

CYBERSECURITY OF ELECTRICAL INFRASTRUCTURES

KIRTI GUPTA



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

JUNE 2024

CYBERSECURITY OF ELECTRICAL INFRASTRUCTURES

by

KIRTI GUPTA

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

In fulfilment of the requirements of the degree of doctor of philosophy

to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

JUNE 2024

Dedicated to The Almighty

and

My Loving Family



INDIAN INSTITUTE OF TECHNOLOGY DELHI

CERTIFICATE

This is to certify that the thesis entitled “**CYBERSECURITY OF ELECTRICAL INFRASTRUCTURES**” submitted by **Ms. Kirti Gupta (Entry No. 2019EEZ8353)**, to Indian Institute of Technology Delhi for the award of the degree of **Doctor of Philosophy (Ph.D.)** in Electrical Engineering is a bonafide record of research work carried out by her under my supervision. The contents of this thesis have not been submitted to any other institute or university for the award of any degree or diploma.

.....

Prof. BIJAYA KETAN PANIGRAHI

Professor

Department of Electrical Engineering

Indian Institute of Technology Delhi

Hauz Khas, New Delhi, 110016, India

Date: 06 June, 2024



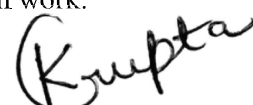
INDIAN INSTITUTE OF TECHNOLOGY DELHI

Acknowledgement

I am deeply grateful to my supervisor, Prof. Bijaya Ketan Panigrahi, for granting me the invaluable opportunity to pursue research in this field. Throughout my Ph.D. journey he has provided constant guidance and encouragement. Working as a member of his esteemed research group has been a great honor and a truly enriching experience.

I extend my deep gratitude to the esteemed members of my doctoral research committee: Prof. A R. Abhyankar, Dr. Sumit Kumar Paramanick, and Dr. Sumit Kumar Chattopadhyay. Their invaluable suggestions and thorough examination of my work have immensely contributed to its quality and rigor. I am also indebted to Dr. Subham Sahoo, Dr. Rabindra Mohanty, and Prof. Frede Blaabjerg for their continuous guidance and insightful mentoring throughout my research journey. Their expertise and suggestions have played a vital role in shaping this work. I would like to express my sincere appreciation to Prof. Anupam Joshi and Prof. K. Paul for their expert advice and constructive feedback. This work is a reflection of their profound thoughts, ideas, and dedicated efforts. I am sincerely grateful for their valuable suggestions and the time they have invested in my research.

I am forever indebted to my parents, Mr. Ramesh Kumar and Mrs. Ruby Gupta, as well as my brother, Mr. Vaibhav Kumar Yashaswi, for their boundless love and patience. Their constant presence has been a tremendous source of inspiration for me. I would like to express my heartfelt gratitude to my seniors for fostering a nurturing research environment. Their guidance and shared experiences have been invaluable to me. I am also grateful to all my friends and juniors who have made my Ph.D. years incredibly memorable. Additionally, I extend my thanks to the staff members of IIT Delhi, for their unwavering support. Finally, I would like to express my gratitude to the Ministry of Human Resources and Development, India, for providing the scholarship grant that has supported my research work.


KIRTI GUPTA

Date: 06 June, 2024

Abstract

Power electronic systems (PES) are pivotal in achieving efficiency, sustainability, and flexibility goals. The integration of resilient control with communication transforms PES into sophisticated cyber-physical systems. While information and communication technology (ICT) enables accurate and time-stamped measurements for efficient control, the increasing reliance on ICT also exposes PES to cyber-attacks. This work focuses on addressing challenges associated with data integrity attacks, data availability attacks, and dynamic load altering attacks (DLAAs) in PES. Data integrity attacks, also known as false data injection attacks (FDIAs), involve manipulating exchanged information, undermining its integrity. Such attacks can mislead control and protection systems, leading to compromised PES operation. Data availability attacks disrupt the availability of exchanged information, encompassing latency attacks, data dropouts, and time synchronization attacks (TSAs). These attacks impair the control system's awareness of the system's condition, impeding its operation. Furthermore, the growing integration of internet of things (IoT) devices and the utilization of ICT for demand-side management (DSM) have given rise to a new type of attack called DLAAs, which target consumers by manipulating power demand. Additionally, the increased adoption of electric vehicles (EVs) in response to environmental concerns has led to an expansion of electric vehicle infrastructure (EVI). However, this expanded connectivity introduces vulnerabilities such as privacy breaches, malware injection, and disruptions in EV charging processes. These vulnerabilities in PES pose significant risks to grid stability, protection and emergency services, emphasizing the importance of securing PES to mitigate their adverse effects on end applications.

In this thesis, the primary focus is on enhancing the resiliency of PES against data integrity attacks and data availability attacks, by drawing inspiration from the guidelines provided by the National Institute of Standard and Technology (NIST) for critical infrastructure cybersecurity. Additionally the vulnerability assessment of the PES with adoption of EVs is also investigated. The studies carried out in this thesis cover a wide range of areas, ranging from development of a cyber-physical co-simulation testbed to assess vulnerabilities and validate control algorithms. Moreover, an EV charging infrastructure testbed is developed

for conducting risk assessments. It offers a realistic environment for charging EVs using standard charging protocols. These testbeds also serve as a platform for verifying proposed algorithms, thereby strengthening the overall cybersecurity of the system. Further, anomaly diagnosis schemes are proposed for both AC and DC systems to ensure reliable and secure operation of PES in the presence of large signal disturbances. These schemes are capable of distinguishing between grid faults and cyber-attacks for selective relay operations. To mitigate data availability attacks such as latency, data dropouts, and time synchronization attacks (TSAs) in both AC and DC systems, semantic principles are integrated into the sampling process. Moreover, a framework is developed for DLAAAs in PES, from the defender's perspective, particularly for vulnerable loads like remotely controllable and frequency-responsive loads. In addition, a generic small-signal state-space model (SSM) of EVs integrated into PES is presented, uncovering the dynamic interplay between DER elements, network parameters, and the cyber graph topology. The study also highlights the denial of charging (DoC) attack, which disrupts the charging process of electric vehicles (EVs). A real hardware setup based on the Bharat EV DC charging standard (BEV DC-001) is utilized to demonstrate this attack, leveraging the controller area network (CAN) bus for communication between the EV charger and EV. Real-time simulation case studies are conducted to validate the proposed approaches and concepts. The findings contribute to the development of robust and cyber-secure designs for PES cybersecurity investigations, offering insights and paving the way for future research in this field.

Keywords: Anomaly diagnosis, cyber security, cyber-attacks, data integrity attacks, data availability attacks, denial of charging (DoC) attack, dynamic load altering attacks (DLAAs), electric vehicle infrastructure (EVI), faults, small signal modeling.

पावर इलेक्ट्रॉनिक सिस्टम (PES) दक्षता, स्थिरता और लचीलेपन के लक्ष्यों को प्राप्त करने में महत्वपूर्ण हैं। संचार के साथ लचीले नियंत्रण का एकीकरण PES को परिष्कृत साइबर-भौतिक प्रणालियों में बदल देता है। जबकि सूचना और संचार प्रौद्योगिकी (ICT) कुशल नियंत्रण के लिए सटीक और समयबद्ध माप को सक्षम करती है, ICT पर बढ़ती निर्भरता भी PES को साइबर हमलों के लिए उजागर करती है। यह कार्य PES में डेटा अखंडता हमलों, डेटा उपलब्धता हमलों और गतिशील भार परिवर्तन हमलों (DLAAs) से जुड़ी चुनौतियों का समाधान करने पर केंद्रित है। डेटा इंटीग्रिटी अटैक, जिसे फाल्स डेटा इंजेक्शन अटैक (FDIA) के रूप में भी जाना जाता है, में एक्सचेंज की गई जानकारी में हेरफेर करना, इसकी अखंडता को कम करना शामिल है। इस तरह के हमले नियंत्रण और सुरक्षा प्रणालियों को भ्रमित कर सकते हैं, जिससे समझौता किए गए PES ऑपरेशन हो सकते हैं। डेटा उपलब्धता हमले आदान-प्रदान की गई जानकारी की उपलब्धता को बाधित करते हैं, जिसमें विलंबता हमले, डेटा ड्रॉपआउट और टाइम सिंक्रोनाइजेशन अटैक (TSA) शामिल हैं। ये हमले नियंत्रण प्रणाली की प्रणाली की स्थिति के बारे में जागरूकता को कम करते हैं, इसके संचालन को बाधित करते हैं। इसके अलावा, इंटरनेट ऑफ थिंग्स (IoT) उपकरणों के बढ़ते एकीकरण और मांग-पक्ष प्रबंधन (DSM) के लिए (ICT) के उपयोग ने LAAs नामक एक नए प्रकार के हमले को जन्म दिया है, जो बिजली की मांग में हेरफेर करके उपभोक्ताओं को लक्षित करता है। इसके अतिरिक्त, पर्यावरणीय चिंताओं के जवाब में इलेक्ट्रिक वाहनों (EVs) को अपनाने से इलेक्ट्रिक वाहन इंफ्रास्ट्रक्चर (EVI) का विस्तार हुआ है। हालाँकि, यह विस्तारित कनेक्टिविटी गोपनीयता उल्लंघनों, मैलवेयर इंजेक्शन और EV चार्जिंग प्रक्रियाओं में व्यवधान जैसी कमजोरियों का परिचय देती है। PES में ये भेद्यताएं ग्रिड स्थिरता, सुरक्षा और आपातकालीन सेवाओं के लिए महत्वपूर्ण जोखिम पैदा करती हैं, अंतिम अनुप्रयोगों पर उनके प्रतिकूल प्रभावों को कम करने के लिए PES को सुरक्षित करने के महत्व पर जोर देती हैं।

इस थीसिस में, महत्वपूर्ण आधारभूत संरचना साइबर सुरक्षा के लिए राष्ट्रीय मानक और प्रौद्योगिकी संस्थान (NIST) द्वारा प्रदान किए गए दिशानिर्देशों से प्रेरणा लेते हुए, डेटा अखंडता हमलों और डेटा उपलब्धता हमलों के खिलाफ PES की लचीलापन बढ़ाने पर प्राथमिक ध्यान केंद्रित किया गया है। इसके अतिरिक्त EVs को अपनाने के साथ PES की भेद्यता मूल्यांकन की भी जांच की जाती है। इस थीसिस में किए गए अध्ययनों में साइबर-भौतिक सह-सिमुलेशन परीक्षण के विकास से लेकर कमजोरियों का आकलन करने और नियंत्रण एल्गोरिदम को मान्य करने तक कई क्षेत्रों को शामिल किया गया है। इसके अलावा, जोखिम मूल्यांकन करने के लिए एक EV चार्जिंग इंफ्रास्ट्रक्चर टेस्टबेड विकसित किया गया है। यह मानक चार्जिंग प्रोटोकॉल का उपयोग करके EV को चार्ज करने के लिए एक यथार्थवादी वातावरण प्रदान करता है। ये टेस्टबेड प्रस्तावित एल्गोरिदम को सत्यापित करने के लिए एक मंच के रूप में भी कार्य करते हैं, जिससे सिस्टम की समग्र साइबर सुरक्षा मजबूत होती है। इसके अलावा, बड़े सिग्नल गड़बड़ी की उपस्थिति में PES के विश्वसनीय और सुरक्षित संचालन को सुनिश्चित करने के लिए AC और DC दोनों प्रणालियों के लिए

विसंगति निदान योजनाएं प्रस्तावित हैं। ये योजनाएँ चयनात्मक रिले संचालन के लिए ग्रिड दोषों और साइबर हमलों के बीच अंतर करने में सक्षम हैं। AC और DC दोनों प्रणालियों में विलंबता, डेटा ड्रॉपआउट और समय सिंक्रनाइज़ेशन हमलों (TSA) जैसे डेटा उपलब्धता हमलों को कम करने के लिए, सिमेंटिक सिद्धांतों को नमूनाकरण प्रक्रिया में एकीकृत किया गया है। इसके अलावा, रक्षक के दृष्टिकोण से, PES में DLAA के लिए एक रूपरेखा विकसित की गई है, विशेष रूप से दूरस्थ रूप से नियंत्रणीय और आवृत्ति-उत्तरदायी भार जैसे कमजोर भार के लिए। इसके अलावा, PES में एकीकृत EVs का एक सामान्य लघु-सिग्नल स्टेट-स्पेस मॉडल (SSM) प्रस्तुत किया गया है, जो DER तत्वों, नेटवर्क मापदंडों और साइबर ग्राफ टोपोलॉजी के बीच गतिशील परस्पर क्रिया को उजागर करता है। अध्ययन में चार्जिंग से इनकार (DoC) हमले पर भी प्रकाश डाला गया है, जो इलेक्ट्रिक वाहनों (EVs) की चार्जिंग प्रक्रिया को बाधित करता है। इस हमले को प्रदर्शित करने के लिए भारत ईवी डीसी चार्जिंग मानक (BEVDC – 001) पर आधारित एक वास्तविक हार्डवेयर सेटअप का उपयोग किया जाता है, जो ईवी चार्जर और ईवी के बीच संचार के लिए नियंत्रक क्षेत्र नेटवर्क (सीएएन) बस का लाभ उठाता है। प्रस्तावित दृष्टिकोणों और अवधारणाओं को मान्य करने के लिए रीयल-टाइम सिमुलेशन केस स्टडीज आयोजित की जाती हैं। निष्कर्ष PES साइबर सुरक्षा जांच के लिए मजबूत और साइबर-सुरक्षित डिजाइन के विकास में योगदान करते हैं, अंतर्दृष्टि प्रदान करते हैं और इस क्षेत्र में भविष्य के शोध का मार्ग प्रशस्त करते हैं।

मुख्य शब्द: विसंगति निदान, साइबर सुरक्षा, साइबर हमले, डेटा अखंडता हमले, डेटा उपलब्धता हमले, चार्जिंग हमले से इनकार (DoC), गतिशील भार परिवर्तन हमले (DLAAs), इलेक्ट्रिक वाहन बुनियादी ढांचे (EVI), दोष, छोटे सिग्नल मॉडलिंग।

Contents

Certificate	i
Acknowledgement	ii
Abstract	iii
Contents	vii
List of Figures	xii
List of Tables	xxi
List of Symbols	xxiii
List of Abbreviations	xxiv
1 Introduction	1
1.1 Motivation of the Work	1
1.1.1 Background	1
1.1.2 Real world Cyber Incidents	1
1.2 Cyber-Physical Power Electronic Systems (PES)	3
1.3 Vulnerabilities in PES	3
1.4 Guidelines for Cybersecurity	3
1.5 Existing Research Work and Major Research Gaps	5
1.5.1 Development of Testbeds for Vulnerability Assessment	5
1.5.2 Anomaly Diagnosis for Power Electronic Interfaced AC Systems	6
1.5.3 Anomaly Diagnosis for Power Electronic Interfaced DC Systems	7
1.5.4 Mitigation of Delay-Based Attacks for Power Electronic Interfaced Systems	7

1.5.5	Dynamic Load Altering Attacks (DLAAs) Against Power-Electronic Interfaced AC System	8
1.5.6	Electric Vehicle Charging Infrastructure	8
1.5.7	Major Research Gaps Summarized	9
1.6	Thesis Objectives	10
1.7	Assumptions Considered in the Research Work	11
1.8	Brief Overview of the Research Work	11
1.8.1	Development of Testbeds for Vulnerability Assessment	11
1.8.2	Anomaly Diagnosis for Power Electronic Interfaced AC Systems	12
1.8.3	Anomaly Diagnosis for Power Electronic Interfaced DC Systems	13
1.8.4	Mitigation of Delay-Based Attacks for Power Electronic Interfaced Systems	14
1.8.5	Dynamic Load Altering Attacks (DLAAs) Against Power-Electronic Interfaced AC System	15
1.8.6	Electric Vehicle Charging Infrastructure	15
1.8.7	Major Contributions Summarized	16
1.9	Thesis Organization	17
2	Development of Testbeds for Vulnerability Assessment	19
2.1	Co-simulation Testbed at IIT Delhi	19
2.1.1	Introduction	19
2.1.2	Description of Various Layers of Microgrid (MG) Ecosystem	21
2.1.3	Applications of Testbed	21
2.1.4	Features of Testbed	23
2.1.5	Vulnerability Assessment	26
2.2	Electric Vehicle Charging Infrastructure Testbed at IIT Delhi	28
2.2.1	Introduction	28
2.2.2	Description of Various Layers of Electric Vehicle (EV) Ecosystem	29
2.2.3	Applications of Testbed	31
2.2.4	Features of Testbed	31
2.2.5	Vulnerability Assessment	38
2.2.6	Conclusions	40
3	Anomaly Diagnosis for Power Electronic Interfaced AC Systems	41
3.1	Introduction	41
3.2	Cyber-Physical Modeling of AC System	42
3.2.1	Physical Framework	42
3.2.2	Cyber Framework	43

3.3	False Data Injection Attack (FDIA) Modeling	44
3.4	Impact Analysis of Faults and FDIAs	45
3.5	Proposed Non-Invasive Anomaly Diagnosis Scheme	46
3.6	Results and Discussion	49
3.6.1	Responses for the Modified CIGRE LV Benchmark System	49
3.6.2	Responses for the Modified IEEE 37-Bus AC Distribution System	52
3.7	Hardware Implementation	55
3.8	Features of the Proposed Scheme	56
3.9	Conclusions	57
4	Anomaly Diagnosis for Power Electronic Interfaced DC Systems	58
4.1	Anomaly Diagnosis for MVDC Shipboard Systems	58
4.1.1	Introduction	58
4.1.2	Cyber-Physical Modeling of MVDC System	59
4.1.3	Problem Statement	63
4.1.4	Proposed Local Trajectory Mapping Based Anomaly Diagnosis Scheme	64
4.1.5	Results and Discussion	69
4.2	Cyber Intrusion Detection for Line Current Differential Relays	74
4.2.1	Introduction	74
4.2.2	Problem Formulation	74
4.2.3	Revisiting the Available Superimposed Current Based Unit Protection Scheme	78
4.2.4	Fault Analysis	78
4.2.5	Cyber-Intrusion Analysis	79
4.2.6	Proposed Cyber-Intrusion Detection Scheme	82
4.2.7	Performance Evaluation	85
4.2.8	Conclusions	90
5	Mitigation of Delay-Based Attacks for Power Electronic Interfaced Systems	91
5.1	Delay Mitigation in Power-Electronic Interfaced AC Systems	91
5.1.1	Introduction	91
5.1.2	Science and Relevance of Semantics	92
5.1.3	Modeling Preliminaries	93
5.1.4	Modeling of Data Availability Attacks	94
5.1.5	Proposed Delay-Aware Semantic Sampling Scheme	96
5.1.6	Performance Evaluation	99
5.2	Delay Mitigation in MVDC Shipboard Systems	112
5.2.1	Introduction	112

5.2.2	Modeling Preliminaries	112
5.2.3	Proposed Model-Agnostic Estimator Scheme	114
5.2.4	Performance Evaluation	116
5.2.5	Conclusions	118
6	Dynamic Load Altering Attacks (DLAAs) Against Power-electronic Interfaced AC System	120
6.1	Introduction	120
6.2	Description of DLAAs	121
6.3	Small-Signal State Space Modeling of PES	122
6.3.1	Inverter Modeling	122
6.3.2	Network Modeling	124
6.3.3	Load Modeling	124
6.3.4	Droop-controlled MG Model involving Load Dynamics	128
6.3.5	Complete MG Model with Distributed Secondary Control (DSC) involving Load Dynamics	129
6.4	Adversarial Model: Least-Effort DLAAs using Parametric Sensitivity	130
6.5	Results and Discussion	133
6.6	Conclusions	136
7	Electric Vehicle Charging Infrastructure	137
7.1	Small-Signal State-Space Model for EV Integrated PES	137
7.1.1	Introduction	137
7.1.2	Preliminaries	138
7.1.3	Distributed Energy Resource (DER) Modeling	140
7.1.4	Network modeling	145
7.1.5	Load modeling	145
7.1.6	Complete Microgrid (MG) Model	152
7.1.7	System Under Study	154
7.1.8	Performance Evaluation	155
7.2	Demonstration of Denial of Charging (DoC) Attack and Its Consequences	161
7.2.1	Introduction	161
7.2.2	Vulnerabilities	162
7.2.3	Communication Protocol Under Study in Detail	163
7.2.4	Demonstration of DoC Attack	165
7.2.5	Results and Discussion	166
7.2.6	Consequences of DoC Attack	172
7.2.7	Disruption of Charging and Transportation Services	172

7.2.8	Economic Impacts	172
7.2.9	Over Frequency Excursion in Microgrid (MG)	172
7.2.10	Conclusions	175
8	Conclusions and Future Scopes	177
	References	181
	Appendix	201
	List of Publications	208
	Author's Biography	211

List of Figures

1.1	NIST cybersecurity framework [22].	4
2.1	Test MG with four DERs.	22
2.2	Co-simulation testbed for MG cybersecurity.	22
2.3	Message exchanges on Wireshark.	23
2.4	Real-time simulation results on HYPERSIM with load change at 2 s, FDIA initiated at 5 s with small value and increased to unfair value at 8 s (a) frequency restoration; (b) proportional active power sharing; (c) proportional reactive power sharing; and (d) voltage across buses.	24
2.5	Communication protocols available in MG Testbed.	25
2.6	Attack pathways in a MG CPS.	26
2.7	Pin configuration in (a) AC and (b) DC chargers.	29
2.8	Testbed for EV charging infrastructure.	32
2.9	Protocols available in EV charging testbed.	33
2.10	Connection diagram for insulation resistance emulation.	33
2.11	EV test mode during DC charging.	34
2.12	EVSE test mode during DC charging.	34
2.13	MitM test mode during DC charging.	35
2.14	Variation of different parameters for EV test mode during AC charging over IEC 61851-1:2010 standard obtained through CDS.	36
2.15	Message exchanges during EV test mode during AC charging obtained through CDS.	36
2.16	Variation of different parameters for EV test mode during DC charging over DIN SPEC 70121:2014-12 standard obtained through CDS.	37
2.17	Few message exchanges during EV test mode during DC charging obtained through CDS.	37
2.18	Attack pathways in a EV charging infrastructure.	39

3.1	An exemplary two-bus cyber-physical system with two DERs, equipped with high-fidelity protection and monitoring systems.	42
3.2	Time domain simulation of current for a cycle with various cyber-physical anomalies at DER A of a two-bus test system (Figure. 3.1).	45
3.3	Cyber-physical anomaly diagnosis mechanism (CP-ADM) for DERs. . . .	48
3.4	Modified CIGRE LV islanded distribution system (in dashed section). . . .	50
3.5	Testbed for real-time simulation to evaluate the performance of the proposed scheme – the modeling and control schematic of one DER interacting with the cyber layer is highlighted. This DER model can be integrated into the benchmark systems in Figure. 3.4 and 3.7.	51
3.6	Trajectories captured for voltage and frequency deviation at DER A for modified CIGRE LV distribution system within 5 ms.	51
3.7	Modified IEEE 37-bus islanded AC distribution system.	52
3.8	Trajectories of voltage and frequency deviation at DER A for bus fault at B15 (solid lines) and line fault between B14 and B15 (dashed lines) for modified IEEE 37-bus AC distribution system for W1 at DER A in Figure. 3.7. . . .	53
3.9	Trajectories of voltage and frequency deviation at DER A for LLLG fault at B 15 with different R_f for modified IEEE 37-bus AC distribution system for W1 in Figure. 3.7.	53
3.10	Trajectories of voltage and frequency deviation at DER A at different loading conditions for modified IEEE 37-bus AC distribution system for W1 in Figure. 3.7.	53
3.11	Trajectories of voltage and frequency deviation at DER A at different loading conditions for modified IEEE 37-bus AC distribution system for W1 in Figure. 3.7.	54
3.12	Trajectories of voltage and frequency deviation at DER A with V_{sec} attack at DER A and LLLG fault between B11 and B33 for modified IEEE 37-bus AC distribution system for W1 in Figure. 3.7.	54
3.13	Trajectories of voltage and frequency deviation at DER A with SNR of 30 dB for modified IEEE 37-bus AC distribution system for W1 in Figure. 3.7.	54
3.14	Experimental prototype of the system topology in Figure. 3.1	55
3.15	(a) Voltage of DER A during the emulated fault, (b) voltage of DER A during the cyber-attack in the experimental prototype—a buffer time of 0.05 s was given for the decision by the trajectory monitor in (c) for a sampling frequency of 100 Hz for the relay signals. Finally, a decision schematic has been shown in (d) to distinguish between cyber-attacks and faults using the proposed trajectory monitor and the corresponding action in each case. . . .	56

4.1	(a) A notional 12 kV four zone MVDC SPS with four PGMs, with installed monitoring and protection devices for reliable operation of the system; and (b) block diagram of cyber-physical PGM.	60
4.2	$K_d\Delta t$ for PGM 2 (as shown in the Figure. 4.1(a)) for allowable load changes.	63
4.3	$K_d\Delta t$ for PGM 1 (as shown in the Figure. 4.1) for (a) fault on bus B1 (b) fault on the cable section CS9; (c) cyber-attack on voltage correction term.	64
4.4	Fault current for a short circuit fault at B1 (connected to PGM1) at 0.1 s.	65
4.5	Timescale range for critical events and the protection system requirements in MVDC SPS—the <i>timeliness</i> of the proposed anomaly diagnosis scheme is quite vital.	66
4.6	A novel anomaly diagnosis scheme for MVDC SPSs—locally observed trajectories segregate between the anomalies with cyber-attacks in Q I and III and faults in Q IV.	68
4.7	A real-time simulation testbed with notional 12 kV four zone MVDC SPS powered by four PGMs.	69
4.8	Trajectories of deviation in current and voltage at PGM 1 for fault on both bus B1 (solid green line) and cable section CS9 (dashed green line) lie in Q I; and for $+\Delta V$ attack and $-\Delta V$ attack lie in Q I and Q III respectively.	70
4.9	Trajectories of deviation in current and voltage at PGM 1 for bus fault at B1 with different values of R_f lie only in the fault region (Q IV).	70
4.10	Trajectories of deviation in current and voltage at all PGMs for load variations at the PMM load in Z2.	71
4.11	Trajectories of deviation in current and voltage at all PGMs are shown. The trajectory for PGM 1 (corresponding to bus fault at B1) lies in Q IV and trajectories for PGM 3 (corresponding to $-\Delta V$ attack lies in Q III.	71
4.12	Trajectories of deviation in current and voltage at PGM 1 (in presence of noise) for fault on both bus B1 (solid green line) and cable section CS9 (dashed green line) lie in Q I; and for $+\Delta V$ attack and $-\Delta V$ attack lie in Q I and Q III respectively.	72
4.13	Integration of the proposed scheme between the sensing circuitry and IED logic circuit.	72
4.14	Control structure of a converter in DC distribution system.	75
4.15	Modified IEEE 37-bus DC distribution system with seven converters.	75
4.16	Vulnerabilities in LCDR.	76
4.17	Remote end attack occurred at 0.1 s (a) current seen by LCDR; (b) current difference computed by LCDR.	77
4.18	Various cases of faults and cyber-attacks on LCDR installed line segment.	78

4.19	Current for fault F1, measured by CT at (a) bus 1; and (b) bus 2.	79
4.20	The currents seen by the LCDR during (a) fault; (b) remote end attack; (c) both end attack. Further, the current difference computed by the LCDR during (d) fault; (e) remote end attack; and (f) both end attack.	80
4.21	Plane for superimposed currents at local and remote end for a line segment.	81
4.22	Variation in angle of slope between superimposed currents at local and remote end for a line segment during different cases.	83
4.23	Flowchart for the proposed scheme.	84
4.24	Tripping logic with the proposed scheme.	84
4.25	Fault occurred at 0.1 s and $L_f = 0.5$ with $R_f = 0.1\Omega$ (a) currents seen by the LCDR; (b) current difference computed by the LCDR; (c) superimposed components of current at local and remote end of the line segment; (d) angle of slope between the superimposed current components; and (e) status of trip signal.	85
4.26	Distinct fault cases (a) angle of slope between the superimposed current components for fault length of 10%, 90% from Bus B1 and high resistance fault ($R_f = 15\Omega$); and (b) status of trip signal.	86
4.27	Remote end attack at 0.1 s (a) current seen by the LCDR; (b) current difference computed by the LCDR; (c) angle of slope between the superimposed current components; and (d) status of trip signal.	86
4.28	Both end attack at 0.1 s (a) current seen by the LCDR; (b) current difference computed by the LCDR; (c) angle of slope between the superimposed current components; and (d) status of trip signal.	87
4.29	During overloading (by 25%) at 0.1 s (a) current seen by the LCDR; (b) current difference computed by the LCDR; and (c) status of trip signal. . . .	88
4.30	During switching event at 0.1 s (a) current seen by the LCDR; (b) current difference computed by the LCDR; and (c) status of trip signal.	88
4.31	Distinct fault cases with addition of WGN to make the SNR of 50 dB and 40 dB for i_1 and i_2 respectively, (a) angle of slope between the superimposed current components for fault length (L_f) of 10%, 90% from Bus B1 and high resistance fault ($R_f = 15\Omega$); and (b) status of trip signal.	89
4.32	Remote end attack occurred at 0.1 s with addition of WGN (a) angle of slope between the superimposed current components; and (b) status of trip signal.	89
5.1	Semantic information exchange and estimation in PES – sparse event-driven sampling from local error measurements steer the estimation and reconstruction process during latency attack/data dropout/TsAs.	93

5.2	(a) The modified IEEE 37-bus islanded AC distribution system powered by seven DERs is shown. (b) The block diagram of cyber-physical DER with primary and DSC architecture is presented. The DSC receives local measurements (σ_j) and neighbouring measurements (σ_m) as input to generate frequency and voltage correction terms ($\Delta\omega$ and ΔV). Note that the MUs receive the timing information from GPS satellite. These time-stamped measurements are then used by the controllers for generating control signals, which can directly affect the control operation of the system.	94
5.3	(a) Latency attack and data dropout; and (b) TSA.	96
5.4	Proposed delay-aware semantic sampling scheme.	98
5.5	Real-time simulation testbed with Ethernet interface to facilitate establishment of IEC 61850 sampled values protocol.	100
5.6	Time-domain signals during latency attack ($\tau_m=0.05$ s), without the proposed scheme for (a) phase voltage of DER 1; (b) frequency for all DERs; (c) active power sharing for all DERs; and (d) reactive power sharing for all DERs.	101
5.7	Time-domain signals during latency attack ($\tau_m=0.05$ s), with the proposed scheme for (a) phase voltage of DER 1; (b) frequency for all DERs; (c) active power sharing for all DERs; and (d) reactive power sharing for all DERs.	101
5.8	The time-domain signals during latency attack ($\tau_m=0.05$ s) and 10% data dropout for (a) frequency; (b) active power sharing; (c) reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for (d) frequency; (e) active power sharing; (f) reactive power sharing, with the proposed scheme are shown.	102
5.9	The time-domain signals during TSA for (a) frequency; (b) active power sharing; (c) reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for (d) frequency; (e) active power sharing; (f) reactive power sharing, with the proposed scheme are shown.	103
5.10	The cyber graphs (G) considered are (a) G1: fully-connected graph; and (b) G2: ring-connected graph.	103
5.11	The time-domain signals during latency attack ($\tau_m=0.05$ s) with cyber graph variations for (a) frequency; (b) active power sharing; (c) reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for (d) frequency; (e) active power sharing; (f) reactive power sharing, with the proposed scheme are shown.	104

5.12	Plots of time of convergence (T_c) for (a) O1; and (b) O2, without and with the deployment of the proposed scheme.	105
5.13	Plots of steady-state error with different attack cases for (a) O1; and (b) O2, without the proposed scheme.	105
5.14	Plots of steady-state error with different attack cases for (a) O1; and (b) O2, with the proposed scheme.	105
5.15	The time-domain signals during latency attack ($\tau_m=0.05$ s) with cyber graph variations for (a) d -axis error signals input to VC, e_1^{dVC} ; (b) process-aware sparsely sampled d -axis error signals input to VC, e_1^{dD} ; (c) reconstructed signal input to SC, $e_1^{p\varphi}$; (d) q -axis error signals input to VC, e_1^{qVC} ; (e) process-aware sparsely sampled q -axis error signals input to VC, e_1^{qD} ; and (f) reconstructed signal input to SC, $e_1^{q\varphi}$	106
5.16	Plots for variation in T_c for attaining O1 and O2 with variations in (a) down-sampling factor (D); and (b) amount of delay (τ_m).	107
5.17	The time-domain signals during data loss of 10 packets for (a) frequency; (b) active power sharing; and (c) reactive power sharing, with the proposed scheme are shown. Further, the time-domain signals showing data loss of 10 packets in the communicated signals i.e, (d) frequency; (e) active power; and (f) reactive power, over IEC 61850 sampled values protocol are presented.	107
5.18	Details of IEC 61850 sampled values packet comprising of svID, values of communicated signals etc.	108
5.19	(a) South California Edison's (SCE's) Distributed Energy Resource Inter-connection Map (DERiM) [193]; (b) real-world SCE 47-bus network with five DERs [192] and; (c) cyber topologies T1 and T2.	109
5.20	The time-domain signals during balanced FDIA for (a) frequency; (b) active power sharing; (c) reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for (d) frequency; (e) active power sharing; (f) reactive power sharing, with the proposed scheme are shown.	110
5.21	The time-domain signals during unbalanced FDIA for (a) frequency; (b) active power sharing; (c) reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for (d) frequency; (e) active power sharing; (f) reactive power sharing, with the proposed scheme are shown.	111
5.22	(a) A notional 12 kV two-zone MVDC SPS with two PGMs; and (b) block diagram of cyber-physical PGM.	113
5.23	Proposed MAE scheme.	115

5.24	A real-time simulation testbed with notional 12 kV two-zone MVDC SPS powered by two PGMs.	116
5.25	Time-domain signals during latency attack, without the proposed scheme for (a) average voltage; (b) current; and with the proposed scheme for (c) average voltage and (d) current, received at PGM 1.	117
5.26	Time-domain signals during latency attack and data dropouts, without the proposed scheme for (a) average voltage; (b) current; and with the proposed scheme for (c) average voltage and (d) current, received at PGM 1.	117
5.27	Time-domain signals during TSA, without the proposed scheme for (a) average voltage; (b) current; and with the proposed scheme for (c) average voltage and (d) current, received at PGM 1.	118
6.1	Illustration of single-point closed-loop DLAA (P_L is the load power altered by the attacker).	122
6.2	Block diagram of complete small-signal state-space model of a MG with closed-loop DLAA.	123
6.3	Cyber graph topologies (a) spanning tree (T1); (b) partially-connected (T2); and (c) fully-connected (T3).	129
6.4	Modified IEEE 37-bus AC distribution system with seven inverter-interfaced resources.	133
6.5	Eigenvalue spectrum of the system (a) during no attack; and (b) during single-point DLAA for ERL.	134
6.6	Frequency response for DLAA on modified IEEE 37-bus AC distribution system with ERL ($K_{5,19}^{a*} = 0.4147$).	134
6.7	$\ K_{s,v}^{a*}\ $ for different combinations of sensing nodes and vulnerable loads with ERL integrated system.	134
6.8	$\ K_{s,v}^{a*}\ $ for frequency dependent loads corresponding to (a) ERL; (b) ZIP load ($a_0 = a_1 = a_2 = 0.33$); and (c) CL, with and without SC.	135
6.9	$\ K_{s,v}^{a*}\ $ for frequency dependent and independent loads corresponding to ERL; ZIP load ($a_0 = a_1 = a_2 = 0.33$); and composite load, for different topologies.	135
6.10	Attack effort for frequency dependent ($A_\omega = 1$) loads corresponding to (a) ERL ($\ K_{5,19}^{a*}\ = 0.4053$); (b) ZIP load ($a_0 = a_1 = a_2 = 0.33$) ($\ K_{5,19}^{a*}\ = 0.4116$); and (c) composite load ($\ K_{5,19}^{a*}\ = 0.2448$), with deviations in SC gains.	135
7.1	Conventional structure of an autonomous MG with DSC framework with distinct load types.	138

7.2	Block representation of overall SSM of an autonomous MG with DSC architecture.	139
7.3	Block representation of DER.	140
7.4	Power controller.	141
7.5	DSC architecture.	142
7.6	Inner loop controllers.	142
7.7	(a) Block representation of overall SSM of an EVI load in autonomous MG with DSC architecture; and (b) Internal SSM of an EVI.	147
7.8	Block representation of an EVI.	147
7.9	DC-DC current control.	148
7.10	DC link voltage regulator.	149
7.11	Inner current control loop.	150
7.12	Test MG system.	154
7.13	Real-time simulation setup.	154
7.14	Eigenvalue spectrum with (a) R loads; (b) RL loads and (c) EVI loads. . . .	155
7.15	Zoomed complex plane to locate eigenvalues highly contributing to SC states with (a) R loads; (b) RL loads and (c) EVI loads.	156
7.16	Trajectory of low-frequency modes as a function of real power droop gain: $1.57e^{-5} \leq m_p \leq 3.14e^{-4}$ with (a) R loads; (b) RL loads; and (c) EVI loads.	156
7.17	Trajectory of low-frequency modes as a function of reactive power droop gain: $3.17e^{-4} \leq n_q \leq 4.8e^{-3}$ with (a) R loads; (b) RL loads; and (c) EVI loads.	157
7.18	Cyber graph topologies (a) T1: sparse graph; and (b) T2: fully-connected (ring) graph.	158
7.19	Trajectory of low-frequency modes with T1 with EVI loads, as a function of SC integral gain (a) $1 \leq K_{i\omega} \leq 100$; and (b) $1 \leq K_{iv} \leq 100$	158
7.20	Trajectory of low-frequency modes with T2 with EVI loads, as a function of SC integral gain (a) $1 \leq K_{i\omega} \leq 100$; and (b) $1 \leq K_{iv} \leq 100$	159
7.21	Time-domain simulation for change in active power droop gain from $1.57e^{-5}$ to $3e^{-4}$ of all DERs at 10 s for (a) frequency; (b) proportional active power sharing; and (c) proportional reactive power sharing.	159
7.22	Vulnerabilities in EV charging infrastructure.	162
7.23	CHM with BEV DC-001 charging standard.	162
7.24	CAN messages decoding setup.	164
7.25	Implementation of denial of service attack.	165
7.26	Experimental setup.	165

7.27	Details of the experimental arrangement to create a new node in order to launch DoC attack.	166
7.28	CAN packets captured over CAN bus analyzer software.	167
7.29	Fabricated CST message captured over CDS.	167
7.30	Decoded fabricated CST message over CDS.	168
7.31	Messages on HMI panel of DC charger (a) before DoC attack; (b) after DoC attack.	168
7.32	Message popped on EV dashboard (a) before DoC attack; (b) after DoC attack.	168
7.33	Fabricated CRM message captured over CDS.	169
7.34	Decoded fabricated CRM message over CDS.	169
7.35	Message popped on the HMI panel of DC charger with an attack on the CRM message.	169
7.36	Fabricated CEM message captured over CDS.	170
7.37	Decoded fabricated CEM message over CDS.	171
7.38	Message popped on the HMI panel of DC charger with an attack on the CEM message.	171
7.39	Real time co-simulation testbed for autonomous MG system integrated with EV loads.	173
7.40	Frequency excursion observed in the test MG system when DoC attack initiated at 50 s.	173

List of Tables

2.1	Signal states of control pilot	30
3.1	Anomaly characteristics for events at DER^i	48
3.2	Comparative evaluation of the proposed anomaly diagnosis mechanism for DERs.	57
4.1	Key Characteristics of cyber-physical anomalous events at j^{th} PGM.	69
4.2	Features of the proposed scheme.	72
4.3	Key differences between fault and FDI attack	81
4.4	Variation in parameters during remote end attack	87
4.5	Variation in parameters during both end attack	87
4.6	Comparative assessment of the proposed cyber intrusion detection scheme for LCDRs.	90
5.1	Features of the delay-aware semantics scheme.	109
5.2	Features of the proposed MAE scheme.	118
7.1	Elements of connection matrix	152
7.2	Sensitivity of low frequency dominant modes	157
7.3	Comparative assessment	174
A.1	Network and load data of microgrid (MG) test system in Figure 3.1.	201
A.2	Parameters of DERs in MG test system in Figure 3.1.	201
A.3	Parameters for modified CIGRE LV distribution system in Figure 3.4.	202
A.4	Control parameters of DERs in IEEE 37-bus AC distribution system.	202
A.5	Control parameters of DERs in Figure 3.14.	203
A.6	Parameters for notional 12 kV MVDC SPS in Figure 4.1.	203
A.7	Parameters for modified IEEE 37-bus DC distribution system in Figure 4.15.	204
A.8	Parameters for real-world SCE 47-bus distribution system	204

A.9 Parameters for notional 12 kV MVDC SPS in Figure 5.22.	205
A.10 Test system parameters	205

List of Symbols

i, j, m	Index of agents in PES
N_j	The set of neighbouring agents to j^{th} agent
ω_j & f_j	Frequency (in rad/s & Hz) of j^{th} agent
m_j^p & n_j^q	Active & reactive power droop coefficient of j^{th} agent
P_j & Q_j	Active & reactive power of j^{th} agent
R_f	Fault resistance
R_{jm} & X_{jm}	Tie-line resistance & reactance between j^{th} and m^{th} DER
ω_j^*	Local reference frequency of j^{th} DER
V_j^{d*} & V_j^{q*}	Local reference d & q-axis voltage of j^{th} DER
ω_{nom} & V_{nom}	Nominal frequency & voltage of the system
E	Edge connecting agents
L , D_{in} & A_G	Laplacian matrix, Incoming information matrix & Adjacency matrix
$\Delta\omega_{secj}$ & ΔV_{secj}	Frequency & voltage correction term from SC of j^{th} agent
g_j	Convergence parameter of j^{th} agent
a_{jm}	Communication weight
σ_m	Information received from m^{th} agent
V_j^* & $\bar{V}_j^{dc}$	Local reference voltage & average voltage of j^{th} PGM
R_j^{vir}	Droop gain of j^{th} PGM
φ	Threshold value for protection system
D	Downsampling factor
τ_m	Time delay from m^{th} agent
F and R	Freshness and relevance
k_1 and k_2	Tunable gains
t_a	Triggering moment
Other notations are defined in the chapters.	

List of Abbreviations

BMS	Battery Management System
BHM	BMS Handshake Message
BRM	BMS Recognition Message
BEV DC-001	Bharat EV DC charging standard
CMS	Central Management System
CHAdemo	CHArge de MOve
CEM	Charger Error Message
CHM	Charger Handshake Message
CRM	Charger Recognition Message
CST	Charger Suspending Charging
CDS	Charging Discovery System
CB	Circuit Breaker
CCS	Combined Charging System
CL	Communication Link
CL	Composite Load
CIA	Confidentiality, Integrity and Availability
CP	Control Pilot
CAN	Controller Area Network
CI	Coupling Inductor
CC	Current Controller
CPS	Cyber Physical System
DLC	Data Length Code
DSM	Demand Side Management
DoC	Denial of Charging
DoS	Denial of Service
DDoC	Distributed Denial of Charging

DHS	Department of Homeland Security
DLC	Direct Load Control
DER	Distributed Energy Resource
DNP 3	Distributed Network protocol 3
DSC	Distributed Secondary Controller
DLAA	Dynamic Load Altering Attack
DOE	Department of Energy
EV	Electric Vehicle
EV/XFC	Electric Vehicle Extreme Fast Charging
EVI	Electric Vehicle Infrastructure
EVSE	Electric Vehicle Supply Equipment
ENCS	European Network for Cyber Security
ERL	Exponential Recovery Load
FDIA	False Data Injection Attack
FPL	Florida Power & Light Co.
GOOSE	Generic Object-Oriented Substation Event
GNSS	Global Navigation Satellite Signals
GPS	Global Positioning System
G2V	Grid-to-Vehicle
HMI	Human Machine Interface
IM	Induction Machine
ICS	Industrial Control System
ICT	Information and Communication Technology
IT	Information Technology
IED	Intelligent Electronic Device
IoT	Internet of Things
IRIG-B	Inter-Range Instrumentation Group Time Code B
LCDR	Line Current Differential Relay
LCF	LC Filter
LAA	Load Altering Attack
LC	Local Controller
MitM	Man-in-the-Middle

MC	Master Controller
MEO	Medium Earth Orbit
MVDC	Medium Voltage DC
MU	Merging Unit
MG	Microgrid
MAE	Model-Agnostic Estimator
NCCoE	National Cybersecurity Center of Excellence
NISTIR	National Institute of Standards and Technology Internal Reports
1PPS	One Pulse Per Second
OCV	Open Circuit Voltage
OT	Operational Technology
OCR	Overcurrent Relay
PMA	Packet Mistreatment Attack
PGN	Parameter Group Number
POC	Passive Oscillator Circuit
PLL	Phase Locked Loop
PGCIL	Power Grid Corporation of India Limited
PTP	Precision Time Protocol
PC	Primary Controller
PE	Protective Earth
PES	Power Electronic System
PGM	Power Generation Module
PI	Proportional-Integral
PP	Proximity Pilot
PWM	Pulse Width Modulation
RFID	Radio-Frequency IDentification
RTAC	Real-Time Automation Controller
RLDC	Regional Load Dispatch Centre
RMS	Root Mean Square
RTP	Routing Table Poisoning
TSA	Time Synchronization Attack
VC	Voltage Controller

VSI	Voltage Source Inverter
VIN	Vehicle Identification Number
V2G	Vehicle-to-Grid
Wi-Fi	Wireless Fidelity
SV	Sampled Value
SC	Secondary Controller
SPS	Shipboard Power System
SSM	Small-signal state-space model
SoC	State of Charge
SLAA	Static Load Altering Attack
TSA	Time Synchronization Attack
VC	Voltage Controller
VSI	Voltage Source Inverter
VIN	Vehicle Identification Number
V2G	Vehicle-to-Grid
Wi-Fi	Wireless Fidelity