

THREAT ANALYSIS AND IMPACT ON CYBER PHYSICAL SECURITY OF POWER SYSTEMS

KUSH KHANNA



**DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI**

JULY 2019

THREAT ANALYSIS AND IMPACT ON CYBER PHYSICAL SECURITY OF POWER SYSTEMS

by

KUSH KHANNA

Department of Electrical Engineering

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

JULY 2019

I dedicate this thesis to my wife and daughter . . .

Acknowledgements

I would like to convey my deep gratitude and respect for my research advisors, Prof. Bijaya Ketan Panigrahi and Prof. Anupam Joshi. Both of them had a prominent role in inspiring me to become an independent researcher and helped me realize the power of critical reasoning. I would like to sincerely thank my thesis committee members: Prof. Nilanjan Senroy , Prof. A. R. Abhyankar and Dr. Ashu Verma for their valuable suggestions.

I would also like to thank the IIT Delhi organisation. In particular the staff, and all faculty members for helping in one way or the other through out my stay in the campus and providing a better place to focus on my research work. I specially want to thank the Dean Academics, Prof. Bhim Singh and the Head of the Department, Prof. S. D. Joshi who made my life at IIT Delhi very comfortable. I wholeheartedly thank my colleagues and friends at IIT Delhi for every second I spent with them, their support both personally and professionally made me what I am today.

Finally, I would like to thank my parents, my wife and my daughter for their patience, support, and the unconditional love that helped me get through my doctoral journey in the most positive way.

Date:

Kush Khanna

Abstract

The power grid is evolving rapidly. With the addition of micro grids, distributed energy resources, and increasing automation in decision making enabled by sensors, the grid has become very complex. Conventional power system was originally designed to provide efficient and reliable power. With the integration of information technology and advanced metering infrastructure, the power grid has become smart. The inclusion of communication technologies in smart grid, has also bridged the gap between utilities and consumers by increasing transparency and enabling consumers to efficiently monitor and control their electricity usage through AMI. The smart meters have allowed the system operators to continuously monitor the power system in real time and take necessary action to avoid system failures. The cyber physical security of power grid has gained more attention in the research community in recent past. Smart meters and communication infrastructure are vulnerable to cyber-threats and if the security is compromised then the consequence can be devastating. It is necessary to study all the possible impacts that cyber-attacks may have on the power grid in order to make the grid immune to cyber-physical intrusions.

Recent studies in this space has exploited the vulnerabilities of the existing power infrastructure to false data injection attacks. A well crafted attack can pass the bad data detection systems during state estimation and affect the operation and control of the power grid. The false data injection attacks are detailed in the thesis and various attacking scenarios are considered to analyse the impact on power system operation and control. The feasibility of false data injection attacks with complete as well as incomplete network knowledge is explained considering IEEE test systems. The conditions for crafting a stealthy attack on state estimations are presented and explained using different case studies and attacking scenarios.

With more and more renewable energy and information technology integration, electricity companies must make sure that they are not paying for spoofed electricity. A study is presented, proposing a new attack through which a private actor injects false data into multiple meters to deceive the system operator with new modified system state to gain momentary profit by projecting higher energy export than actual. Considering limited attacking resources available to the adversary, the attack model exploits the vulnerability and dependency on the metered values to spoof the power export for monetary benefits. From the system operator's perspective, the most vulnerable buses are obtained and ranked based on the severity and minimum set of meters required to launch an attack.

The dependency on the metered values for estimating the power system states for market operations can be further exploited by manipulating the measurements and compromising the real-time locational marginal prices of the system. A virtual bidder leverage this possibility for financial misconducts. A two stage attack reveals that the adversary optimises the incremental and decremental bids to maximise the profits by carrying out false data injection attack as either a load re-distribution attack or a topology masking attack. Attacker with complete system access can also stealthily launch cascading tripping of transmission lines and generators by attacking the integrity of state estimation. It is shown that by injecting false data in certain power injection and power flow measurements, adversary force system operator to change the dispatch and hence making the power system $N - 1$ in-compliant.

Cybersecurity in the power system is a huge concern which must be addressed with topmost priority. Securing all the entry points of the cyber-attacks may not be economically feasible, hence a critical set of sensors must be identified and secured to protect grid against malicious actors. A new priority based defence strategy using normalised measurement Jacobian is presented to select the most critical measurements for securing the power system operation against false data injection attacks. The proposed approach is compared with existing methodologies in the literature and validated using the standard IEEE test cases. However, making a system completely hack proof is rather idealistic, therefore it is also necessary to detect the false data injection attacks in the real-time. A new Log transformation based method

is proposed in the thesis to detect the FDIA in real time with high probability. The proposed method is built on the dynamics of measurement variations. The detection probability of the proposed scheme is compared with existing methodology using benchmark IEEE test system.

To completely alleviate the possibility of cyber threats, the compromised meters must be identified and system operator should be alarmed. To identify the attacked measurements, an artificial intelligence (AI) based identification method is proposed to correctly single out the malicious meters. The proposed AI based method successfully identifies the compromised measurements by predicting the measurements in the event of the cyber-attack. The efficiency of the proposed method is compared for artificial neural network and extreme learning machine based AI techniques. To summarise, the main objective of the thesis is to present various impacts of false data injection attacks on power system state estimation and to build comprehensive risk analysis models forming a basic foundation on which various security measures and algorithms are built to ensure the cyber-physical security of the power system. The defence strategies proposed against data manipulation attacks, not only provides added security to the power system from stealthy data manipulation attacks but also identifies the compromised measurements for ensuring the integrity of power system operation and making the future power grid both fault and attack resilient.

सार

पावर ग्रिड तेजी से विकसित हो रहा है। माइक्रोग्रिड्स के साथ, वितरित ऊर्जा साधन और सेंसर द्वारा सक्षम निर्णय लेने में बढ़ते स्वचालन के कारण ग्रिड बहुत जटिल हो गया है। पारंपरिक शक्ति तंत्र (पावर ग्रिड) मूल रूप कुशल और विश्वसनीय शक्ति प्रदान करने के लिए रचित की गई थी। सूचना प्रौद्योगिकी के एकीकरण और उन्नत पैमाइश बुनियादी ढांचे से शक्ति तंत्र (पावर ग्रिड) बुद्धिमान बन गया है। स्मार्ट ग्रिड में संचार प्रौद्योगिकियों के समावेश ने वितरकों और उपभोक्ताओं के बीच की खाई को पाटा है, साथ ही उत्कृष्ट पारदर्शिता और उपभोक्ताओं को सक्षम किया है। कुशलतापूर्वक निगरानी एवं उनके विद्युत् उपयोग को उन्नत पैमाइशी ढांचे से संयमित किया है। स्मार्ट मीटर ने प्रणाली संचालकों को अनुमति दी है की लगातार वास्तविक समय में बिजली व्यवस्था की निगरानी करें और प्रणाली को विफलताओं से बचाने के लिए आवश्यक कार्रवाई करें। हाल के दिनों में अनुसंधान समुदाय में शक्ति तंत्र की साइबर भौतिक सुरक्षा पर अधिक ध्यान दिया गया है। स्मार्ट मीटर तथा संचार के बुनियादी ढांचे साइबर खतरे के लिए कमजोर हैं और अगर सुरक्षा से समझौता किया जाता है तो परिणाम विनाशकारी हो सकते हैं। यह उन सभी संभावित प्रभावों का अध्ययन करने के लिए आवश्यक है जिनमें साइबर आक्रमण पावर ग्रिड पर हो सकते हैं एवं जो साइबर भौतिक घुसपैठ के लिए ग्रिड को प्रतिरक्षित करते हैं।

हाल के अध्ययनों ने मौजूदा शक्ति की बुनियादी ढांचों में झूठे आधार-सामग्री अन्तःक्षेपण आक्रमणों के कमजोरियों का लाभ उठाया है। एक अच्छी तरह से तैयार किया गया आक्रमण खराब आधार-सामग्री की स्थिति आंकलन के दौरान पारित कर सकता है और शक्ति के संचालन और नियंत्रण को प्रभावित कर सकता है। झूठे आधार-सामग्री अन्तःक्षेपण हमले इस शोध-कार्य में विभिन्न हमलावर परिदृश्यों में विस्तृत हैं जो की बिजली प्रणाली के संचालन और नियंत्रण पर प्रभाव का विश्लेषण करने के लिए माने जाते हैं। संभाव्यता पूर्ण के साथ-साथ अधूरे नेटवर्क ज्ञान के साथ झूठे आधार-सामग्री अन्तःक्षेपण हमलों का IEEE परीक्षण प्रणालियों पर विचार करते हुए समझाया गया है। स्थितियों पर एक गुप्त हमले का मसौदा तैयार करने की शर्तें विभिन्न मामलों का अध्ययन और आक्रमण परिदृश्यों का उपयोग करके आकलन प्रस्तुत और समझाया गया है।

अधिक से अधिक नवीकरणीय ऊर्जा और सूचना प्रौद्योगिकी एकीकरण, बिजली कंपनियों को यह सुनिश्चित करना चाहिए कि वे खराब बिजली के लिए भुगतान नहीं कर रहे हैं। यहाँ एक अध्ययन

प्रस्तुत किया गया है, जिसमें एक नए हमले का प्रस्ताव क्षणिक लाभ हासिल करने के लिए नए संशोधित तंत्र के साथ प्रणाली संचालकों को धोखा देने के लिए वास्तविक की तुलना में उच्च ऊर्जा निर्यात का अनुमान लगाकर, जिसके माध्यम से एक निजी माध्यम झूठे आधार-सामग्री को कई मीटर में अन्तःक्षेपण करता है। सीमित हमलावर संसाधनों को देखते हुए जो की आक्रमणकरियों के पास उपलब्ध है, हमले के मॉडल पर भेद्यता मौद्रिक लाभ के लिए बिजली निर्यात को बिगाड़ने के लिए मिले हुए मूल्य और निर्भरता का शोषण करता है। प्रणाली संचालकों के परिप्रेक्ष्य में, सबसे कमजोर बसों को गंभीरता के आधार पर प्राप्त और हमले शुरू करने के लिए आवश्यक न्यूनतम संख्याओं पर निर्धारित किया जाता है।

बाजार के लिए बिजली व्यवस्था का आकलन करने के लिए पैमाइश मूल्यों पर निर्भरता माप में हेरफेर और तंत्र के वास्तविक समय के स्थानीय सीमांत मूल्य में समझौता करके संचालन का और अधिक शोषण किया जा सकता है। एक आभासी बोलीदाता इस संभावना का वित्तीय कदाचार के लिए लाभ उठाता है। एक द्विचरणीय हमले से पता चलता है कि एक विरोधी वृद्धिशील अनुकूलन करता है और झूठा आधार-सामग्री अन्तःक्षेपण हमले के रूप में बाहर ले जाने के द्वारा लाभ को अधिकतम करने के लिए बढ़ती बोली या तो एक लोड पुनः वितरण हमला या एक टोपोलॉजी मास्किंग हमला करता है। एक हमलावर पूरे तंत्र के उपयोग से भी ट्रांसमिशन लाइनों और जनरेटर को चुपके से स्थिति आकलन की अखंडता पर हमला करके कैस्केडिंग ट्रिपिंग को लॉन्च कर सकता है। शोध कार्य में यह दिखाया गया है कि कुछ में गलत डेटा इंजेक्ट करके बिजली इंजेक्शन और बिजली प्रवाह माप, बदलने के लिए विरोधी बल प्रणाली ऑपरेटर प्रेषण करता है और इसलिए बिजली प्रणाली $N - 1$ को अनिवार्य बनाता है।

बिजली व्यवस्था में साइबर सुरक्षा एक बहुत बड़ी चिंता है जिसका सर्वोच्च प्राथमिकता के साथ समाधान किया जाना चाहिए। हो सकता है कि आर्थिक रूप से साइबर हमलों के सभी प्रवेश बिंदु सुरक्षित न संभव हों, इसलिए सेंसर के एक महत्वपूर्ण सेट की पहचान की जानी चाहिए और ग्रीड से बचाने के लिए हानिकारक माध्यमों से सुरक्षित किया जाना चाहिए। सामान्यीकृत माप का उपयोग करके एक नई प्राथमिकता आधारित रक्षा रणनीति जैकबियन को बिजली प्रणाली को गलत डेटा इंजेक्शन हमलों के खिलाफ ऑपरेशन सुरक्षित करने के लिए सबसे महत्वपूर्ण माप का चयन करने के लिए प्रस्तुत किया गया है। यहाँ प्रस्तावित दृष्टिकोण की कार्यप्रणाली तुलना मौजूदा साहित्य के साथ की जाती है और मानक IEEE परीक्षण मामलों का उपयोग करके मान्य

की गयी है। हालाँकि, एक प्रणाली को पूरी तरह से हैक प्रूफ बनाना आदर्शवादी है, इसलिए यह आवश्यक भी है वास्तविक समय में झूठे आधार-सामग्री अन्तःक्षेपण हमलों का पता लगाएं। उच्च संभावना के साथ वास्तविक समय में एफडीआई का पता लगाने के लिए शोध कार्य में एक नया लॉग परिवर्तन आधारित विधि प्रस्तावित है। प्रस्तावित विधि माप विविधताओं की गतिशीलता पर बनाया गया है संभावना प्रस्तावित स्कीम की तुलना बेंचमार्क IEEE टेस्ट सिस्टम के इस्तेमाल से की गई है।

साइबर खतरों की संभावना को पूरी तरह से कम करने के लिए त्रुटिपूर्ण मीटर की पहचान होनी चाहिए और सिस्टम ऑपरेटर को सतर्क किया जाना चाहिए। हमले के माप की पहचान करने के लिए, कृत्रिम बुद्धिमत्ता (एआई) आधारित पहचान विधि त्रुटिपूर्ण मीटर को सही ढंग से एकल करने का प्रस्ताव है। प्रस्तावित AI आधारित विधि साइबर आक्रमण की स्थिति में मापों की भविष्यवाणी करके त्रुटिपूर्ण मापनों की सफलतापूर्वक पहचान करती है। सक्षमता प्रस्तावित विधि की तुलना मशीन आधारित एआई (AI) तकनीक कृत्रिम तंत्रिका नेटवर्क (ANN) और एक्सट्रीम लर्निंग मशीन्स (ELM) के द्वारा किया गया है। संक्षेप में प्रस्तुत करने के लिए थीसिस का मुख्य उद्देश्य बिजली प्रणाली राज्य के आकलन प्रस्तुत करना है और निर्माण पर झूठे आधार-सामग्री इंजेक्शन हमलों के विभिन्न प्रभाव पर एक व्यापक आधार बनाने वाली व्यापक जोखिम विश्लेषण मॉडल, जिस पर विभिन्न सुरक्षा उपायों और एल्गोरिदम को बिजली प्रणाली की साइबर-भौतिक सुरक्षा सुनिश्चित करने के लिए बनाया गया है। यहाँ प्रस्तुत रक्षा रणनीति डेटा हेरफेर हमलों के खिलाफ प्रस्तावित है, यह न केवल चोरी के आधार-सामग्री हेरफेर हमलों से बिजली प्रणाली को अतिरिक्त सुरक्षा प्रदान करता है अपितु बिजली व्यवस्था संचालन और त्रुटिपूर्ण मापनों से भविष्य की बिजली ग्रिड बनाने की अखंडता हेतु दोनों दोष और आक्रमण रहित करता है।

Contents

Certificate	v
Acknowledgements	vii
Abstract	ix
List of Figures	xvii
List of Tables	xix
Nomenclature	xxiii
1 Introduction	1
1.1 Introduction	1
1.2 Smart Grid Infrastructure	3
1.3 Cybersecurity Concerns and Countermeasures: Literature Review	5
1.4 Research Gaps and Motivation	10
1.5 Research Objectives	12
1.6 Summary of research work	13
1.7 Proposed outline of the thesis	17
2 Feasibility of false data injection attacks	21
2.1 Introduction	21
2.2 Brief overview of State Estimation	21

2.2.1	Weighted Least Square (WLS) State Estimation	23
2.2.2	Bad Data Detection	26
2.3	False Data Injection Attacks	27
2.3.1	FDIAs on State Estimation	28
2.3.2	FDIAs with limited network information	29
2.4	Observable and Unobservable Attacks	30
2.4.1	Formulation of FDIAs using NRLF	31
2.4.2	Observability of Attacks	33
2.4.3	Simulations and Discussion	35
2.5	Summary	36
3	FDIAs to spoof over injection with limited network information	39
3.1	Introduction	39
3.2	FDIAs to spoof over-injection	40
3.2.1	Formulation of Attacking Region	41
3.2.2	Attack Model	44
3.3	Vulnerability Analysis	48
3.3.1	IEEE 14 bus	48
3.3.2	IEEE 30 bus	53
3.4	Possible defense strategies	56
3.5	Summary	57
4	Analysis of FDIAs on Electricity Markets	59
4.1	Introduction	59
4.2	Electricity Markets and Virtual Bidding	59
4.3	Maximizing profits by FDIAs on SE	60
4.3.1	Load Redistribution Attack	61
4.3.2	Topology Attack	73
4.4	Summary	78

5	Attack on Security Constrained Optimal Power Flow	79
5.1	Introduction	79
5.2	Formulation of attack on SCOPF	80
5.2.1	Considering Line Contingencies only	83
5.2.2	Considering both Line and Generator Contingencies	86
5.3	Impact Analysis and Discussion	87
5.3.1	Sample 3 bus system	88
5.3.2	IEEE 14 and 30 bus system	91
5.4	Summary	97
6	Priority based protection strategy against FDIAs	101
6.1	Introduction	101
6.2	Generalising the impacts of FDIAs	102
6.3	Problem with the existing methods	103
6.4	Normalised measurement Jacobian based protection strategy	108
6.4.1	Considering conventional measurements only	108
6.4.2	Considering both PMU and conventional measurements	110
6.5	Test Cases and Simulations	112
6.5.1	Considering conventional measurements only	112
6.5.2	Considering both PMUs and conventional measurements	114
6.6	Summary	114
7	Real-time detection of FDIAs and identification of compromised measurement sensors	117
7.1	Introduction	117
7.2	False Data Detection	118
7.2.1	Attack Formulation	118
7.2.2	Attacking Region	122
7.2.3	Detection Methodology	122

7.2.4	Results and Discussion	125
7.3	AI based Identification of malicious meters	130
7.3.1	Proposed Scheme	131
7.3.2	System Details	134
7.3.3	Generalised Attack Formulation	134
7.3.4	False Data Detection for Generalised Attack	136
7.3.5	Identification of attacked meters	138
7.4	Summary	142
8	Conclusion	145
8.1	Summary of the Thesis	145
8.2	Scope for future research	146
	References	149
	List of Publications	157
	Bio-Data	159

List of Figures

1.1	Complete Smart Grid Schematic	4
1.2	Cyber vulnerabilities in smart grid environment.	7
1.3	Outline of the Thesis	17
2.1	SCADA/EMS operation flow	22
2.2	Six bus example	30
2.3	False data injection attack with limited network knowledge	31
2.4	Case 1	36
2.5	Case 2	37
3.1	Six bus example with primary attacking region.	42
3.2	Extended attacking region for simple six bus system.	43
3.3	Attack with generator at bus 3.	47
3.4	Primary attacking regions for IEEE 14 bus system.	49
3.5	Primary attacking regions for IEEE 30 bus system.	54
4.1	Stage 1: Optimizing the amount of P_i^v (bus 3-8) considering load redistribution attack.	71
4.2	Stage 1: Optimizing the amount of P_i^v (bus 9-14) considering load redistribu- tion attack.	72
4.3	A simple topology attack with limited network information	74
4.4	Stage 1: Optimizing the amount of P_i^v (bus 4-9) considering topology masking attack.	76

4.5	Stage 1: Optimizing the amount of P_i^v (bus 10-14) considering topology masking attack.	77
5.1	Security threats in smart grid.	81
5.2	Attack formulation as a bi-level optimization problem	82
5.3	Three bus system, no attack.	89
5.4	Three bus system, with attack.	90
5.5	Critical lines and sequence of events (post-attack). ‘1’/‘2’ is target event and ‘1+’/‘2+’ are events post occurrence of ‘1’/‘2’	93
6.1	5 bus system.	106
6.2	Percentage of injection sensors, flow sensors and total sensors protected for all test systems	113
7.1	Attacking regions for IEEE 14 bus system.	123
7.2	IEEE 14 bus system.	125
7.3	NYISO map showing 11 load zones.	126
7.4	Histogram of Kullback Leibler Distance Using Log transformation for attack scenario 1.	128
7.5	Histogram of Kullback Leibler Distance Using Log transformation for attack scenario 2.	129
7.6	The complete schematic for detection and identification of FDIAs	131
7.7	Histogram of KLDs considering No-attack and attack scenarios	137

List of Tables

1.1	FDIAs and Defence Techniques.	11
2.1	GMI and ZIMI indices for IEEE 14 Bus System	35
2.2	States and Power Injections for Different Attack Cases for IEEE 14 Bus System	37
3.1	Attack Vector for N_9^{pri}	51
3.2	Attack Vector for $\{4, 7, 9, 10, 11, 14\}$	51
3.3	Attack Vector for $\{4, 7, 9, 10, 13, 14\}$	51
3.4	Attack Vector for N_{10}^{pri}	52
3.5	Attack Vector for N_{14}^{pri}	52
3.6	Attack Locations and Ranking for IEEE 14 Bus System	53
3.7	Attacking Regions for IEEE 30 Bus System	55
3.8	Attack Locations and Ranking for IEEE 30 Bus System	55
4.1	IEEE 14 Bus Line Limits	70
4.2	Stage 1: Optimizing the amount of P_i^v and corresponding attack vectors . .	71
4.3	Stage 2: Optimizing the corresponding attack vectors in real-time	73
4.4	Stage 1: Optimizing P^v for single line-outage topology attack	78
5.1	Generator dispatch, load and line flows before and after attack for a 3 bus system	91
5.2	Attack Vector for Load Measurements in IEEE 14 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)	92

5.3	Attack Vector for Power Flow Measurements in IEEE 14 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)	92
5.4	Attack Vector for Load Measurements in IEEE 30 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)	95
5.5	Attack Vector for Power Flow Measurements in IEEE 30 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)	96
5.6	Generator Cost Data for 3 Bus System	97
5.7	IEEE 14 Bus Line Limits	98
5.8	IEEE 30 Bus Line Limits	99
6.1	5 Bus system Load/Generator Data and State (θ).	106
6.2	Attack Vector $\mathbf{a}$ when P_4 is not attacked	107
6.3	$\mathbf{c}$ and x_{est} when P_4 is not attacked.	107
6.4	J for each θ when one measurement sensor is not attacked	107
6.5	Solution for Test Cases: Considering Conventional Measurements only . . .	113
6.6	Solution for Test Cases: Considering both PMU and Conventional Measurements	115
7.1	Detection Percentage Comparison for Attack Scenario 1	127
7.2	Detection Percentage Comparison for Attack Scenario 2	130
7.3	MAPE and Threshold for P_i and Q_i measurements using ANN based load estimator	138
7.4	MAPE and Threshold for P_{ij} measurements using ANN based load estimator	139
7.5	MAPE and Threshold for P_i and Q_i measurements using ELM based load estimator	139
7.6	MAPE and Threshold for P_{ij} measurements using ELM based load estimator	139
7.7	Identification of compromised measurements considering attack on θ with different c (%) using ANN	140
7.8	Identification of compromised measurements considering attack on θ with different c (%) using ELM	141

7.9	Identification of compromised measurements considering attack on V with different c (%) using ANN	142
7.10	Identification of compromised measurements considering attack on V with different c (%) using ELM	143

Nomenclature

Chapter 2

$\mathbf{a}$	Attack vector.
$\mathbf{c}$	Error caused in the state vector due to attack vector $\mathbf{a}$.
$\mathbf{H}$	Measurement Jacobian.
$\mathbf{V}$	$V \angle \theta$.
$\mathbf{Y}^A$	Bus admittance matrix for the attacking region.
G_{ij}, B_{ij}	$(i, j)^{th}$ element of bus admittance matrix.
g_{ij}, b_{ij}	Conductance and susceptance of line $i - j$.
g_{si}, b_{si}	Shunt conductance and shunt susceptance at bus i .
N	Number of buses in the system.
P_i	Real power injection at bus i .
P_{ij}	Real power flow in the line $i - j$.
Q_i	Reactive power injection at bus i .
Q_{ij}	Reactive power flow in the line $i - j$.

Chapter 3

$\delta^{pre-attack}$	$ N_{bus} \times 1$ vector for load angles obtained through DCOPF before the attack
$\delta_{N_i^{pri}}$	Load angle vector for the primary attacking region.
δ	Column matrix for angles in radians.
a	Attack Vector.
B	Bus admittance matrix of the network.
c	Estimated error injected in the state variable by the attacker.
e	Measurement error vector.
H	$[h_{ij}]_{m \times n}$.
$P_D^{N_i^{pri}}$	Real power demand vector of the primary attacking region.
$P_D^{pre-attack}$	$ N_{bus} \times 1$ vector for real power demand before the attack.
P_D	Real power demand vector.
$P_G^{pre-attack}$	$ N_{bus} \times 1$ vector for real power generation before the attack.
P_G	Real power generation vector.
$P_{N_i^{pri}}$	Power injection vector for the primary attacking region.
x	State variable vector ($n \times 1$).
z_a	Measurement vector with false data injected.
z	True measurement vector ($m \times 1$).
Δf	Net changes in the line flows in the attacking region.
ϕ	Null set.
BB_i^{pri}	Set of boundary buses for the attacking region N_i^{pri} .

BB_i^{ext}	Set of the boundary buses for the extended attacking region.
$C_g(P_{Gg})$	Generation cost function for the generator at bus g .
$h(x)$	Measurement function $[h_1(x_1, x_2, \dots, x_n), \dots, h_m(x_1, x_2, \dots, x_n)]^T$.
N_G	Set of generator buses.
N_i^{adj}	Set of all the adjoining buses of the primary region N_i^{pri} .
N_i^{pri}	Set of buses in primary attacking region for the bus i .
N_{Bi}	Set of all buses directly connected to bus i .
N_{Bj}	Set of all the buses directly connected to bus j .
N_{ik}^{ext}	Set of all the buses in the extended attacking region considering k^{th} subset of power set $\mathcal{P}(N_i^{adj})$.
p	Total number of subsets of the power set $\mathcal{P}(N_i^{adj})$.
P_{Gg}	Power generation at bus g .
P_{Gg}^{max}	Maximum generation specified for the generator at the bus g .
P_{Gg}^{min}	Minimum generation specified for the generator at the bus g .

Chapter 4

ΔF	Attack vector for power flow measurements.
ΔP_D	Load redistribution vector.
$\Omega^{DA+}, \Omega^{DA-}$	Binary variables $(N_L \times 1)$.
$\Omega^{RT+}, \Omega^{RT-}$	Binary variables $(N_L \times 1)$.
ϕ^{DA+}, ϕ^{DA-}	Binary variables $(N_G \times 1)$.
ϕ^{RT+}, ϕ^{RT-}	Binary variables $(N_G \times 1)$.

F^{DA}	Line flow vector for day-ahead formulation.
F^{RT}	Line flow vector for real-time formulation.
P_D^{RT}	Real-time demand vector.
P_D	Day-ahead demand vector.
P_G^{DA}	Day-ahead generator dispatch schedules.
P_G^{RT}	Real-time generator dispatch schedules.
S, K_D, K_G, K_V	Shift factor matrix, bus-load incidence matrix, bus-generator incidence matrix, bus-virtual bid incidence matrix.
$\Lambda^{DA}, \mu^{DA+}, \mu^{DA-}$	Lagrange multipliers for day-ahead formulation.
$\Lambda^{RT}, \mu^{RT+}, \mu^{RT-}$	Lagrange multipliers for real-time formulation.
$\lambda_i^{DA}, \lambda_i^{RT}$	Day-ahead and real-time LMPs for the i^{th} bus.
$\underline{F}_l, \overline{F}_l$	Minimum and maximum line flow limits for the line ' l '.
$\underline{P}_i^v, \overline{P}_i^v$	Lower and upper limit for the amount of power a virtual trader can buy/sell in DAM.
$\underline{P}_{Gg}, \overline{P}_{Gg}$	Minimum and maximum generation limits for the generator ' g '.
$C_{Gg}(\bullet)$	Generation cost function for g^{th} generator.
M	Scalar constant with high scalar value ($\gg 0$).
N_D	Set of buses with load connected.
N_G	Set of buses with generator connected.
N_L	Set of transmission lines in the network.
P_i^v	Amount of power traded as virtual bid at bus ' i '.

Chapter 5

D	Bus-Load incidence matrix.
F^N	Flows considering dispatch P'_g and actual load P_D .
$F^{N-1(cg)}$	Flows considering dispatch P'^{cg}_g , actual load P_D and cg^{th} generator outage.
$F^{N-1(cl)}$	Flows considering dispatch P'_g , actual load P_D and cl^{th} line outage.
G^{cg}	Bus-Generator incidence matrix considering cg^{th} generator outage.
G	Bus-Generator incidence matrix.
P_D	Real power demand vector.
P'^{cg}_g	Real power generation vector considering cg^{th} generator outage.
P'_g	Generator dispatch vector considering corrupted load measurements.
P_g, R^{cg}_g	Dispatch variables for the inner level optimization problem.
R'^{cg}_g	Real power generation ramp vector considering cg^{th} generator outage.
R'_g	Generator ramp vector considering corrupted load measurements.
S^{cl}	Shift factor matrix considering cl^{th} line outage.
S	Shift factor matrix.
ΔF_l	Change in the flow measurement of l^{th} branch.
ΔP_{Dd}	Change in the load measurement of d^{th} bus.
ϵ	Fraction of allowable load change.
$\overline{F}_l / \underline{F}_l$	Maximum/Minimum flow limit of the branch l .
$\underline{P}_{gi} / \overline{P}_{gi}$	Minimum/Maximum generation limits of generator at i^{th} bus.

B_{gen}	Count for lines violating the limits for one generator contingency.
B_{line}	Count for lines violating the limits for one line contingency.
$C_{gi}(P_{gi})$	Cost of generator on i^{th} bus.
FL_l	$FL_l = 1$ indicating $\Delta F_l \neq 0$.
L_d	$L_d = 1$ indicating $\Delta P_{Dd} \neq 0$.
N_D	Set of all the buses where load is connected.
N_L	Set of all the branches of the network.
N_{bus}	Number of bus in the network.
r	Fraction of allowable generation change during generator contingency.

Chapter 6

$\mathbf{a}$	Attack vector.
$\mathbf{c}$	Error caused in the state vector due to attack vector $\mathbf{a}$.
$\mathbf{H}^*$	Binary matrix for the Jacobian matrix $\mathbf{H}$.
$\mathbf{H}_s^*$	Normalised measurement Jacobian.
$\mathbf{H}$	Measurement Jacobian.
μ_k	Binary variable. $\mu_k=1/0$ denotes that PMU is present/absent at bus k .
ω_k	Binary variable. $\omega_k=1/0$ denotes that k^{th} PMU is protected/unprotected.
ψ_i	Binary variable. $\psi_i = 1/0$ denotes that measurement i is protected/unprotected.
l_i	Coupling variable for measurement i .
M	Limit on number of sensors that can be protected.

N_μ Limit on number of PMUs that can be protected.

Chapter 7

e Gaussian measurement error vector.

PD^*, QD^* Attacked real and reactive power demand for all the buses in the attacking region N_i .

PD^{true} Real power demand vector before attack.

QD^{true} Reactive power demand vector before attack.

V^*, δ^* Attacked voltage and angle for all the buses in the attacking region N_i .

x_{bad} State vector after attack.

z_{bad} Perturbed measurements after attack.

ΔP_{di} Change in real power load at the bus i .

ΔQ_{di} Change in reactive power load at the bus i .

ϕ Null set.

f, t From bus and To bus matrix for transmission lines.

N_A^i Set of buses directly affected by change in the state θ_i or V_i .

N_b^i Set of buses directly connected to the bus i .

N_G^1, N_G^0 Set of generator buses with and without load.

N_i Set of buses attacking region for load altering attack at i^{th} bus.

N_i^B Set of boundary buses in the attacking region N_i

N_Z Set of zero injection buses.

N_{Bi} Set of buses connecting i^{th} bus directly.

n_{flow}^i	Total number of real power flow meters required to be attack to cause change in state θ_i or V_i .
n_{inj}^i	Total number of real and reactive power injection measurements required to be modified to cause intended change in state θ_i or V_i .
N_{line}	Set of transmission lines affected by change in state θ_i or V_i .
N_{line}^i	Set of transmission lines directly connected to the bus i .
P_i^{spec}	Specified real power injection at bus i post attack.
P_i^{true}	True real power injection at bus i before attack.
Q_i^{spec}	Specified reactive power injection at bus i post attack.
Q_i^{true}	True reactive power injection at bus i before attack.
V^{true}, δ^{true}	True voltage and angle vector.