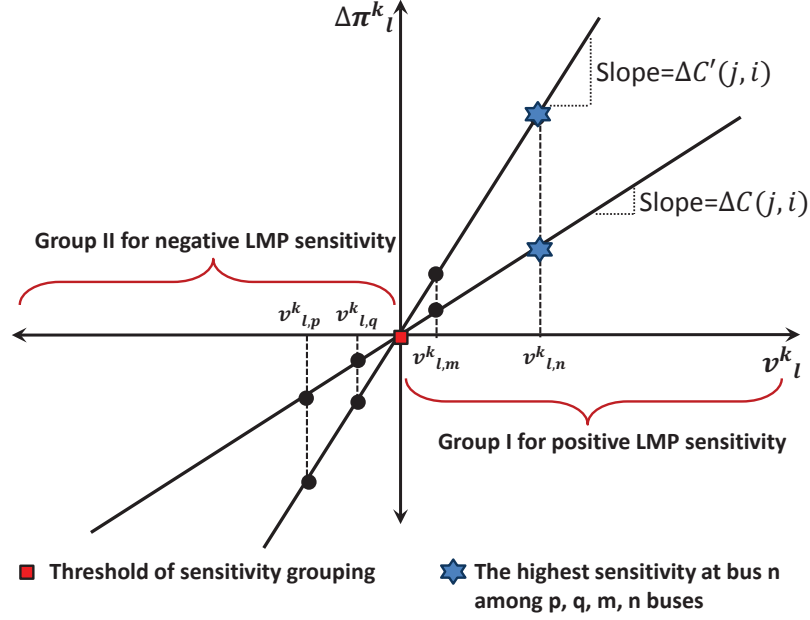


Figure 4.11: Illustration of a linear relationship between $\Delta \pi_l^k$ and \mathbf{v}_l^k .

4.4.3 Simulation Studies

In this subsection, we illustrate and verify the proposed analytical results in quantifying the impact of network topology errors on LMP in the IEEE 14-bus system. Fig. 4.12 shows the detailed bus-breaker model for the IEEE 14-bus system. In this figure, one scenario is illustrated where the misconfigured status of the circuit breaker at bus 5 leads to the (dotted) line 4-5 exclusion error as long as the line 5-6 is congested. It is assumed that this misconfiguration occurs due to a natural error

or man-made attack [56], [57] and hence the corrupted network topology information is fed into economic dispatch module without being detected by topology error processing. Table 4.3 shows generator parameters in the IEEE 14-bus system.

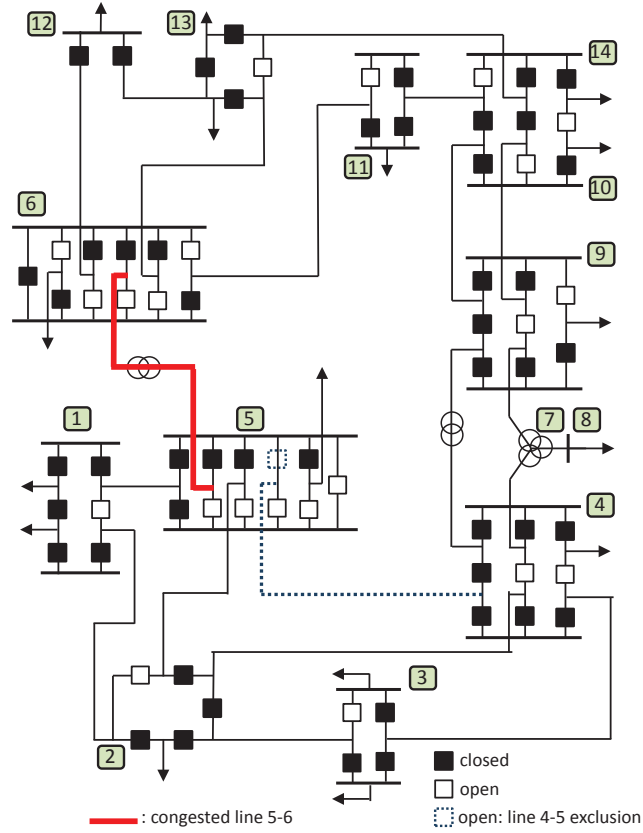


Figure 4.12: IEEE 14-bus system including bus-breaker model.

Figs. 4.13 show the LMPs from the scenario illustrated in Fig. 4.12. Fig. 4.13(a) shows LMPs at all buses with and without the line exclusion error, respectively. These LMPs are obtained as the by-product of SCED formulated in Section 4.4.1. It should be noted in this scenario that the exclusion of the line 4-5 keeps both marginal units (at buses 1 and 8) and congestion pattern (the line 5-6 congestion) unchanged. Fig. 4.13(b) shows two LMP sensitivity plots for all buses with respect to the line 4-5 exclusion. Each plot is obtained using a different approach, which

Table 4.3: Generator Parameters of the IEEE 14-bus Test System.

Bus	P_{\min}	P_{\max}	Marginal Cost
1	0MW	330MW	30\$/MWh
2	0MW	140MW	20\$/MWh
3	0MW	100MW	40\$/MWh
6	0MW	100MW	55\$/MWh
8	0MW	100MW	60\$/MWh

is based on SCED and the proposed analytical approach in Corollary 4.4.0.1. We emphasize again that in comparison with SCED approach the proposed approach computes LMP sensitivities using the derived sensitivity index without further economic redispatch. This could lead to reduced computational time compared with exhaustive numerical simulations. We can observe from Fig. 4.13(b) that the result of the proposed approach is consistent with that of SCED. This observation also holds true in other line exclusion cases under different network congestions. However, due to limited space, the validity of the test results for all other cases is not shown in this paper. We note that LMP sensitivities in all subsequent figures are computed in the proposed approach.

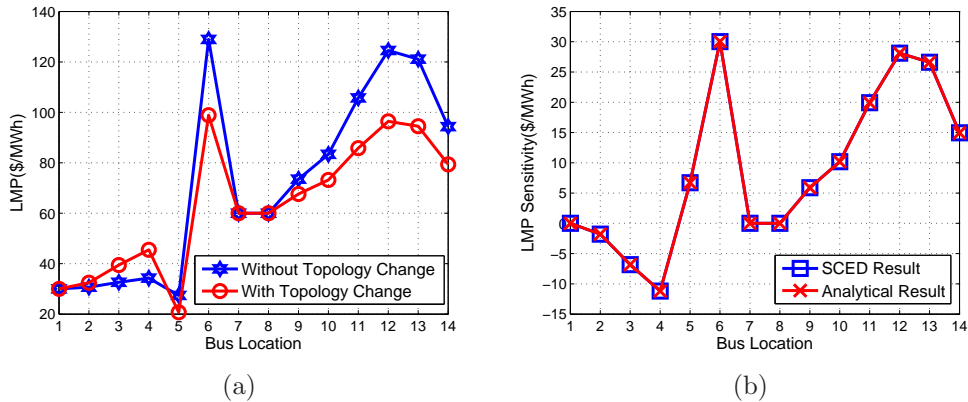


Figure 4.13: LMP results in Fig. 4.12: (a) comparison of LMPs between with and without line exclusion error; (b) comparison of LMP sensitivities obtained by SCED and the proposed approach.

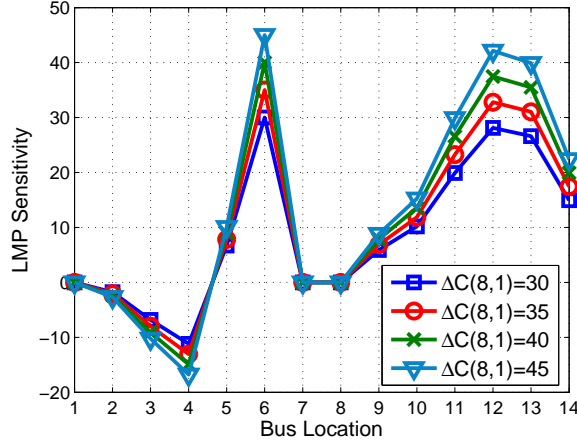


Figure 4.14: Impact of a varying gap between the energy costs of marginal units on LMP sensitivity.

Fig. 4.14 illustrates the impact of a varying gap between the energy costs of marginal units on LMP sensitivity. The results in this figure are based on the same system condition as in Fig. 4.12 so that marginal units are connected to buses 1 and 8, respectively. The energy cost of generator at bus 8 in Table 4.3 is assumed to increase from 60\$/MWh to 75\$/MWh with a step size of 5\$/MWh, thus changing the value of $\Delta C(8,1)$ from 30 to 45. We can observe from Fig. 4.14 that as the gap between the energy costs of marginal units increases, the absolute value of LMP sensitivity at any bus increases as well. This observation justifies Corollary 4.4.0.2(c).

Fig. 4.15 shows LMP sensitivities with four different line exclusion errors under the identical congestion pattern where the line 5-6 is congested. For a clear comparison of sensitivities, we randomly choose four different lines (lines 1-2, 1-5, 2-4 and 6-12) out of twenty lines and then exclude each line from the network model to evaluate the impact of the line exclusion on LMP. First, we observe from Fig. 4.15 that LMP sensitivities at all buses with respect to the line 1-2 exclusion are higher

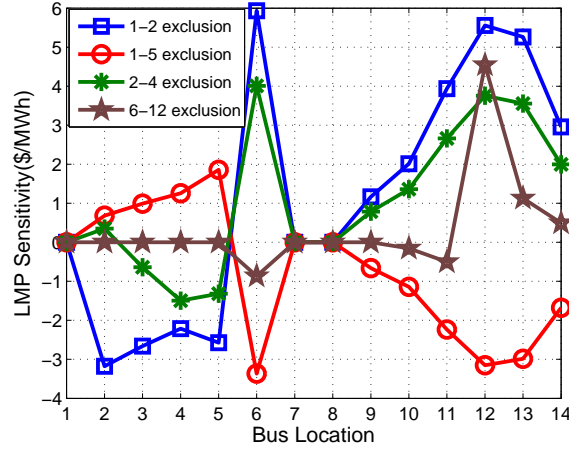


Figure 4.15: Comparison of LMP sensitivities with four different branch exclusion errors under the line 5-6 congestion.

than those with respect to other line exclusions. Therefore, the line 1-2 among chosen four lines has the most significant impact on LMP sensitivity at any bus. From a cybersecurity perspective, sensors collecting the status of CBs associated with the line 1-2 should be protected against bad data or malicious cyber attack with a high priority. Second, the most economically sensitive bus to topology error is identified in each line exclusion. For example, bus 6 has the highest sensitivity to the exclusion of the lines 1-2, 1-5 and 2-4 whereas bus 12 to the exclusion of the line 6-12. Lastly, we verify that buses are grouped according to the sign of sensitivity. For the line 1-2 exclusion, buses (6, 9~14) obtain positive sensitivities, buses (2~5) negative sensitivities and buses (1, 7~8) have zero sensitivities. In particular, using the sign of sensitivity system operators are capable of predicting a market participant' profit or loss. For example, the sensitivities at generation bus 6 to the exclusions of lines 1-2 and 2-4 are positive so that post LMPs decrease, consequently providing a generation company a financial loss. On the other hand, since the sensitivities at the same bus to the exclusions of lines 1-5 and 6-12 are negative, a generation company makes a profit with increasing LMP.

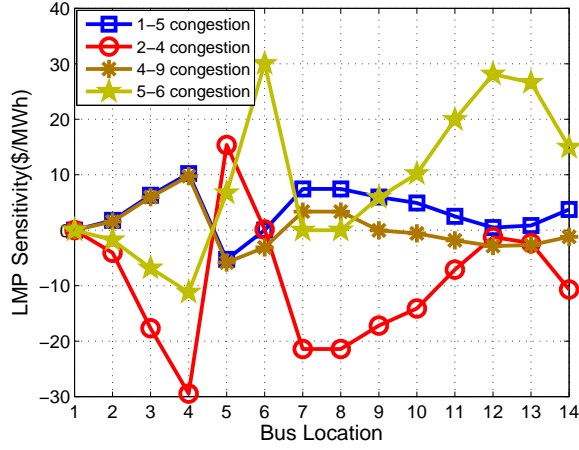


Figure 4.16: Comparison of LMP sensitivities with four different congestion patterns under the line 4-5 exclusion.

Fig. 4.16 shows the sensitivities with respect to the line 4-5 exclusion under four different congestion patterns (the congestions of the lines 1-5, 2-4, 4-9 and 5-6). In this figure, the impact of different congested lines on LMP sensitivity is quantified for all buses. For example, it is observed that the line 2-4 congestion among the chosen four line congestions leads to the highest sensitivity at bus 4.

4.5 Conclusions

In this chapter, the main research consists of two parts where we present an analytical framework for calculating LMP sensitivity in response to variations in power flow and network topology estimate due to the corruption of continuous and discrete sensor data.

In the first part, corrupted *continuous* sensor data are shown to deviate power

system state estimation from their actual values, which subsequently leads to the distortion of real-time market LMPs. We build two matrices: the first with LMP sensitivity at any bus to any estimate, and the second with sensitivity of any estimate to data at any sensor. A unified matrix that combines these two matrices in multiplication form enables system operators to quantify the impact on LMP of data at any sensor at any bus throughout the entire transmission network. Our simulation results suggest that the proposed sensitivity matrix can provide system operators with a quick and accurate method to identify the buses most vulnerable to measurement errors. In addition, we verify that more accurate sensors impact LMP much more significantly.

In the second part, we examine the impact of circuit breaker-induced network topology errors due to *discrete* data corruption on real-time LMP. We derive an analytical index to compute LMP sensitivity with respect to network topology error, particularly line status error, in the power system. The proposed sensitivity index provides system operators an analytical tool to identify economically sensitive transmission lines and circuit breakers, whose status error will significantly impact the real-time LMPs. The proposed sensitivity index is tested using the IEEE 14-bus system. Future work could expand the analysis and study the sensitivity of LMP due to topology error in a more general sense without assumptions (A1)-(A3) in this paper. The LMP sensitivity index due to topology error could also be extended toward a comprehensive financial risk management tool for system operators and market participants.

CHAPTER 5

TOPOLOGY ATTACK OF A SMART GRID: UNDETECTABLE ATTACKS AND COUNTERMEASURES

5.1 Introduction

A defining feature of a smart grid is its abilities to monitor the state of a large power grid, to adapt to changing operating conditions, and to react intelligently to contingencies, all of which depend critically on a reliable and secure cyber-infrastructure. It has been widely recognized that the heavy reliance on a wide area communication network for grid monitoring and real-time operation comes with increasing security risks of cyber-attacks. See [63] for a vulnerability analysis of energy delivery control systems.

While *information* security has been a major focus of research for over half a century, the mechanisms and the impacts of attack on *cyber physical systems* such as the power grid are not yet well understood, and effective countermeasures are still lacking.

We consider a form of “man-in-the-middle” (MiM) attack [64] on the topology of a power grid. An MiM attack exploits the lack of authentication in a system, which allows an adversary to impersonate a legitimate participant. In the context of monitoring a transmission grid, sophisticated authentications are typically not implemented due to the need of reducing communication delay and the presence of legacy communication equipment. If an adversary is able to gain access to remote

terminal units (RTUs) or local data concentrators, it is possible for the adversary to replace actual data packets with carefully constructed malicious data packets and impersonate a valid data source.

MiM attacks on a power grid may have severe consequences. The adversary can mislead the control center that the grid is operating under a topology different from that in reality. Such an attack, if launched successfully and undetected by the control center, will have serious implications: a grid that is under stress may appear to be normal to the operator thereby delaying the deployment of necessary measures to ensure stability. Similarly, a grid operating normally may appear to be under stress to the operator, potentially causing load shedding and other costly remedial actions by the operator.

Launching a topology attack, fortunately, is not easy; a modern energy management system is equipped with relatively sophisticated bad data and topology error detectors, which alerts the operator that either the data in use are suspicious or there may indeed be changes in the network topology. When there are inconsistencies between the estimated network topology (estimated mostly using switch and breaker states) and the meter data (*e.g.*, there is significant amount of power flow on a line disconnected in the estimated topology,) the operator takes actions to validate the data in use. Only if data and the estimated topology pass the bad data test, will the topology change be accepted and updates be made for subsequent actions.

The attacks that are perhaps the most dangerous are those that pass the bad data detection so that the control center accepts the change (or the lack of change)

of network topology. To launch such attacks, the adversary needs to modify simultaneously the meter data and the network data (switch and breaker states) in such a way that the estimated topology is consistent with the data. Such attacks are referred to as *undetectable attacks*; they are the main focus of our study.

5.1.1 Related Works

Liu, Ning, and Reiter [7] appear to be the first to introduce the concept of data injection attack (also referred to as malicious data attack) of a power grid. Assuming that the attacker is capable of altering data from a set of meters, a similar scenario assumed in our problem setting, the authors of [7] show that if the set of compromised meters satisfies certain condition, the adversary can perturb the network state by an arbitrarily large amount without being detected by any detector. In other words, the data attack considered in [7] is undetectable. The main difference between [7] and our work is that the attacks considered in [7] perturb only the network state, not the network topology. It is thus most appropriate to refer to attacks in [7] and many follow-ups as *state attack*, in distinguishing the *topology attack* considered in our work.

The work in [7] is influential; it has inspired many further developments, *e.g.*, [65, 66, 67, 68] and references therein, all focusing on state attacks. A key observation is made by Kosut *et al.* in [69, 8], showing that the condition of non-existence of an undetectable attack is equivalent to that of network observability [70, 71]. This observation leads to graph theoretic techniques that characterize network vulnerability [8]. The condition to be presented in this chapter on the non-existence

of an undetectable topology attack mirrors the state attack counterpart in [8].

The problem of adding protection on a set of meters to prevent undetectable state attacks was considered by Bobba *et al.* [65]. We consider the same problem in the context of topology attack. While meter protection problem for state attacks is equivalent to protecting a sufficient number of meters to ensure observability [65, 8], the corresponding problem for topology attacks is somewhat different and more challenging.

The problem of detecting topology error from meter data is in fact a classical problem, casted as part of the bad data detection problem [12, 11, 13]. Monticelli [14] pioneers the so-called generalized state estimation approach where, once the state estimate fails the bad data test, modifications of topology that best represent the meter data are considered. Abur *et al.* [72] extend this idea to the least absolute value state estimation formulation, and Mili *et al.* [73] apply the idea to the state estimation with the Huber M-estimator. Extensive works followed to improve computational efficiency, estimation accuracy, and convergence property over the aforementioned methods (*e.g.*, see [74, 75, 76] and references therein). The use of fuzzy pattern recognition [77] was also proposed to identify topology errors based on analog measurements.

Finally, there is a limited discussion on the impact of a malicious data attack on power system operations. Should state estimates be used in closed-loop control of the power grid, such an attack may cause serious stability problems. The current state of the art, however, uses state estimates for real-time dispatch only in a limited fashion. However, state estimates are used extensively in calculating real-

time locational marginal price (LMP) [17]. Thus, attacks that affect state estimates will affect the real-time LMP calculation [16, 78, 9]. The way that a topology attack affects LMP is significantly different from that of a state attack. We demonstrate that a topology attack has significant impact on real-time LMP.

5.1.2 Summary of Results and Organization

We aim to achieve two objectives. First, we characterize conditions under which undetectable attacks are possible, given a set of vulnerable meters that may be controlled by an adversary. To this end, we consider two attack regimes based on the *information set* available to the attacker. The more information the attacker has, the stronger its ability to launch a sophisticated attack that is hard to detect.

The *global information* regime is where the attacker can observe all meter and network data before altering the adversary-controlled part of them. Although it is unlikely in practice that an adversary is able to operate in such a regime, in analyzing the impact of attacks, it is typical to consider the worst case by granting the adversary additional power. In Section 5.3, we present a necessary and sufficient algebraic condition under which, given a set of adversary controlled meters, there exists an undetectable attack that misleads the control center with an incorrect “target” topology. This algebraic condition provides not only numerical ways to check if the grid is vulnerable to undetectable attacks but also insights into which meters to protect to defend against topology attacks. We also provide specific constructions of attacks and show certain optimality of the proposed attacks.

A more practically significant situation is the *local information* regime where the attacker has only local information from those meters it has gained control. Under certain conditions, undetectable attacks exist and can be implemented easily based on simple heuristics. We present in Section 5.4 intuitions behind such simple attacks and implementation details.

The second objective is to provide conditions under which topology attack cannot be made undetectable. Such a condition, even if it may not be the tightest, provides insights into defense mechanisms against topology attacks. In Section 5.5, we show that if a set of meters satisfying a certain branch covering property are protected, then topology attacks can always be detected. In practice, protecting a meter may be carried out at multiple levels, from physical protection measures to software protection schemes using more sophisticated authentication protocols.

The rest of the chapter is organized as follows. Section 5.2 presents mathematical models of state estimation, bad data test, and topology attacks. In Section 5.3, we study topology attacks in the global information regime. The algebraic condition for an undetectable attack is presented, and construction of a cost-effective undetectable attack is provided. Section 5.4 presents a heuristic attack for the attacker with local information. Based on the algebraic condition presented in Section 5.3, Section 5.5 provides a graph theoretical strategy to add protection to a subset of meters to prevent undetectable attacks. Section 5.6 presents simulation results to demonstrate practical uses of our analysis and feasibility of the proposed attacks, and Section 5.7 finishes the chapter with concluding remarks.

5.2 Preliminaries

In this section, we present models for the power network, measurements, and adversary attacks. We also summarize essential operations such as state estimation and bad data detection that are targets of data attacks.

5.2.1 Network and Measurement Models

The control center receives two types of data from meters and sensors deployed throughout the grid. One is the digital network data $\mathbf{s} \in \{0, 1\}^d$, which can be represented as a string of binary bits indicating the on and off states of various switches and line breakers. The second type is the analog meter data \mathbf{z} , which is a vector of bus injection and line flow measurements.

Without an attack or a sensing error, \mathbf{s} gives the true breaker states. Each $\mathbf{s} \in \{0, 1\}^d$ corresponds to a system topology, which is represented by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where \mathcal{V} is the set of buses and \mathcal{E} is the set of *connected* transmission lines. For each physical transmission line between two buses (*e.g.*, i and j), we assign an arbitrary direction for the line (*e.g.*, (i, j)), and (i, j) is in \mathcal{E} if and only if the line is connected. In addition, \mathcal{E}_0 denotes the set of all lines (with the assigned directions), both connected and disconnected. Assigning arbitrary directions for lines is not intended to deliver any physical meaning, but only for ease of presentation.

The state of a power system is defined as the vector \mathbf{x} of voltage phasors on all

buses. In the absence of attacks and measurement noise, the meter data \mathbf{z} collected by the SCADA system are related to the system state \mathbf{x} and the system topology \mathcal{G} via the AC power flow model [4]:

$$\mathbf{z} = h(\mathbf{x}, \mathcal{G}) + \mathbf{e} \quad (5.1)$$

where \mathbf{z} typically includes real and reactive parts of bus injection and line flow measurements, h is the nonlinear measurement function of \mathbf{x} and \mathcal{G} , and \mathbf{e} the additive noise.

A simplified model, one that is often used in real-time operations such as the computation of real-time LMP, is the so-called DC model [4] where the nonlinear function h is linearized near the operating point. In particular, the DC model is given by

$$\mathbf{z} = H\mathbf{x} + \mathbf{e} \quad (5.2)$$

where $\mathbf{z} \in \mathbb{R}^m$ consists of only the real parts of injection and line flow measurements, $H \in \mathbb{R}^{m \times n}$ is the measurement matrix, $\mathbf{x} \in \mathbb{R}^n$ is the state vector consisting of voltage phase angles at all buses except the slack bus, and $\mathbf{e} \in \mathbb{R}^m$ is the Gaussian measurement noise with a diagonal covariance matrix Σ .

The fact that the measurement matrix H depends on the network topology \mathcal{G} is important, although we use the notation H without explicit association with its topology \mathcal{G} for notational convenience. For ease of presentation, consider the noiseless measurement $\mathbf{z} = H\mathbf{x}$. If an entry z_k of \mathbf{z} is the measurement of the line flow from i to j of a *connected* line in \mathcal{G} , z_k is $B_{ij}(x_i - x_j)$ where B_{ij} is the line susceptance and x_i is the voltage phase angle at bus i . The corresponding row of

H is equal to

$$\mathbf{h}_{(i,j)} \triangleq [0 \cdots 0 \quad \underbrace{B_{ij}}_{i\text{th entry}} \quad 0 \cdots 0 \quad \underbrace{-B_{ij}}_{j\text{th entry}} \quad 0 \cdots 0]. \quad (5.3)$$

On the other hand, if z_k is the measurement of the line flow through a *disconnected* line in \mathcal{G} , z_k is zero, and the corresponding row of H consists of all zero entries. If z_k is the measurement of bus injection at i , it is the sum of all the outgoing line flows from i , and the corresponding row of H is the sum of the row vectors corresponding to all the outgoing line flows.

We consider both AC and DC power flow models. The DC model allows us to obtain a succinct characterization of undetectable attacks as described in Section 5.3. However, these results hold only locally around the operating point, because the results are obtained from the linearized model. General results for the more realistic (nonlinear) AC model are difficult to obtain. We present in Section 5.4 a heuristic attack that are undetectable for both AC and DC models.

It was shown in [9] that using the DC model and linear state estimator in numerical analysis of an attack tends to exaggerate the impact of the attack. Hence, for accurate analysis, we use the AC model and nonlinear state estimator in the numerical simulations presented in Section 5.6.

5.2.2 Adversary Model

The adversary aims at modifying the topology estimate from $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ to a different “target” topology $\bar{\mathcal{G}} = (\mathcal{V}, \bar{\mathcal{E}})$. Note that \mathcal{G} and $\bar{\mathcal{G}}$ have the same set

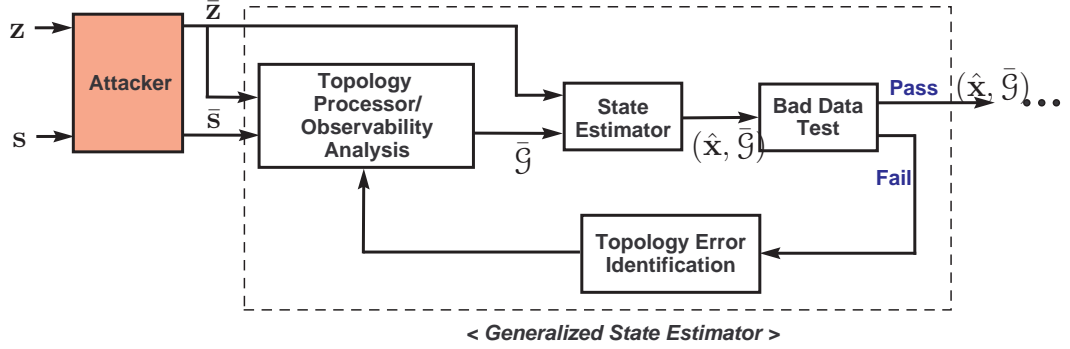


Figure 5.1: Attack Model with Generalized State Estimation

of vertices. In other words, we only consider the attacks aimed at perturbing transmission line connectivities*. In addition, we assume that the power system is observable regardless an attack is present or not: *i.e.*, , the measurement matrix in the DC model always has full rank. This means that the adversary avoids misleading the control center with drastic system changes (*e.g.*, division into two disconnected parts) that may draw too much attention of the control center[†]. We call the lines not common to both $\bar{\mathcal{E}}$ and \mathcal{E} (*i.e.*, , lines in $\bar{\mathcal{E}} \Delta \mathcal{E} \triangleq (\bar{\mathcal{E}} \setminus \mathcal{E}) \cup (\mathcal{E} \setminus \bar{\mathcal{E}})$) *target lines* and the buses at the ends of the target lines *target buses*.

To alter the network topology, the adversary launches a man-in-the-middle attack as described in Fig. 5.1: it intercepts (\mathbf{s}, \mathbf{z}) from RTUs, modifies part of them, and forwards the modified version $(\bar{\mathbf{s}}, \bar{\mathbf{z}})$ to the control center.

Throughout this chapter, except in Section 5.4, we assume that the adversary

*The attacks aiming to split or combine buses are out of scope of this study. Such attacks require modifying the measurements of breaker states *inside* substations. If the control center employs generalized state estimation [79], such modification invokes substation-level state estimation which leads to a robust bad data test. Hence, such attacks are harder to avoid detection.

[†]In fact, the results to be presented in this chapter also hold for the general case where the target topology can be anything (*e.g.*, the system may be divided into several disconnected parts), if the control center employs the same bad data test even when the network is unobservable.

has global information, *i.e.*, it knows network parameters and observes all entries of (\mathbf{s}, \mathbf{z}) before launching the attack, although it may modify only the entries it gained control of. Such an unlimited access to network parameters and data is a huge advantage to the attacker. In Section 5.5, countermeasures are designed under this assumption so that they can be robust to such worst case attacks.

The mathematical model of an attack to modify \mathcal{G} to $\bar{\mathcal{G}}$ is as follows (the notation that a bar is on a variable denotes the value modified by the adversary):

$$\begin{aligned}\bar{\mathbf{s}} &= \mathbf{s} + \mathbf{b} \pmod{2}, \\ \bar{\mathbf{z}} &= \mathbf{z} + \mathbf{a}(\mathbf{z}), \quad \mathbf{a}(\mathbf{z}) \in \mathcal{A},\end{aligned}\tag{5.4}$$

where $\bar{\mathbf{s}}$ is the modified network data corresponding to $\bar{\mathcal{G}}$, $\mathbf{b} \in \{0, 1\}^d$ represents the modifications on the network data \mathbf{s} , $\mathbf{a}(\mathbf{z}) \in \mathbb{R}^m$ denotes the attack vector added to the meter data \mathbf{z} , and $\mathcal{A} \subset \mathbb{R}^m$ denotes the subspace of feasible attack vectors.

We assume that the adversary can modify the network data accordingly for any target topology that deems to be valid to the control center. This is the opposite of the assumption employed by most existing studies on *state* attacks where network data that specify the topology are not under attack.

For the attack on analog meter data, we use the notation $\mathbf{a}(\mathbf{z})$ to emphasize that the adversary can design the attack vector based on the whole meter data \mathbf{z} . This assumption will be relaxed in Section 5.4 to study an attack with local information. In addition, \mathcal{A} has a form of $\{\mathbf{c} \in \mathbb{R}^m : c_i = 0, i \in \mathcal{I}_S\}$ where \mathcal{I}_S is the set of indices of secure meter data entries that the adversary cannot alter and $\{1, \dots, m\} \setminus \mathcal{I}_S$ represents the adversary-controlled entries. Note that \mathcal{A} fully

characterizes the power of the adversary, and the mapping $\mathbf{a} : \mathbb{R}^m \rightarrow \mathcal{A}$ fully defines the attack strategy.

5.2.3 State Estimation, Bad Data Test, and Undetectable Attacks

As illustrated in Fig. 5.1, the control center executes generalized state estimation (GSE) [79] with network and meter data as inputs; the inputs are (\mathbf{s}, \mathbf{z}) in the absence of an attack and $(\bar{\mathbf{s}}, \bar{\mathbf{z}})$ if there is an attack. GSE regards both network and meter data as possibly erroneous. Once the bad data test detects inconsistency among data and estimates, GSE filters out the outliers from the data and searches for a new *pair* of topology and state estimates that fit the data best. Our focus is on the attacks that can pass the bad data test such that no alarm is raised by GSE.

Under the general AC model (5.1), if (\mathbf{s}, \mathbf{z}) is the input to GSE, and $\hat{\mathcal{G}}$ is the topology corresponding to \mathbf{s} , the control center obtains the weighted least squares (WLS) estimate of the state \mathbf{x} :

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{y}} (\mathbf{z} - h(\mathbf{y}, \hat{\mathcal{G}}))^t \Sigma^{-1} (\mathbf{z} - h(\mathbf{y}, \hat{\mathcal{G}})). \quad (5.5)$$

Note that $\hat{\mathcal{G}} = \mathcal{G}$ in the absence of an attack while $\hat{\mathcal{G}} = \bar{\mathcal{G}}$ in the presence of an attack. In practice, nonlinear WLS estimation is implemented numerically [4].

Under the DC model (5.2), the WLS state estimator is a linear estimator with

a closed form expression

$$\begin{aligned}\hat{\mathbf{x}} &= \arg \min_{\mathbf{y}} (\mathbf{z} - \hat{H}\mathbf{y})^t \Sigma^{-1} (\mathbf{z} - \hat{H}\mathbf{y}) \\ &= (\hat{H}^t \Sigma^{-1} \hat{H})^{-1} \hat{H}^t \Sigma^{-1} \mathbf{z},\end{aligned}\tag{5.6}$$

where \hat{H} is the measurement matrix for $\hat{\mathcal{G}}$. The linear estimator is sometimes used as part of an iterative procedure to obtain the nonlinear WLS solution.

The residue error is often used at the control center for bad data detection [4]. In the so-called $J(\hat{\mathbf{x}})$ test [5], the weighted least squares error

$$J(\hat{\mathbf{x}}) = (\mathbf{z} - h(\hat{\mathbf{x}}, \hat{\mathcal{G}}))^t \Sigma^{-1} (\mathbf{z} - h(\hat{\mathbf{x}}, \hat{\mathcal{G}}))$$

is used in a threshold test:

$$\begin{cases} \text{bad data} & \text{if } J(\hat{\mathbf{x}}) > \tau, \\ \text{good data} & \text{if } J(\hat{\mathbf{x}}) \leq \tau, \end{cases}\tag{5.7}$$

where τ is the detection threshold, and it is determined to satisfy a certain false alarm constraint α .

We define that an attack is *undetectable* if its detection probability is as low as the false alarm rate of the detector. We assume that the $J(\hat{\mathbf{x}})$ test is used as the bad data detector.

Definition 5.2.1. *An attack \mathbf{a} to modify \mathcal{G} to $\bar{\mathcal{G}}$ is said to be undetectable if, for any true state \mathbf{x} , the $J(\hat{\mathbf{x}})$ -test with any false alarm constraint detects the attack with the detection probability no greater than its false alarm rate.*

In the absence of noise, the only source of bad data is, presumably, an attack. In this case, the probabilistic statement of undetectability becomes a deterministic

one. A data attack $(\mathbf{z} + a(\mathbf{z}), \bar{\mathbf{s}})$ that modifies the topology from \mathcal{G} to $\bar{\mathcal{G}}$ is undetectable if for every noiseless measurement \mathbf{z} , there exists a state vector $\bar{\mathbf{x}}$ such that $\mathbf{z} + a(\mathbf{z}) = h(\bar{\mathbf{x}}, \bar{\mathcal{G}})$. Unfortunately, such a nonlinear condition is difficult to check.

Under the DC model, however, the undetectability condition has a simple algebraic form. Let (\mathbf{s}, \mathbf{z}) be the input to GSE and H is the measurement matrix for the topology corresponding to \mathbf{s} . In the presence of an attack, GSE receives $(\bar{\mathbf{s}}, \bar{\mathbf{z}})$ instead of (\mathbf{s}, \mathbf{z}) , and \bar{H} —the measurement matrix for the target topology $\bar{\mathcal{G}}$ —replaces H . In the absence of noise, the $J(\hat{\mathbf{x}})$ -detector is equivalent to checking whether the received meter data is in the column space of the valid measurement matrix. Thus, the equivalent undetectable topology attack can be defined by the following easily checkable form:

Definition 5.2.2. *An attack to modify \mathcal{G} to $\bar{\mathcal{G}}$ with the attack vector \mathbf{a} is said to be undetectable if*

$$\mathbf{z} + \mathbf{a}(\mathbf{z}) \in \text{Col}(\bar{H}), \quad \forall \mathbf{z} \in \text{Col}(H), \quad (5.8)$$

where H and \bar{H} are the measurement matrices for \mathcal{G} and $\bar{\mathcal{G}}$ respectively, and $\text{Col}(H)$ is the column space of H and $\text{Col}(\bar{H})$ the column space of \bar{H} .

5.3 Topology Attack with Global Information

We assume the DC model (5.2) and present the result for the existence of undetectable topology attacks.

5.3.1 Condition for an Undetectable Attack

We first derive a necessary and sufficient algebraic condition for existence of an undetectable attack that modifies \mathcal{G} to $\bar{\mathcal{G}}$ with the subspace \mathcal{A} of feasible attack vectors. To motivate the general result, consider first the noiseless case.

Noiseless Measurement Case

Suppose there is an undetectable attack \mathbf{a} with $\mathbf{a}(\mathbf{z}) \in \mathcal{A}$, $\forall \mathbf{z} \in \text{Col}(H)$. Then, undetectability implies that $\mathbf{z} + \mathbf{a}(\mathbf{z}) \in \text{Col}(\bar{H})$, $\forall \mathbf{z} \in \text{Col}(H)$, and thus, $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$.[‡]

Now suppose $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$. There exists a basis $\{\mathbf{c}_1, \dots, \mathbf{c}_p, \mathbf{d}_1, \dots, \mathbf{d}_q\}$ of $\text{Col}(\bar{H}, \mathcal{A})$ such that $\{\mathbf{c}_1, \dots, \mathbf{c}_p\}$ is a subset of columns of \bar{H} and $\{\mathbf{d}_1, \dots, \mathbf{d}_q\}$ is a set of linearly independent vectors in \mathcal{A} . For any $\mathbf{z} \in \text{Col}(H)$, since $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$, there exist unique $(\alpha_i)_{i=1}^p \in \mathbb{R}^p$ and $(\beta_j)_{j=1}^q$ such that $\mathbf{z} = \sum_{i=1}^p \alpha_i \mathbf{c}_i + \sum_{j=1}^q \beta_j \mathbf{d}_j$. If we set $\mathbf{a}(\mathbf{z}) = -\sum_{j=1}^q \beta_j \mathbf{d}_j$, $\mathbf{z} + \mathbf{a}(\mathbf{z}) = \sum_{i=1}^p \alpha_i \mathbf{c}_i \in \text{Col}(\bar{H})$. In addition, $\mathbf{a}(\mathbf{z}) \in \mathcal{A}$ for all \mathbf{z} . Hence, there exists an undetectable attack with the subspace \mathcal{A} of feasible attack vectors.

The above arguments lead to the following theorem.

Theorem 5.3.1. *There exists an undetectable attack to modify \mathcal{G} to $\bar{\mathcal{G}}$ with the subspace \mathcal{A} of feasible attack vectors if and only if $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$.*

[‡] $\text{Col}(\bar{H}, \mathcal{A})$ denotes the space spanned by the columns of \bar{H} and a basis of \mathcal{A} .

Noisy Measurement Case

The following theorem states that the algebraic condition in Theorem 5.3.1 can also be used in the noisy measurement case.

Theorem 5.3.2. *There exists an undetectable attack to modify \mathcal{G} to $\bar{\mathcal{G}}$ with the subspace \mathcal{A} of feasible attack vectors if and only if $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$.*

In addition, if an attack \mathbf{a} is such that $\text{Col}(H) \not\subset \text{Col}(\bar{H}, \mathcal{A})$, then for almost every[§] $\mathbf{x} \in \mathbb{R}^n$, when \mathbf{x} is the true state, the detection probability for the attack approaches 1 as the noise variances uniformly decrease to 0 (i.e., $\max_i(\Sigma_{ii})$, where Σ_{ii} is the (i, i) entry of Σ , decays to 0).

Proof: See Section 5.8.

Note that when the algebraic condition is not met, the attack can be detected with high probability if the noise variances are sufficiently small. With this algebraic condition, we can check whether the adversary can launch an undetectable attack with \mathcal{A} for the target $\bar{\mathcal{G}}$. The condition will be used in Section 5.5 to construct a meter protection strategy to disable undetectable attacks for any target topology.

By finding the smallest dimension of \mathcal{A} satisfying the condition, we can also characterize the minimum cost of undetectable attacks for $\bar{\mathcal{G}}$; in the adversary's point of view, a smaller dimension of \mathcal{A} is preferred, because increasing the dimension of \mathcal{A} necessitates compromising more RTUs or communication devices. In the

[§]This means “for all $\mathbf{x} \in \mathbb{R}^n \setminus \mathcal{S}$, for some $\mathcal{S} \subset \mathbb{R}^n$ with a zero Lebesgue measure”.

following section, we present an undetectable attack requiring a small number of data modifications and prove its optimality for a class of targets by utilizing the algebraic condition.

5.3.2 State-preserving Attack

This section presents a simple undetectable attack, referred to as *state-preserving attack*. As the name suggests, the attack intentionally preserves the state in order to have a sparse attack vector. We again motivate our result by considering first the noiseless case.

Noiseless Measurement Case

Given $\mathbf{z} = H\mathbf{x} \in \text{Col}(H)$, the state-preserving attack sets $\mathbf{a}(\mathbf{z})$ equal to $(\bar{H} - H)\mathbf{x}$. Then, $\mathbf{z} + \mathbf{a}(\mathbf{z}) = \bar{H}\mathbf{x} \in \text{Col}(\bar{H})$; the attack is *undetectable*. Note that the state \mathbf{x} remains the same after the attack. Since H has full column rank, $\mathbf{a}(\mathbf{z})$ can be simply calculated as

$$\mathbf{a}(\mathbf{z}) = (\bar{H} - H)\mathbf{x} = (\bar{H} - H)(H^t H)^{-1} H^t \mathbf{z}. \quad (5.9)$$

For $\mathbf{a}(\mathbf{z})$ above to be a valid attack vector, it is necessary to be a sparse vector constrained by the meters, the data of which can be altered by the adversary.

To see an intuitive reason why $\bar{H}\mathbf{x} - H\mathbf{x}$ is sparse, consider the simple case that a line is removed from the topology while the state is *preserved*. In this case, the

line flows through all the lines, except the removed line, stay the same. Because, the line flow from i to j is determined by (i) (x_i, x_j) and (ii) whether i and j are connected, and for most lines, these two factors remain the same. Hence, only few entries are different between $\bar{H}\mathbf{x}$ and $H\mathbf{x}$. Below, we will show that, for all state $\mathbf{x} \in \mathbb{R}^n$, all entries of $(\bar{H} - H)\mathbf{x}$ are zeros except those associated with the target lines.

As noted in [71], H can be decomposed as $H = MBA^t$, where $M \in \mathbb{R}^{m \times l}$ is the measurement-to-line incidence matrix with $l \triangleq |\mathcal{E}_0|$, $B \in \mathbb{R}^{l \times l}$ is a diagonal matrix with the line susceptances in the diagonal entries, and $A^t \in \mathbb{R}^{l \times n}$ is the line-to-bus incidence matrix. Each column of M (each row of A^t) corresponds to a distinct line in \mathcal{E}_0 . For $1 \leq j \leq l$, if the j th column of M corresponds to $(a, b) \in \mathcal{E}_0$, let $v_j^+ \triangleq a$ and $v_j^- \triangleq b$. Then, M is defined such that $M_{ij} = \pm 1$ if the i th meter (the meter corresponding to the i th row of M) measures (i) the line flow from v_j^+ to v_j^- or (ii) the injection at bus v_j^+ ; otherwise, $M_{ij} = 0$. For A^t , $(A^t)_{ji} = \pm 1$ if $v_j^+ = i$, and the line corresponding to the j th row of A^t (or equivalently the j th column of M) is *connected* in \mathcal{G} ; otherwise, $(A^t)_{ji} = 0$. Note that M and B are independent of the topology, but A^t does depend on \mathcal{G} . Fig. 5.2 provides an example to illustrate the structures of M , B , and A^t . Similarly, \bar{H} is decomposed as $\bar{H} = M\bar{B}\bar{A}^t$.

As illustrated in Fig. 5.2, the entries of $BA^t\mathbf{x} \in \mathbb{R}^{l \times 1}$ correspond to the line flows of all the lines in \mathcal{E}_0 when the state is \mathbf{x} and the topology is \mathcal{G} . Similarly, $B\bar{A}^t\mathbf{x}$ is the vector of line flows when the state is \mathbf{x} and the topology is $\bar{\mathcal{G}}$. Since the states are the same, the k th entry of $BA^t\mathbf{x}$ and that of $B\bar{A}^t\mathbf{x}$ are different only if the corresponding line is connected in one of \mathcal{G} and $\bar{\mathcal{G}}$ while disconnected in the other. Therefore, $(B\bar{A}^t - BA^t)\mathbf{x}$ has all zero entries except the entries corresponding to

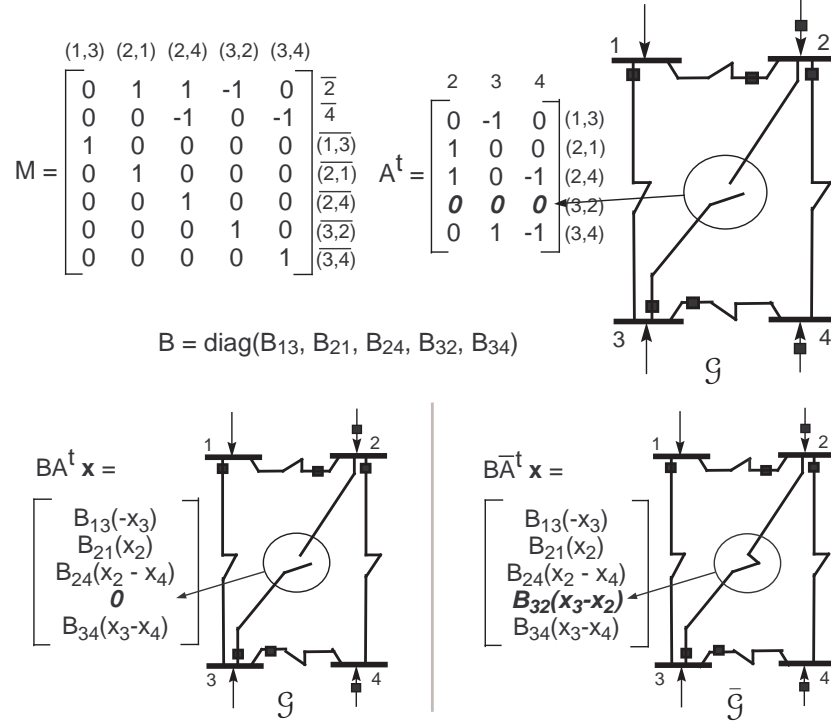


Figure 5.2: The measurement, line, or bus corresponding to each row or column is labeled. Bus 1 is the slack bus. For the rows of M , \bar{i} denotes the injection meter at bus i , and $\overline{(i,j)}$ the meter for the line flow from i to j .

the lines in $\bar{\mathcal{E}} \Delta \mathcal{E}$. Specifically, the entry corresponding to $(i,j) \in \bar{\mathcal{E}} \setminus \mathcal{E}$ assumes $f_{ij}(\mathbf{x}) \triangleq B_{ij}(x_i - x_j)$, and the entry corresponding to $(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}$ assumes $-f_{ij}(\mathbf{x})$. Hence, $(\bar{H} - H)\mathbf{x} = M(B\bar{A}^t - BA^t)\mathbf{x}$ is equal to

$$\sum_{(i,j) \in \bar{\mathcal{E}} \setminus \mathcal{E}} f_{ij}(\mathbf{x}) \mathbf{m}_{(i,j)} - \sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} f_{ij}(\mathbf{x}) \mathbf{m}_{(i,j)} \quad (5.10)$$

where $\mathbf{m}_{(i,j)}$ is the column vector of M corresponding to (i,j) . Note that $\mathbf{m}_{(i,j)}$ is a sparse vector that has nonzero entries only at the rows corresponding to the line flow meters on the line (i,j) and the injection meters at i and j .

From (5.10), for any state $\mathbf{x} \in \mathbb{R}^n$, $(\bar{H} - H)\mathbf{x}$ is a linear combination of elements in $\{\mathbf{m}_{(i,j)} : (i,j) \in \bar{\mathcal{E}} \Delta \mathcal{E}\}$. Hence, the state-preserving attack, which sets $\mathbf{a}(\mathbf{z}) =$

$(\bar{H} - H)\mathbf{x}$, modifies at most the line flow meters on the target lines and the injection meters at the target buses.

We now show in the next two theorems that, under certain conditions, the state-preserving attack has the least cost in the sense that it requires the adversary to modify the smallest number of meter data (*i.e.*, , the smallest dimension for \mathcal{A}).

Theorem 5.3.3. *Assume that (i) the actual and target topologies differ by only one line, *i.e.*, , $|\bar{\mathcal{E}} \Delta \mathcal{E}| = 1$, and (ii) every line in $\bar{\mathcal{E}}$, incident[¶] from or to any target bus with an injection meter, has at least one line flow meter on it. Then, among all undetectable attacks, the state-preserving attack modifies the smallest number of meters, which is the total number of line flow and injection meters located on the target line and target buses.*

Proof: See Section 5.8.

Another scenario that the state-preserving attack has the minimum cost is when the adversary aims to delete lines from the actual topology.

Theorem 5.3.4. *Let \mathcal{G}^* and $\bar{\mathcal{G}}^*$ denote the undirected versions of \mathcal{G} and $\bar{\mathcal{G}}$ respectively. Suppose that the adversary aims to remove lines from \mathcal{G} , *i.e.*, , $\bar{\mathcal{E}} \subsetneq \mathcal{E}$, and the following hold:*

- *Every line in $\bar{\mathcal{E}}$, incident from or to a target bus with an injection meter, has at least one line flow meter on it.*
- *In \mathcal{G}^* , target lines do not form a closed path.*

[¶]A line (i, j) is said to be incident from i and incident to j .

- $\bar{\mathcal{G}}^*$ does not include a tree \mathcal{T} satisfying the following:
 - 1) (number of nodes in \mathcal{T}) ≥ 4 , and
 - 2) every node in \mathcal{T} is a target bus with an injection meter.

Then, among all undetectable attacks, the state-preserving attack modifies the smallest number of meters, which is the total number of line flow and injection meters located on the target lines and target buses.

Proof: *See Section 5.8.*

Roughly speaking, the assumptions in Theorem 5.3.4 hold when target lines are far from each other such that there is no big tree in $\bar{\mathcal{G}}$ consisting solely of target buses.

The main advantage of the state-preserving attack is that by preserving the system state during the attack, the attack can be launched by perturbing only *local* meters around the target lines; hence, only few data entries need to be modified. Theorem 5.3.3 and Theorem 5.3.4 supports the claim by stating the optimality of the state-preserving attack under the mild assumptions. The theorems also imply that the minimum cost of an undetectable attack can be easily characterized if the target topology satisfies the theorem assumptions.

Noisy Measurement Case

Following the intuition behind the state-preserving attack in the noiseless case, we will construct its counterpart for the noisy measurement case. Recall the relation (5.10):

$$(\bar{H} - H)\mathbf{x} = \sum_{(i,j) \in \bar{\mathcal{E}} \setminus \mathcal{E}} f_{ij}(\mathbf{x})\mathbf{m}_{(i,j)} - \sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} f_{ij}(\mathbf{x})\mathbf{m}_{(i,j)}.$$

The above implies that

$$(\bar{H} - H)\mathbf{x} \in \mathcal{M} \triangleq \text{span}\{\mathbf{m}_{(i,j)} : (i,j) \in \bar{\mathcal{E}} \Delta \mathcal{E}\} \quad (5.11)$$

We set $\mathbf{a}(\mathbf{z})$ as a minimizer of the $J(\hat{\mathbf{x}})$ -test statistic^{||}:

$$\mathbf{a}(\mathbf{z}) \triangleq \arg \min_{\mathbf{d} \in \mathcal{M}} \|(\mathbf{z} + \mathbf{d}) - \bar{H}\hat{\mathbf{x}}_{\text{WLS}}[\mathbf{z} + \mathbf{d}]\|_{\Sigma^{-1}}^2 \quad (5.12)$$

where $\hat{\mathbf{x}}_{\text{WLS}}[\mathbf{z} + \mathbf{d}]$ denotes the WLS state estimate when the topology estimate is $\bar{\mathcal{G}}$, and $\mathbf{z} + \mathbf{d}$ is observed at the control center. Note that, since $\mathbf{a}(\mathbf{z}) \in \mathcal{M}$, the attack with \mathbf{a} modifies at most the line flow measurements of the target lines and the injection measurements of the target buses.

Now, suppose that the adversary modifies breaker state measurements such that the topology estimate becomes $\bar{\mathcal{G}}$ and simultaneously modifies the meter data with $\mathbf{a}(\mathbf{z})$. Then, the $J(\hat{\mathbf{x}})$ -test statistic at the control center is upper bounded as

$$\begin{aligned} & \|(\mathbf{z} + \mathbf{a}(\mathbf{z})) - \bar{H}\hat{\mathbf{x}}_{\text{WLS}}[\mathbf{z} + \mathbf{a}(\mathbf{z})]\|_{\Sigma^{-1}}^2 \\ & \leq \|(\bar{H}\mathbf{x} + \mathbf{e}) - \bar{H}\hat{\mathbf{x}}_{\text{WLS}}[\bar{H}\mathbf{x} + \mathbf{e}]\|_{\Sigma^{-1}}^2, \end{aligned}$$

^{||}We use $\|\mathbf{r}\|_{\Sigma^{-1}}^2$ to denote the quadratic form $\mathbf{r}^t \Sigma^{-1} \mathbf{r}$.

because $(\bar{H} - H)\mathbf{x}$ is an element of \mathcal{M} . Note that the right hand side is the $J(\hat{\mathbf{x}})$ -test statistic when the meter data are consistent with the topology estimate $\bar{\mathcal{G}}$. Hence, it has χ_{m-n}^2 distribution, the same as the distribution of the $J(\hat{\mathbf{x}})$ -test statistic under the absence of bad data [5]. This argument leads to the following theorem stating that this attack is undetectable.

Theorem 5.3.5. *The state-preserving attack \mathbf{a} , defined in (5.12), is undetectable.*

Note that $\hat{\mathbf{x}}_{\text{WLS}}[\mathbf{z} + \mathbf{d}]$ in (5.12) is a linear function of $\mathbf{z} + \mathbf{d}$, so $\mathbf{a}(\mathbf{z})$ can be obtained as a linear weighted least squares solution. Specifically, $\mathbf{a}(\mathbf{z})$ has a form of $\mathbf{a}(\mathbf{z}) = D\mathbf{z}$ where $D \in \mathbb{R}^{m \times m}$ depends on \mathcal{G} , $\bar{\mathcal{G}}$, and Σ , but not on \mathbf{z} . Hence, D can be obtained off-line before observing \mathbf{z} .

Note also that the state-preserving attacks in the noiseless and noisy cases modify the same set of meters. In addition, recall that the condition for existence of an undetectable attack is the same for both noiseless and noisy cases. The optimality statements for the state-preserving attack in Theorem 5.3.3 and Theorem 5.3.4 were derived purely based on the condition for undetectability. Hence, the same optimality statements hold for the noisy measurement case, as stated in the following corollary, and the same interpretation can be made.

Corollary 5.3.5.1. *For the noisy measurement DC model, suppose that the condition in Theorem 5.3.3 or the condition in Theorem 5.3.4 hold. Then, among all undetectable attacks, the state-preserving attack modifies the smallest number of meters, which is the total number of line flow and injection meters located on the target lines and target buses.*

5.4 Topology Attack with Local Information

In this section, we consider the more realistic scenario of a weak attacker who does not have the measurement data of the entire network; it only has access to a few meters. The information available to the adversary is local. We also generalize the linear (DC) measurement model to the nonlinear (AC) model. The resulting undetectable attacks, however, are limited to line removal attacks, *i.e.*, the adversary only tries to remove lines from the actual network topology.

We first consider the noiseless measurement case under the DC model. Since we are restricted to line-removal attacks, $\bar{\mathcal{E}}$ is a strict subset of \mathcal{E} . Therefore, recalling (5.10), we have

$$(\bar{H} - H)\mathbf{x} = - \sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} f_{ij}(\mathbf{x}) \mathbf{m}_{(i,j)} \quad (5.13)$$

where $f_{ij}(\mathbf{x})$, as defined in Section 5.3, denotes the line flow from i to j when the line is connected, and the state is \mathbf{x} .

Let z_{ij} denote the measurement of the line flow from i to j . Due to the absence of noise, $z_{ij} = f_{ij}(\mathbf{x}) = -f_{ji}(\mathbf{x}) = -z_{ji}$. With this observation and (5.13), we have

$$(\bar{H} - H)\mathbf{x} = - \sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} z_{ij} \mathbf{m}_{(i,j)} \quad (5.14)$$

Therefore, setting $\mathbf{a}(\mathbf{z}) = (\bar{H} - H)\mathbf{x}$, which is the state-preserving attack, is *equivalent* to setting

$$\mathbf{a}(\mathbf{z}) = - \sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} z_{ij} \mathbf{m}_{(i,j)} \quad (5.15)$$

From (5.15), one can see that adding the above $\mathbf{a}(\mathbf{z})$ to \mathbf{z} is equivalent to the following heuristic described in Fig. 5.3:

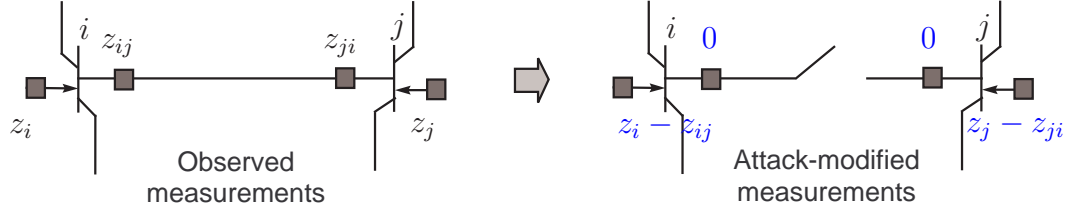


Figure 5.3: Heuristic Operations Around the Target Line (i, j)

1. For every target line (i, j) , subtract z_{ij} and z_{ji} from the injection measurements at i and j respectively.
2. For every target line (i, j) , modify z_{ij} and z_{ji} to 0.

This heuristic simply forces the line flows through the target lines, which are disconnected in $\bar{\mathcal{G}}$, to be zeros, while adjusting the injections at the target buses to satisfy the power balance equations [4]. If a target line (i, j) has only one line flow meter (*e.g.*, z_{ji}), we can use $-z_{ji}$ in the place of z_{ij} . But, if some target line has no line flow meter, this heuristic is not applicable. Note that the heuristic only requires the ability to observe and modify the line flow measurements of the target lines and the injection measurements at the target buses. The adversary can launch it without knowing the topology or network parameters (*i.e.*, \mathbf{H} and $\bar{\mathbf{H}}$ are not necessary). Since the heuristic is equivalent to the state-preserving attack, it is undetectable.

The same heuristic is applicable to the noisy measurements $\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}$. To avoid detection, the adversary can make $\mathbf{a}(\mathbf{z})$ approximate $\bar{\mathbf{H}}\mathbf{x} - \mathbf{H}\mathbf{x}$ such that $\mathbf{z} + \mathbf{a}(\mathbf{z})$ is close to $\bar{\mathbf{H}}\mathbf{x} + \mathbf{e}$. Because $z_{ij} = f_{ij}(\mathbf{x}) + e_{ij}$, z_{ij} is an unbiased estimate of $f_{ij}(\mathbf{x})$. Similarly, $-\sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} z_{ij} \mathbf{m}_{(i,j)}$ is an unbiased estimate of $-\sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} f_{ij}(\mathbf{x}) \mathbf{m}_{(i,j)}$, which is equal to $\bar{\mathbf{H}}\mathbf{x} - \mathbf{H}\mathbf{x}$. Hence, it is reasonable to set

$\mathbf{a}(\mathbf{z}) = -\sum_{(i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}} z_{ij} \mathbf{m}_{(i,j)}$ even in the noisy measurement case.

The same idea is applicable to the AC power flow model with the nonlinear state estimator. Suppose that \mathbf{z} is the real power measurement from the AC power flow model: $\mathbf{z} = h(\mathbf{x}) + \mathbf{e}$, where \mathbf{x} is the vector of the voltage phasors at all buses, and h is the nonlinear measurement function for \mathcal{G} . Let \bar{h} denote the measurement function for $\bar{\mathcal{G}}$. If $\mathbf{a}(\mathbf{z})$ is equal to $\bar{h}(\mathbf{x}) - h(\mathbf{x})$,

$$\bar{\mathbf{z}} = (h(\mathbf{x}) + \mathbf{e}) + \mathbf{a}(\mathbf{z}) = \bar{h}(\mathbf{x}) + \mathbf{e}, \quad (5.16)$$

which is consistent with $\bar{\mathcal{G}}$, so the attack cannot be detected. We will show that the attack vector of the heuristic approximates $\bar{h}(\mathbf{x}) - h(\mathbf{x})$.

For simplicity, assume that the attacker aims at removing a single line (i, j) from \mathcal{G} . Then, $h(\mathbf{x})$ and $\bar{h}(\mathbf{x})$ are different only in the entries corresponding to the injections at i and j and the line flows through (i, j) . Specifically, $\bar{h}(\mathbf{x}) - h(\mathbf{x})$ has all zero entries except $-h_{ij}(\mathbf{x})$ at the rows corresponding to the injection at i and the line flow from i to j , and $-h_{ji}(\mathbf{x})$ at the rows corresponding to the injection at j and the line flow from j to i , where $h_{ij}(\mathbf{x})$ denotes the entry of $h(\mathbf{x})$ corresponding to the line flow from i to j . Since $z_{ij} = h_{ij}(\mathbf{x}) + e_{ij}$ and $z_{ji} = h_{ji}(\mathbf{x}) + e_{ji}$, z_{ij} and z_{ji} can be considered as unbiased estimates of $h_{ij}(\mathbf{x})$ and $h_{ji}(\mathbf{x})$ respectively. Hence, the attacker can use z_{ij} and z_{ji} to construct an unbiased estimate of $\bar{h}(\mathbf{x}) - h(\mathbf{x})$. Adding this estimate to \mathbf{z} is equivalent to the heuristic operation of Fig. 5.3, which subtracts z_{ij} and z_{ji} from z_i and z_j respectively, and sets z_{ij} and z_{ji} to zeros. The same argument holds for the reactive measurement part and multiple-line removal attacks. In practice, the heuristic attack should be executed twice separately, once for real measurements and second for reactive measurements. In Section 5.6, numerical simulations demonstrate that the heuristic attack on the AC power flow

model with the nonlinear state estimation has a very low detection probability.

5.5 Countermeasure for Topology Attacks

In this section, we consider countermeasures that prevent attacks by a strong adversary with global information. In particular, we assume that a subset of meters can be secured so that the adversary cannot modify data from these meters. In practice, this can be accomplished by implementing more sophisticated authentication protocols. We present a so-called cover-up protection that identifies the set of meters that need to be secured.

The algebraic condition in Theorems 5.3.1-5.3.2 provides a way to check whether a set of adversary-controlled meters is enough to launch an undetectable attack. Restating the algebraic condition, there exists an undetectable attack with the subspace \mathcal{A} of feasible attack vectors, if and only if $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$ for some $\bar{\mathcal{G}}$ (different from \mathcal{G}).

Let \mathcal{J}_S denote the set of indices for the entries of \mathbf{z} corresponding to the protected meters. Then, \mathcal{A} is $\{\mathbf{c} \in \mathbb{R}^m : c_i = 0, i \in \mathcal{J}_S\}$. The objective of the control center is to make any undetectable attack infeasible while minimizing the cost of protection (*i.e.*, minimizing $|\mathcal{J}_S|$ or equivalently, maximizing the dimension of \mathcal{A}).

To achieve the protection goal, \mathcal{A} should satisfy that for any target topology $\bar{\mathcal{G}}$, $\text{Col}(H) \not\subset \text{Col}(\bar{H}, \mathcal{A})$. However, finding such \mathcal{A} by checking the conditions for all possible targets is computationally infeasible. To avoid computational burden,

the following theorem gives a simple graph-theoretical strategy.

Theorem 5.5.1 (Cover-up strategy). *Let $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{E}}_0$ denote the undirected counterparts of \mathcal{E} and \mathcal{E}_0 respectively. For $i \in \mathcal{V}$, let \mathcal{L}_i denote the set of edges in $(\mathcal{V}, \tilde{\mathcal{E}}_0)$ that are incident to i .*

Suppose there is a spanning tree $\mathcal{T} = (\mathcal{V}, \mathcal{E}_{\mathcal{T}})$ of $(\mathcal{V}, \tilde{\mathcal{E}})$ (the current topology) and a vertex subset \mathcal{B} ($\mathcal{B} \subset \mathcal{V}$) that satisfies

$$\mathcal{E}_{\mathcal{T}} \cup (\cup_{b \in \mathcal{B}} \mathcal{L}_b) = \tilde{\mathcal{E}}_0. \quad (5.17)$$

Then, if we protect (i) one line flow meter for each line in $\mathcal{E}_{\mathcal{T}}$ and (ii) the injection meters at all buses in \mathcal{B} , an undetectable attack does not exist for any target topology.

Proof: See Section 5.8.

The condition (5.17) means that the edges of \mathcal{T} and the edges incident to vertices in \mathcal{B} can cover all the lines (both connected and disconnected) of the grid. One can easily find such \mathcal{T} and \mathcal{B} using available graph algorithms.

Fig. 5.4 describes a cover-up strategy for IEEE 14-bus system. The strategy used the spanning tree \mathcal{T} marked by red dash lines, and $\mathcal{B} = \{1, 4, 13\}$. The unprotected meters and protected meters are marked by black rectangles and blue circles respectively. In this example, the strategy requires protection of 30% of meters. In addition, numerically checking the algebraic condition showed that if the control center removes *any* of the protections, the grid becomes vulnerable to

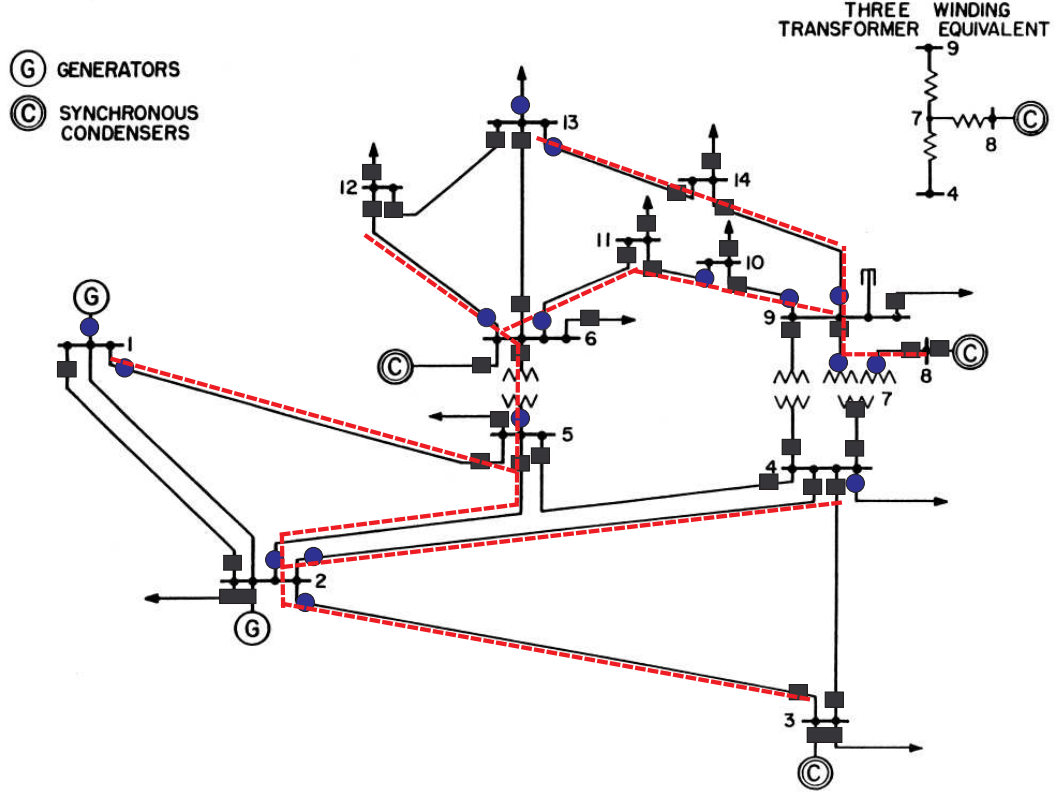


Figure 5.4: Rectangles (or circles) on buses and lines represent injection meters and line flow meters respectively. We assume that $\mathcal{E} = \mathcal{E}_0$. The attacker may attempt to remove lines from \mathcal{G} .

undetectable topology attacks. This suggests that the strategy does not require protection of an excessive number of meters. For IEEE 118-bus system, a cover-up strategy required protection of 31% of meters.

The cover-up strategy also prevents undetectable state attacks [7]. It follows from Theorem 1 in [8], which states that an undetectable state attack does not exist if and only if the secure meters, protected by the control center, make the system state observable. Because the strategy protects one line meter for each line in the spanning tree \mathcal{T} , the system state is always observable with the protected meters [71].

5.6 Numerical Results

We first present practical uses of the algebraic condition for undetectable attacks. Then, we test the proposed attacks with IEEE 14-bus and 118-bus systems, and present their effect on real-time LMPs.

5.6.1 Application of Undetectability Condition

In Section 5.3.1, the necessary and sufficient algebraic condition is given to check whether an adversary can launch an undetectable attack for a target $\bar{\mathcal{G}}$ with a subspace \mathcal{A} of feasible attack vectors. Here, we provide examples of how the condition can be used by both attackers and the control center.

Suppose that an attacker with global information aims to remove a specific set of lines from the topology. In Section 5.3.1, we have shown that the state-preserving attack requires the smallest dimension of \mathcal{A} among undetectable attacks under mild conditions. If the conditions are met and the attacker can perform the necessary meter modifications, the state-preserving attack can be launched with the guaranteed optimality. However, if the attacker cannot perform some meter modification required by the state-preserving attack, it should search for an undetectable alternative with a reasonably small dimension for \mathcal{A} . The algebraic condition can be used to find such an alternative^{**}. For instance, for a line-removal

^{**}One heuristic way to find an alternative, which we employed, is to begin with a large set \mathcal{K} of adversary-controlled meters that satisfies the algebraic condition and the constraint (*e.g.*, exclude a certain injection meter) and remove meters from \mathcal{K} one by one such that after each removal of a meter, \mathcal{K} still satisfies the algebraic condition. If no more meter can be removed, we take \mathcal{K} as an alternative. The final set depends on the initial \mathcal{K} and the sequence of removed elements.

Table 5.1: The adversary-controlled meters for the attacks to remove lines (2, 4) and (12, 13): $i \rightarrow j$ denotes the meter for the line flow from bus i to bus j . i denotes the injection meter at bus i .

	Adversary-controlled meters
State-preserving attack	$2 \rightarrow 4, 4 \rightarrow 2, 12 \rightarrow 13,$ $13 \rightarrow 12, 2, 4, 12, 13$
Alternative 1 (not modifying 12)	$2 \rightarrow 4, 4 \rightarrow 2, 12 \rightarrow 13, 13 \rightarrow 12,$ $6 \rightarrow 12, 12 \rightarrow 6, 2, 4, 6, 13$
Alternative 2 (not modifying 4)	$2 \rightarrow 4, 4 \rightarrow 2, 12 \rightarrow 13, 13 \rightarrow 12, 2 \rightarrow 3,$ $3 \rightarrow 2, 3 \rightarrow 4, 4 \rightarrow 3, 2, 3, 12, 13$

attack on the IEEE 14-bus network in Fig. 5.4, Table 5.1 shows some alternatives to the state-preserving attack when the attacker cannot modify some injection meter.

When the set of adversary-controlled meters is fixed, the algebraic condition can be exploited to find the target topologies, for which the attacker can launch undetectable attacks. For instance, in the IEEE 14-bus network in Fig. 5.4, assume that the attacker can modify the data from the injection meters at 11, 12, and 14, and all the line flow meters on (6, 12), (6, 11), (10, 11), (9, 10), (9, 14), and (13, 14). Then, numerically checking the algebraic condition show that the attacker cannot launch an undetectable attack for any target. However, if the attacker can additionally control the line flow meters on (12, 13), it can launch an undetectable attack to remove any set of lines listed in Table 5.2 from the current topology.

The control center can also utilize the algebraic condition to decide which meters to put more security measures on. For instance, in the IEEE 14-bus network,

One can try this procedure multiple times with different initial \mathcal{K} s and removal sequences, and pick the one with the smallest size.

Table 5.2: The Sets of Lines Undetectable Attacks Can Remove

$ \bar{\mathcal{E}}\Delta\mathcal{E} $	$\bar{\mathcal{E}}\Delta\mathcal{E}$ (lines to be removed by the attack)
1	$\{(6, 12)\}, \{(6, 11)\}, \{(10, 11)\}, \{(9, 10)\},$ $\{(9, 14)\}, \{(13, 14)\}, \{(12, 13)\}$
2	$\{(10, 11), (13, 14)\}, \{(9, 14), (12, 13)\}, \{(9, 10), (13, 14)\},$ $\{(6, 12), (13, 14)\}, \{(6, 12), (10, 11)\}, \{(6, 12), (9, 10)\},$ $\{(6, 11), (12, 13)\}, \{(6, 11), (9, 14)\}$
3	$\{(6, 11), (9, 14), (12, 13)\}, \{(6, 12), (9, 10), (13, 14)\},$ $\{(6, 12), (10, 11), (13, 14)\}$

suppose that the control center protects all the injection meter. In the worst case, the attacker may be able to modify all the line flow measurements. In this case, checking the algebraic condition shows that the attacker can launch an undetectable line-removal attack for any target topology, as long as the system with the target topology is observable. However, checking the algebraic condition also shows that if the control center can additionally protect any line flow meter, an undetectable attack does not exist for any target. Therefore, it is worthwhile for the control center to make an effort to secure one more line flow meter.

5.6.2 Undetectability and Effects on Real-time LMP

We tested the state-preserving attack with global information and the heuristic with local information on IEEE 14-bus and IEEE 118-bus system, and investigated their effect on real-time LMPs. The AC power flow model and nonlinear state estimation were used to emulate the real-world power grid.

For simulations, we first assigned the line capacities, generation limits, and estimated loads, and obtained the day-ahead dispatch. Then, we modeled the voltage magnitudes and phases of buses as Gaussian random variables centered at the system state for the day-ahead dispatch, with small variances. In each Monte Carlo run, we generated a state vector from the distribution and used the nonlinear AC power flow model^{††} with Gaussian measurement noise to generate the noisy measurements. The attacker observed the noisy measurements, added the corresponding attack vector to them, and passed the corrupt measurements to the control center. The control center employed the nonlinear state estimator to obtain the residue and performed the $J(\hat{\mathbf{x}})$ -test with the residue. If $J(\hat{\mathbf{x}})$ -test failed to detect the attack, the real-time LMPs were calculated based on the state estimate.

In simulations, we assumed that the attacker aims to remove a single line from the topology. Fig. 5.5 presents the detection probability of the proposed attacks on IEEE 14-bus system, for different target lines. The attacks on most target lines succeeded with low detection probabilities, close to the false alarm constraint 0.1. Table 5.3 shows the detection probability averaged over all possible single-line removal attacks. In both IEEE 14-bus and 118-bus systems, the proposed attacks were hardly detected. In most cases, detection probabilities were as low as the false alarm rates. The performance of the heuristic was remarkably good, considering that it only requires to observe and control few local data.

We also examined the absolute perturbation of the real-time LMPs (see [17])

^{††}In simulations, we have reactive measurements, which were not considered in our analysis of the state-preserving attack. We simply applied the same analysis for the reactive components of the linearized decoupled model [4] and derived the reactive counterpart of the state-preserving attack.

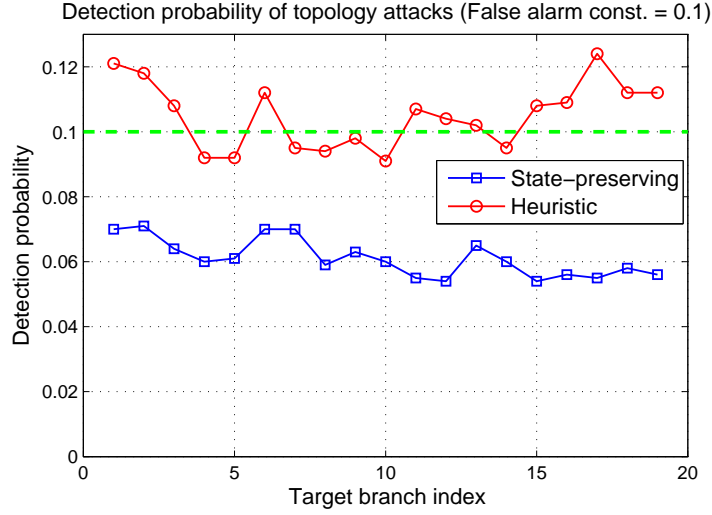


Figure 5.5: Detection Probability of Single-line Attack: the x-axis is for the index of the target line. Measurement noise standard deviation is 0.5 p.u., and 1000 Monte Carlo runs are used.

Table 5.3: Average Detection Probabilities of Single-line Attacks: 1000 Monte Carlo runs are used. The false alarm constraint of the bad data detector is set as α in the table.

	14-bus ($\alpha = 0.1$)	14-bus ($\alpha = 0.01$)	118-bus ($\alpha = 0.1$)	118-bus ($\alpha = 0.01$)
state-preserving	0.061	0.009	0.075	0.005
heuristic	0.105	0.019	0.095	0.009

for real-time LMP). The parameters in the real-time LMP calculation include the estimated set of congested lines and the shift-factor matrix; both depend on the topology estimate. Hence, we expect that topology attacks would disturb the real-time LMP calculation. In our simulations, both the state-preserving attack and the heuristic perturbed the real-time LMPs by 10% on average for IEEE 14-bus system and 3.3% for IEEE 118-bus system. In the 118-bus system, attacks on some target lines had effects on only the buses near the target lines, so the average perturbation was lower than the 14-bus case.

5.7 Conclusion

In this chapter, we have considered undetectable malicious data attack aimed at creating a false topology at the control center. We obtain a necessary and sufficient condition for an attack launched by a strong attacker to be undetectable. We also present a class of undetectable line removal attacks that can be launched by weak attackers with only local information. Finally, we present a countermeasure against strong attackers by protecting a subset of meters.

Some of the results presented in this chapter are obtained under strong conditions. Here, we mention several of such limitations as pointers for further study. First, the DC model assumed in Section 5.3 makes the results valid only near the operating point. It has been demonstrated in [9] that the DC model tends to exaggerate the effect of state attacks, and the nonlinear state estimator has the ability to significantly reduce the attacks' impact on the state estimate. Obtaining conditions for undetectable topology attacks under the AC model is of considerable interest.

Second, we have focused mostly on state-preserving topology attacks. Even though such attacks are optimal under certain scenarios, to understand the full implication of topology attacks, it is necessary to consider attacks that affect both topology and states.

Finally, we consider only one particular form of countermeasure, namely implementing authentication at a subset of meters. Other mechanisms should be studied, including one with more sophisticated bad data detection and those tak-

ing into accounts of system dynamics.

5.8 Proofs

5.8.1 Proof of Theorem 5.3.2

The *if* statement can be proved by constructing an undetectable attack following the arguments used to prove Theorem 5.3.1 and Theorem 5.3.5. Due to the space limit, we only provide the proof of the *only if* statement.

Let \mathbf{a} be any attack with $\text{Col}(H) \not\subseteq \text{Col}(\bar{H}, \mathcal{U})$ where $\mathcal{U} \triangleq \{\mathbf{u}_1, \dots, \mathbf{u}_K\}$ denotes the basis of \mathcal{A} consisting of unit vectors in \mathbb{R}^m and $U \in \mathbb{R}^{m \times K}$ is the matrix having the vectors in \mathcal{U} as its columns. Without loss of generality, we assume that the columns of \bar{H} and the unit vectors in \mathcal{U} are linearly independent; if not, we can just work with a smaller set of \mathcal{U} satisfying the independence condition.

Because $\text{Col}(H) \not\subseteq \text{Col}(\bar{H}, \mathcal{U})$, $\text{Col}(H) \cap \text{Col}(\bar{H}, \mathcal{U})$ is a subspace of $\text{Col}(H)$ with a strictly smaller dimension. Hence, $\mathcal{S} \triangleq \{\mathbf{x} \in \mathbb{R}^n : H\mathbf{x} \in \text{Col}(H) \cap \text{Col}(\bar{H}, \mathcal{U})\}$ has the dimension less than n and thus a zero Lebesgue measure in \mathbb{R}^n . Let \mathbf{x} be an arbitrary element of $\mathbb{R}^n \setminus \mathcal{S}$. Then, $\mathbf{y} \triangleq H\mathbf{x} \notin \text{Col}(\bar{H}, \mathcal{U})$. When \mathbf{x} is the true state, $\mathbf{z} = \mathbf{y} + \mathbf{e}$, and the $J(\hat{\mathbf{x}})$ -test statistic for \mathbf{a} is

$$J = \|W(\mathbf{y} + \mathbf{e} + \mathbf{a}(\mathbf{y} + \mathbf{e}))\|_{\Sigma^{-1}}$$

where $W = I - \bar{H}(\bar{H}^t \Sigma^{-1} \bar{H})^{-1} \bar{H}^t \Sigma^{-1}$. Since $\mathbf{a}(\mathbf{z}) \in \text{Col}(\mathcal{U})$ for all \mathbf{z} , J is lower

bounded by

$$L \triangleq \min_{(a_k)_{k=1}^K} \|W(\mathbf{y} + \mathbf{e} + \sum_{k=1}^K a_k \mathbf{u}_k)\|_{\Sigma^{-1}}.$$

The minimization in L is achieved by the linear WLS solution, and one can show that $L = (\hat{W}(\mathbf{y} + \mathbf{e}))^t \Sigma^{-1} \hat{W}(\mathbf{y} + \mathbf{e})$ where $\hat{W} \triangleq W - (WU)[(WU)^t \Sigma^{-1} (WU)]^{-1} (WU)^t \Sigma^{-1} W$. W and \hat{W} are idempotent and $\Sigma^{-1} W$ is symmetric. Using these properties, one may derive that

$$L = (\Sigma^{-\frac{1}{2}}(\mathbf{y} + \mathbf{e}))^t \Sigma^{\frac{1}{2}} \hat{W}^t \Sigma^{-\frac{1}{2}} (\Sigma^{-\frac{1}{2}}(\mathbf{y} + \mathbf{e})).$$

The above quadratic form has the following properties: (i) $\Sigma^{\frac{1}{2}} \hat{W}^t \Sigma^{-\frac{1}{2}}$ is idempotent and symmetric, (ii) $\Sigma^{-\frac{1}{2}}(\mathbf{y} + \mathbf{e}) \sim \mathcal{N}(\Sigma^{-\frac{1}{2}} \mathbf{y}, I_m)$, and (iii) $\text{rank}(\Sigma^{\frac{1}{2}} \hat{W}^t \Sigma^{-\frac{1}{2}}) = m - n - K$. With these three properties, Theorem B.33 and Theorem 1.3.3 in [80] imply that L has the noncentral chi-squared distribution with the $(m - n - K)$ degree of freedom and the noncentral parameter $\lambda \triangleq (\hat{W} \mathbf{y})^t \Sigma^{-1} (\hat{W} \mathbf{y})$.

It can be shown that $\mathbf{y} \notin \text{Col}(\bar{H}, \mathcal{U})$ implies $\hat{W} \mathbf{y} \neq \mathbf{0}$. Hence, if the diagonal entries of Σ (denoted by σ_{ii}^2 , $1 \leq i \leq m$) uniformly decrease to 0, then $\lambda = \sum_{i=1}^m \sigma_{ii}^{-2} (\hat{W} \mathbf{y})_i^2$ grows to infinity. Suppose that the $J(\hat{\mathbf{x}})$ -test uses a threshold τ . The detection probability of the attack is $\Pr(J > \tau)$, and it is lower bounded by $\Pr(L > \tau)$. And, $\Pr(L > \tau)$ approaches 1 as the noncentral parameter λ grows to infinity. Therefore, if the diagonal entries of Σ (*i.e.*, , noise variances) uniformly decreases to 0, then λ grows to infinity and $\Pr(J > \tau)$ approaches 1. Hence, the only if statement and the additional statement are proved.

5.8.2 Proof of Theorem 5.3.3

Let $\bar{\mathcal{E}} \triangle \mathcal{E} = \{(a, b)\}$. We prove the statement for the case that the attack removes (a, b) , and there are two line flow meters on (a, b) (one for each direction) and injection meters at both a and b . For the line addition attack and other meter availabilities, the similar argument can be made.

Suppose there exists an undetectable attack with \mathcal{A} , and let $\mathcal{U} = \{\mathbf{u}_1, \dots, \mathbf{u}_K\}$ denote the basis of \mathcal{A} consisting of unit vectors in \mathbb{R}^m . Theorem 5.3.1 implies $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{A})$. It can be easily verified that $\mathbf{m}_{(a,b)} \in \text{Col}(\bar{H}, \mathcal{A})$, and this implies $\mathbf{m}_{(a,b)} = \bar{H}\mathbf{x} + \sum_{k=1}^K \alpha_k \mathbf{u}_k$ for some $\mathbf{x} \in \mathbb{R}^n$ and $(\alpha_k)_{k=1}^K \in \mathbb{R}^K$. Then, $\bar{\mathbf{m}} \triangleq \mathbf{m}_{(a,b)} - \sum_{k=1}^K \alpha_k \mathbf{u}_k \in \text{Col}(\bar{H})$.

Let \bar{m}^{ij} (\bar{m}^i) denote the row entry of $\bar{\mathbf{m}}$ corresponding to the line flow from i to j (the injection at i) and $\mathbf{u}_{(i,j)}$ ($\mathbf{u}_{(i)}$) denote the m -dimensional unit vector with 1 at the row corresponding to the line flow from i to j (the injection at i). Physically, $\bar{\mathbf{m}} \in \text{Col}(\bar{H})$ means that $\bar{\mathbf{m}}$ is a vector of meter data consistent with the topology $\bar{\mathcal{G}}$. It implies that (i) \bar{m}^{ab} and \bar{m}^{ba} are zeros, since (a, b) is disconnected in $\bar{\mathcal{G}}$, and (ii) the Kirchhoff's current laws (KCL) should hold at bus a and b in $\bar{\mathcal{G}}$, *i.e.*, the sum of all outgoing line flows from a should be equal to the injection amount at a . Using the special structure of $\mathbf{m}_{(a,b)}$ and $\bar{\mathbf{m}}$, the following can be proved. From (i), one can prove that $\mathbf{u}_{(a,b)}, \mathbf{u}_{(b,a)} \in \mathcal{U}$. From (ii), one can show that \mathcal{U} should include $\mathbf{u}_{(a)}$ or some $\mathbf{u}_{(a,k)}$ (or $\mathbf{u}_{(k,a)}$) with a and k connected in \mathcal{G} . Similarly, \mathcal{U} should include $\mathbf{u}_{(b)}$ or some $\mathbf{u}_{(b,l)}$ (or $\mathbf{u}_{(l,b)}$) with b and l connected in \mathcal{G} . Hence, $|\mathcal{U}|$ is no less than the total number of meters located on the target line (a, b) and the target buses a and b .

5.8.3 Proof of Theorem 5.3.4

Suppose \mathbf{a} is an undetectable attack with \mathcal{A} for the target topology $\bar{\mathcal{G}}$ satisfying the theorem conditions. Let $\mathcal{U} = \{\mathbf{u}_1, \dots, \mathbf{u}_K\}$ be the basis of \mathcal{A} consisting of unit vectors in \mathbb{R}^m , and $\mathcal{J} \subset \mathcal{V}$ denote the set of target buses with injection meters. For ease of presentation, we assume that each target line (i, j) has two line flow meters, one for each direction. For other meter availabilities, the similar argument can be made.

Theorem 5.3.1 implies that $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{U})$. It can be easily shown that if the target lines do not form a closed path in \mathcal{G} , then $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{U})$ implies that $\mathbf{m}_{(i,j)} \in \text{Col}(\bar{H}, \mathcal{U})$ for all target lines $(i, j) \in \mathcal{E} \setminus \bar{\mathcal{E}}$.

$\mathbf{m}_{(i,j)} \in \text{Col}(\bar{H}, \mathcal{U})$ means that it is possible to find a linear combination of vectors in \mathcal{U} , $\sum_{k=1}^K \alpha_k \mathbf{u}_k$, such that $\bar{\mathbf{m}}_{(i,j)} \triangleq \mathbf{m}_{(i,j)} + \sum_{k=1}^K \alpha_k \mathbf{u}_k \in \text{Col}(\bar{H})$. $\bar{\mathbf{m}}_{(i,j)} \in \text{Col}(\bar{H})$ implies that (i) the row entries of $\bar{\mathbf{m}}_{(i,j)}$ corresponding to the line flows of the disconnected lines in $\bar{\mathcal{G}}$ are zeros, and (ii) the entries of $\bar{\mathbf{m}}_{(i,j)}$ satisfy KCLs at all buses in $\bar{\mathcal{G}}$.

For each $(i, j) \in \mathcal{E} \setminus \bar{\mathcal{E}}$, since (i, j) is disconnected in $\bar{\mathcal{G}}$, $\bar{m}_{(i,j)}^{ij} = \bar{m}_{(i,j)}^{ji} = 0$. On the other hand, $m_{(i,j)}^{ij} = 1$ and $m_{(i,j)}^{ji} = -1$. Hence, \mathcal{U} should include $\mathbf{u}_{(i,j)}$ and $\mathbf{u}_{(j,i)}$. Therefore, \mathcal{U} should contain $\{\mathbf{u}_{(i,j)}, \mathbf{u}_{(j,i)} : (i, j) \in \mathcal{E} \setminus \bar{\mathcal{E}}\}$.

For each $i \in \mathcal{J}$, the assumptions imply that each line adjacent to i in $\bar{\mathcal{G}}$ has at least one line flow meter. We let \mathbf{n}_i denote the set of the line flow meters on the lines incident to i in $\bar{\mathcal{G}}$, and $\mathbf{m}_{(i,j)}^{\mathbf{n}_i}$ denote the vector of the corresponding entries in

$\mathbf{m}_{(i,j)}$. Because $\mathbf{m}_{(i,j)}$ has nonzero entries only for the injections at i and j and the line flows through (i,j) , $\mathbf{m}_{(i,j)}^{\mathbf{n}_i}$ has all zero entries. On the other hand, $m_{(i,j)}^i = 1$. Hence, for $\bar{\mathbf{m}}_{(i,j)}$ to satisfy the KCL at bus i in $\bar{\mathcal{G}}$, at least one of $m_{(i,j)}^i$ or entries of $\mathbf{m}_{(i,j)}^{\mathbf{n}_i}$ has to be modified by $\sum_{k=1}^K \alpha_k \mathbf{u}_k$. Thus, \mathcal{U} should contain $\mathbf{u}_{(i)}$ or $\mathbf{u}_{(a,b)}$ for some $(a,b) \in \mathbf{n}_i$.

In case that $\mathbf{u}_{(i)} \notin \mathcal{U}$, for $\bar{\mathbf{m}}_{(i,j)}$ to satisfy the KCL at bus i in $\bar{\mathcal{G}}$, at least one entry of $\bar{\mathbf{m}}_{(i,j)}^{\mathbf{n}_i}$ should have a nonzero value: suppose $\bar{m}_{(i,j)}^{ik}$ takes a nonzero value. If $k \in \mathcal{J}$, we can make a similar argument based on the KCL at k : \mathcal{U} should contain $\mathbf{u}_{(k)}$ or $\mathbf{u}_{(a,b)}$ for some $(a,b) \in \mathbf{n}(k) \setminus \{(i,k), (k,i)\}$. Following this line of argument, we can derive that for each $i \in \mathcal{J}$, \mathcal{U} should contain unit vectors corresponding to at least one of the following sets: (i) injection meter at i , (ii) line flow meters on all the lines in some path (i, v_2, \dots, v_n) in $\bar{\mathcal{G}}^*$ and injection meter at v_n where $v_2, \dots, v_n \in \mathcal{J}$, or (iii) line flow meters on all the lines in some path (i, v_2, \dots, v_n) in $\bar{\mathcal{G}}^*$ where $v_2, \dots, v_{n-1} \in \mathcal{J}$ and v_n is either equal to one of $\{v_2, \dots, v_{n-1}\}$ or not in \mathcal{J} . For each $i \in \mathcal{J}$, \mathcal{U} should contain at least one set of unit vectors corresponding to any of the above three cases: we let \mathcal{S}_i to denote an arbitrary one of such sets.

Note that $\{\mathbf{u}_{(i,j)}, \mathbf{u}_{(j,i)} : (i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}\}$ does not overlap with $\cup_{i \in \mathcal{J}} \mathcal{S}_i$. Hence, $|\mathcal{U}| \geq |\cup_{i \in \mathcal{J}} \mathcal{S}_i| + |\{\mathbf{u}_{(i,j)}, \mathbf{u}_{(j,i)} : (i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}\}|$. Proving $|\cup_{i \in \mathcal{J}} \mathcal{S}_i| \geq |\mathcal{J}|$ gives us the theorem statement, because $|\mathcal{J}| + |\{\mathbf{u}_{(i,j)}, \mathbf{u}_{(j,i)} : (i,j) \in \mathcal{E} \setminus \bar{\mathcal{E}}\}|$ is the exact number of meters the state-preserving attack modifies.

We will prove the following statement for all $n \leq |\mathcal{J}|$, by mathematical induction: for any subset $\bar{\mathcal{J}} \subset \mathcal{J}$ with $|\bar{\mathcal{J}}| = n$, $|\cup_{i \in \bar{\mathcal{J}}} \mathcal{S}_i| \geq n$. For $n = 1, 2, 3$, the statement can be easily verified. Suppose the statement is true for all $n \leq k$

($k \geq 3$), and $\bar{\mathcal{J}}$ is an arbitrary subset of \mathcal{J} with $|\bar{\mathcal{J}}| = k + 1$. The tree condition guarantees that $\bar{\mathcal{J}}$ can be partitioned into two nonempty sets $\bar{\mathcal{J}}_1$ and $\bar{\mathcal{J}}_2$ such that for any $b_1 \in \bar{\mathcal{J}}_1$ and $b_2 \in \bar{\mathcal{J}}_2$, every path in $\bar{\mathcal{G}}^*$ between b_1 and b_2 contains a node not in \mathcal{J} . This implies that $\cup_{b \in \bar{\mathcal{J}}_1} \mathcal{S}_b$ and $\cup_{b \in \bar{\mathcal{J}}_2} \mathcal{S}_b$ are disjoint. By the induction hypothesis, we have $|\cup_{b \in \bar{\mathcal{J}}_1} \mathcal{S}_b| \geq |\bar{\mathcal{J}}_1|$ and $|\cup_{b \in \bar{\mathcal{J}}_2} \mathcal{S}_b| \geq |\bar{\mathcal{J}}_2|$. Thus, $|\cup_{b \in \bar{\mathcal{J}}} \mathcal{S}_b| = |\cup_{b \in \bar{\mathcal{J}}_1} \mathcal{S}_b| + |\cup_{b \in \bar{\mathcal{J}}_2} \mathcal{S}_b| \geq |\bar{\mathcal{J}}_1| + |\bar{\mathcal{J}}_2| = |\bar{\mathcal{J}}|$. Therefore, the induction implies $|\cup_{i \in \mathcal{J}} \mathcal{S}_i| \geq |\mathcal{J}|$, and the theorem statement follows.

5.8.4 Proof of Theorem 5.5.1

Suppose meters are protected as described with \mathcal{T} and \mathcal{B} . Let \mathcal{A} be the resulting subspace of feasible attack vectors and $\mathcal{U} \triangleq \{\mathbf{u}_1, \dots, \mathbf{u}_K\}$ denote the basis of \mathcal{A} consisting of unit vectors in \mathbb{R}^m . Assume that an undetectable attack can be launched for some target topology $\bar{\mathcal{G}}$ (different from \mathcal{G}). We will show that this assumption leads to a contradiction.

Note that \mathcal{U} cannot contain the unit vectors corresponding to the protected measurements. In addition, Theorem 5.3.2 implies that $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{U})$. These two imply that the lines in $\mathcal{E}_{\mathcal{T}}$ cannot be removed by the attack, because each line has a protected line flow meter.

Let \hat{H} ($\hat{\bar{H}}$) denote the submatrix of H (\bar{H}) obtained by selecting the rows corresponding to the protected meter measurements. One can easily verify that $\text{Col}(H) \subset \text{Col}(\bar{H}, \mathcal{U})$ if and only if $\text{Col}(\hat{H}) \subset \text{Col}(\hat{\bar{H}})$. Hence, we have $\text{Col}(\hat{H}) \subset \text{Col}(\hat{\bar{H}})$. This means that for all $\mathbf{x} \in \mathbb{R}^n$, there exists $\mathbf{y} \in \mathbb{R}^n$ such that $\hat{\bar{H}}\mathbf{y} = \hat{H}\mathbf{x}$.

Let $H_{\mathcal{T}}$ denote the submatrix of \widehat{H} obtained by selecting the rows corresponding to the protected line flow meters on the spanning tree \mathcal{T} . Since the lines in $\mathcal{E}_{\mathcal{T}}$ cannot be removed by the attack, the $H_{\mathcal{T}}$ part of H remains the same in \bar{H} ; hence, $H_{\mathcal{T}}$ is also a submatrix of \widehat{H} . Thus, $\widehat{H}\mathbf{y} = \widehat{H}\mathbf{x}$ implies $H_{\mathcal{T}}\mathbf{y} = H_{\mathcal{T}}\mathbf{x}$. Since \mathcal{T} is a spanning tree and it has one protected line flow meter per line, the protected line meters on \mathcal{T} makes the grid observable [71]. Hence, $H_{\mathcal{T}}$ has full column rank. Consequently, $H_{\mathcal{T}}\mathbf{y} = H_{\mathcal{T}}\mathbf{x}$ implies $\mathbf{y} = \mathbf{x}$, and we have $\widehat{H}\mathbf{x} = \widehat{H}\mathbf{x}$. This holds for all $\mathbf{x} \in \mathbb{R}^n$.

Let a be any element in \mathcal{B} . We will show that any line in \mathcal{L}_a cannot be a target line. Note that the injection meter at a is protected, so \widehat{H} and \bar{H} have the row corresponding to the injection at a . $\widehat{H}\mathbf{x} = \bar{H}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$ implies that the injection at bus a should be the same for \mathcal{G} and $\bar{\mathcal{G}}$ as long as the state is the same for the two cases. When the state is \mathbf{x} , the injection at a in \mathcal{G} is $\sum_{k:\{a,k\} \in \tilde{\mathcal{E}}} B_{ak}(x_a - x_k)$, and the injection at a in $\bar{\mathcal{G}}$ is $\sum_{l:\{a,l\} \in \tilde{\bar{\mathcal{E}}}} B_{al}(x_a - x_l)$. Thus we have,

$$\sum_{k:\{a,k\} \in \tilde{\mathcal{E}}} B_{ak}(x_a - x_k) = \sum_{l:\{a,l\} \in \tilde{\bar{\mathcal{E}}}} B_{al}(x_a - x_l), \quad \forall \mathbf{x} \in \mathbb{R}^n,$$

which can be rewritten as follows: for all $\mathbf{x} \in \mathbb{R}^n$,

$$\sum_{k:\{a,k\} \in \tilde{\mathcal{E}} \setminus \tilde{\bar{\mathcal{E}}}} B_{ak}(x_a - x_k) - \sum_{l:\{a,l\} \in \tilde{\bar{\mathcal{E}}} \setminus \tilde{\mathcal{E}}} B_{al}(x_a - x_l) = 0.$$

If $\mathcal{L}_a \cap (\tilde{\mathcal{E}} \Delta \tilde{\bar{\mathcal{E}}})$ is not empty, the above statement is true only when $B_{ak} = 0$ for all $\{a, k\} \in \mathcal{L}_a \cap (\tilde{\mathcal{E}} \Delta \tilde{\bar{\mathcal{E}}})$. B_{ak} is the susceptance of the line $\{a, k\}$ when it is “connected”, and this value is nonzero in practice for every line. Hence, $\mathcal{L}_a \cap (\tilde{\mathcal{E}} \Delta \tilde{\bar{\mathcal{E}}})$ should be empty; *i.e.*, a line in \mathcal{L}_a cannot be a target line.

It was shown that the lines in \mathcal{T} and $\cup_{a \in \mathcal{B}} \mathcal{L}_a$ cannot be a target line. Thus, the

condition (5.17) implies that no line can be a target line, and this contradicts the assumption that there exists an undetectable topology attack.

BIBLIOGRAPHY

- [1] F. Wu, P. Varaiya, P. Spiller, and O. S., “Folk theorems on transmission access: proofs and conterexamples,” *Journal of Regulatory Economics*, vol. 10, 1996.
- [2] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi, “Marginal loss modeling in LMP calculation,” *IEEE Transactions on Power Systems*, vol. 19, no. 2, May 2004.
- [3] T. Zheng and E. Litvinov, “Ex-post pricing in the co-optimized energy and reserve market,” *IEEE Transactions on Power Systems*, vol. 21, no. 4, November 2006.
- [4] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. CRC, 2000.
- [5] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, “Bad data analysis for power system state estimation,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-94, no. 2, pp. 329–337, Mar/Apr 1975.
- [6] F. C. Schweppe, J. Wildes, and D. P. Rom, “Power system static state estimation, Parts I, II, III,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 120–135, 1970.
- [7] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in *ACM Conference on Computer and Communications Security*, 2009, pp. 21–32.
- [8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, dec. 2011.
- [9] L. Jia, R. J. Thomas, and L. Tong, “On the nonlinearity effects on malicious data attack on power system,” in *2012 Power and Energy Society general meeting*, July 2012.
- [10] G. Hug and J. Giampapa, “Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

- [11] F. F. Wu and W. E. Liu, "Detection of topology errors by state estimation," *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 176–183, Feb 1989.
- [12] K. Clements and P. Davis, "Detection and identification of topology errors in electric power systems," *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1748–1753, nov 1988.
- [13] I. Costa and J. Leao, "Identification of topology errors in power system state estimation," *IEEE Transactions on Power Systems*, vol. 8, no. 4, pp. 1531–1538, nov 1993.
- [14] A. Monticelli, "Modeling circuit breakers in weighted least squares state estimation," *IEEE Transactions on Power Systems*, vol. 8, no. 3, pp. 1143–1149, aug 1993.
- [15] R. J. Thomas, L. Tong, L. Jia, and O. E. Kosut, "Some economic impacts of bad and malicious data," in *PSerc 2010 Workshop*, vol. 1, Portland Maine, July 2010.
- [16] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA., Oct 2010.
- [17] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.
- [18] T. Zhang and E. Litvinov, "Ex-post pricing in the co-optimized energy and reserv markets," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1528–1538, Nov. 2006.
- [19] T. L. Baldwin, L. Mili, M. B. Boisen, and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Transactions on Power Systems*, vol. 8, no. 2, 1993.
- [20] A. Gomez-Exposito, A. Abur, P. Rousseaux, A. de la Villa Jaen, and C. Gomez-Quiles, "On the Use of PMUs in Power System State Estimation," in *17th Power Systems Computation Conference*, Stockholm, Sweden, August 2011.
- [21] J. Kim and L. Tong, "On topology attack of a smart grid," in *2013 IEEE*

PES Innovative Smart Grid Technologies (ISGT), Washington, DC, February 2013.

- [22] —, “On topology attack of a smart grid: undetectable attacks and countermeasures,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, July 2013.
- [23] “Power Systems Test Case Archive.” [Online]. Available: <http://www.ee.washington.edu/research/pstca/>
- [24] T. Kim and H. Poor, “Strategic protection against data injection attacks on power grids,” *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.
- [25] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purpy, “Towards a framework for cyber attack impact analysis of the electric smart grid,” in *Proceedings of First IEEE Smart Grid Communication Conference*, Oct 2010.
- [26] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “Cyber attack in a two-area power system: Impact identification using reachability,” in *Proceedings of American Control Conference*, June 2010, pp. 962–967.
- [27] S. Sridhar and G. Manimaran, “Data integrity attacks and their impacts on SCADA control system,” in *Proceedings of IEEE Power and Energy Society General Meeting*, July 2010, pp. 1–6.
- [28] R. Anderson and S. Fuloria, “Who controls the off switch?” in *Proceedings of First IEEE Smart Grid Communication Conference*, Oct 2010.
- [29] Y. Kim, E. C.-H. Ngai, and M. B. Srivastava, “Cooperative state estimation for preserving privacy of user behaviors in smart grid,” in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.
- [30] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, “Competitive privacy in the smart grid: An information-theoretic approach,” in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.
- [31] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, “Smart meter privacy: A utility-privacy framework,” in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.

- [32] S. Wang, L. Cui, J. Que, D.-H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1317–1324, Sep 2012.
- [33] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 1–15, 2012.
- [34] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Nov 2009.
- [35] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and Countermeasures," in *Proceedings of First IEEE Smart Grid Communication Conference*, Oct 2010.
- [36] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 326–333, June 2011.
- [37] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and Countermeasures," in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.
- [38] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.
- [39] M. Esmalifalak, H. A. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proceedings of Second IEEE Smart Grid Communication Conference*, Oct 2011.
- [40] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proceedings of 2011 International Conference on Acoustics, Speech and Signal Processing*, May 2011, pp. 5952–5955.
- [41] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar 2013.
- [42] T. Zheng and E. Litvinov, "On ex post pricing in the real-time electricity

- market,” *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 153–164, Feb 2011.
- [43] F. Li and R. Bo, “DCOPF-based LMP simulation: Algorithm, comparison with ACOPF, and sensitivity,” *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1475–1485, Nov 2007.
 - [44] F. Li, Y. Wei, and S. Adhikari, “Improving an unjustified common practice in ex post lmp calculation,” *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 1528–1538, May 2010.
 - [45] A. Ott, “Unit commitment in the PJM day-ahead and real-time markets,” in *FERC Technical Conference on Increasing Market and Planning Efficiency Through Improved Software and Hardware*. Washington DC, June 2010.
 - [46] F. F. Wu, P. Varaiya, P. Spiller, and S. Oren, “Folk theorems on transmission access: proofs and counterexamples,” *Journal of Regulatory Economics*, vol. 10, no. 1, pp. 5–23, Jul 1996.
 - [47] L. Xie, P. M. S. Carvalho, L. A. F. M. Ferreira, J. Liu, B. H. Krogh, N. Popli, and M. D. Ilić, “Wind integration in power systems: Operational challenges and possible solutions,” *Proceedings of the IEEE*, vol. 99, no. 1, pp. 1890–1908, Jan 2011.
 - [48] ERCOT, “Functional description of core market management system (MMS) applications for look-ahead SCED,” *White paper*, 2011.
 - [49] CAISO, “Business Practice Manuals (BPM) Library: Market Operations, Version 11,” Aug 2010. [Online]. Available: <http://bpm.caiso.com/bpm/bpm/version/0000000000000096>
 - [50] H. Li and L. Tesfatsion, “Capacity withholding in restructured wholesale power markets: An agent-based test bed study,” in *Proceedings of Power System Conference and Exposition*, Mar 2009.
 - [51] A. Tellidou and A. Bakirtzis, “Agent-based analysis of capacity withholding and tacit collusion in electricity markets,” *IEEE Transactions on Power Systems*, vol. 22, no. 4, p. 17351742, Nov 2007.
 - [52] A. Abur and A. G. Expósito, *Power System State Estimation. Theory and Implementation*. New York: Marcel Dekker, 2004.

- [53] A. J. Conejo, E. Castillo, R. Mínguez, and F. Milano, “Locational marginal price sensitivities,” *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 2026–2033, Nov 2005.
- [54] F. Li, “Continuous locational marginal pricing (CLMP),” *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1638–1646, Nov 2007.
- [55] R. Bo and F. Li, “Probabilistic LMP forecasting considering load uncertainty,” *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1279–1289, Aug 2009.
- [56] J. Kim and L. Tong, “On topology attack of a smart grid,” in *2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*. Washington, DC, Feb 2013.
- [57] A. Ashok and M. Govindarasu, “Cyber attacks on power system state estimation through topology errors,” in *Proc. IEEE Power Eng. Soc. General Meeting*, July 2012.
- [58] W. W. Hogan, “Contract networks for electric power transmission,” *Journal of Regulatory Economics*, vol. 4, no. 3, pp. 211–242, Sep 1992.
- [59] T. A. Stuart and C. J. Herget, “A sensitivity analysis of weighted least squares state estimation for power systems,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-92, no. 5, pp. 1696–1701, Sep 1973.
- [60] R. Mínguez and A. J. Conejo, “State estimation sensitivity analysis,” *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1080–1091, Aug 2007.
- [61] A. L. Ott, “Experience with PJM market operation, sysem design, and implementation,” *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.
- [62] D. Kirschen and G. Strbac, *Fundamentals of Power System Economics*. New York: Wiley, 2004.
- [63] “Vulnerability Analysis of Energy Delivery Control Systems,” Idaho National Laboratory, September 2011, INL/EXT-10-18381.
- [64] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

- [65] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweeden, Apr 2010.
- [66] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweeden, Apr 2010.
- [67] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA., Oct 2010.
- [68] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, oct. 2011, pp. 184–189.
- [69] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA, Oct 2010.
- [70] A. Monticelli and F. Wu, "Network observability: Theory," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-104, no. 5, pp. 1042–1048, May 1985.
- [71] G. R. Krumpholz, K. A. Clements, and P. W. Davis, "Power system observability: a practical algorithm using network topology," *IEEE Trans. Power Apparatus and Systems*, vol. 99, no. 4, pp. 1534–1542, July 1980.
- [72] A. Abur, H. Kim, and M. Celik, "Identifying the unknown circuit breaker statuses in power networks," *IEEE Transactions on Power Systems*, vol. 10, no. 4, pp. 2029–2037, nov. 1995.
- [73] L. Mili, G. Steeno, F. Dobraca, and D. French, "A robust estimation method for topology error identification," *IEEE Transactions on Power Systems*, vol. 14, no. 4, pp. 1469–1476, nov 1999.
- [74] E. Lourenco, A. Costa, and K. Clements, "Bayesian-based hypothesis testing for topology error identification in generalized state estimation," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 1206–1215, may 2004.
- [75] A. Jaen, P. Romero, and A. Exposito, "Substation data validation by a lo-

- cal three-phase generalized state estimator,” *IEEE Transactions on Power Systems*, vol. 20, no. 1, pp. 264 – 271, feb. 2005.
- [76] F. Vosgerau, A. Simoes Costa, K. Clements, and E. Lourenco, “Power system state and topology coestimation,” in *Bulk Power System Dynamics and Control (iREP) - VIII (iREP), 2010 iREP Symposium*, aug. 2010, pp. 1 –6.
 - [77] D. Singh, J. P. Pandey, and D. S. Chauhan, “Topology identification, bad data processing, and state estimation using fuzzy pattern matching,” *Power Systems, IEEE Transactions on*, vol. 20, no. 3, pp. 1570–1579, 2005.
 - [78] L. Jia, R. J. Thomas, and L. Tong, “Malicious data attack on real-time electricity market,” in *Proc. 2011 IEEE Intl. Conf. Acoust. Speech & Sig. Proc. (ICASSP)*, Prague, Czech Republic, May 2011.
 - [79] O. Alsac, N. Vempati, B. Stott, and A. Monticelli, “Generalized state estimation,” *IEEE Transactions on Power Systems*, vol. 13, no. 3, pp. 1069 –1075, aug 1998.
 - [80] R. Christensen, *Plane answers to complex questions: the theory of linear models*. Springer, 2011.