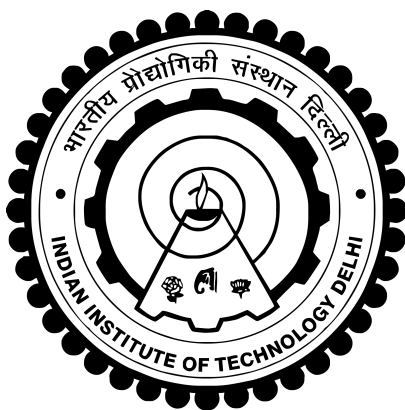


**RESILIENT DISTRIBUTED SECONDARY CONTROLS
FOR DC AND AC MICROGRIDS AGAINST
CYBER-ATTACKS**

A DEVAKUMAR



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

JUNE, 2025

© Indian Institute of Technology Delhi (IITD), New Delhi, 2025

RESILIENT DISTRIBUTED SECONDARY CONTROLS FOR DC AND AC MICROGRIDS AGAINST CYBER-ATTACKS

by

A DEVAKUMAR

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of requirements of degree of Doctor of Philosophy

to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

JUNE, 2025

I dedicate this thesis to my loving family.

CERTIFICATE

This is to certify that the thesis entitled ‘**RESILIENT DISTRIBUTED SECONDARY CONTROLS FOR DC AND AC MICROGRIDS AGAINST CYBER-ATTACKS**’, being submitted by **A DEVAKUMAR** to **Indian Institute of Technology Delhi** is a record of bonafide research work carried out under my supervision and I consider it worthy for consideration of the award of the degree **Doctor of Philosophy** in Electrical Engineering. The results obtained here have not been submitted to any other University or Institute for the award of any degree or diploma.

Prof. Sukumar Mishra

Department of Electrical Engineering,

Indian Institute of Technology Delhi,

New Delhi - 110016, India.

Date:

Acknowledgments

I am deeply grateful to my supervisor, Prof. Sukumar Mishra, for his invaluable support, guidance, and encouragement throughout my research. His insights and mentorship at each stage have been instrumental in fostering both my personal and professional growth. His directions and encouragement to develop hardware testbeds refined my technical and analytical skills, elevating the quality of this thesis and improving my ability to convey complex ideas clearly in presentations and technical papers. His trust in my abilities empowered me to engage with challenging research work, driving my growth in innovative ways. As I conclude this chapter, I carry forward the lessons and inspiration he imparted, which will undoubtedly guide me in future pursuits.

I sincerely thank my doctoral research committee members, Prof. Nilanjan Senroy, Prof. Shubendu Bhasin, and Prof. Ashu Verma, for their invaluable guidance and feedback, shaping my research direction. I thank esteemed teachers like Prof. B. K. Panigrahi, Prof. A R Abhayankar, Prof. Santanu Kapat, and Dr. S S Nag for enriching my coursework.

I extend my heartfelt gratitude to my seniors, Dr. Deepak Pullaguram and Dr. Subham Sahoo, for all the support and research collaborations. A lot of learning from these two people made my research more impactful. I extend my thanks to Prof. Jimmy Chih-Hsien Peng of NUS and Prof. Tomislav Dragicevic of DTU for allowing me to include our joint work in this thesis. I extend my sincere thanks to Dr. Sreedhar Madichetty for all his support during my initial days at IIT Delhi.

I also thank the Ministry of Human Resource Development (MHRD), Government of India, for providing financial support through a research fellowship to complete the Doctoral program at IIT Delhi.

I am very grateful to my seniors Dr. Dushyant Sharma, Dr. Shivraman, Dr. Surya Prakash, Dr. Rishikant Sharma, Dr. Ayesha Firdaus, Dr. Rubi Rana, Dr. Arpan, Dr. Dhiman and Dr. Vaibhav Nougain in our lab and had great working and learning experience with them. Special thanks to my senior, Dr. Abhishek Nayak, for all the support being as a friend and brother for all these days. Special thanks to fellow researchers and friends Manas Ranjan Mishra, Kalyan Dash, Utkarsh Kumar, Debi Prasad Nayak, Ravi Kumar Yakala, Sankar Rao, Subhasish Nayak, Himanshu Sahoo,

Anyuti Tiwary, Vineeth Patil, Shivam Garg, Pritha Paithandy, Gaurav Prit, Sirsendu, Venu Gopal, Anil Yadav, Sagar and many others. Their friendship created an environment filled with collaboration, encouragement, and inspiration, making my time at IIT Delhi a genuinely memorable experience.

I extend my thanks to the IIT Delhi PG section and the electrical engineering department administrative staff, especially Mr. Yatindra Tripathi and Mr. Satish, for all their support during all these years.

I am profoundly grateful to my parents, Mrs. Sujatha and Mr. Ramachandraiah, my sister, Mrs. Revathi, my brother, Mr. Manoj Kumar, and their families, whose unwavering support, sacrifices, and belief drive my academic journey. I extend my sincere thanks to Mrs. Shakuntala Mishra for all her support during my IIT days. I offer my deepest gratitude to Lord Venkateswara Swamy for his constant light and guidance, especially during uncertain moments. His divine presence restored my strength and faith whenever I faltered, making this journey possible through his grace.

— A Devakumar

Abstract

Hierarchical controllers for direct current (DC) microgrids and alternating current (AC) microgrids have gained popularity due to their layer-wise control structure. Distributed controllers at the secondary layer of these microgrids, using distributed communication, enable voltage and frequency restoration along with proportional power-sharing. Distributed controlled microgrids are highly subjected to cyber-attacks due to the sensor feedback and distributed communication. Though cyber-attacks are a low-probability event in the distributed controlled microgrids, they significantly disrupt microgrid operation and the controller's objectives and sometimes may lead to a total system shutdown due to the fast-acting power electronic converters and associated control system. The resiliency against cyber-attacks in microgrids has become the need of the hour, especially for defense, shipboard, remote island microgrids, etc. This thesis focuses on modeling, detecting, and mitigating sophisticated false data injection (FDI) cyber-attacks in microgrids.

First, a stealth FDI attack modeling on the output current measurement of distributed energy resource (DER) in DC microgrids is presented where the attacker's presence is hidden from the system operator. Due to the lack of global information monitoring in the distributed controlled DC microgrids, detecting stealth FDI attacks has become a challenge. This thesis proposes a discordant element (DE)-based attack detection to detect attacked nodes. The proposed detection method is simple to implement and uses local and neighboring DERs inductor current references from the device level control and computes the DE values. Any non-zero value of DE of DER during the DC microgrid operation indicates the presence of an FDI attack.

Cyber-attackers may target to disrupt the microgrid operation or control objectives without the system operator's notice. For this, the second chapter in the thesis proposes localized attack detection and event-driven mitigation to make distributed controlled DC microgrids resilient against FDI attacks. An attack impact analysis is presented to determine the deviation in average voltage and output current caused from its pre-attacked values due to the FDI attack. Based on the analysis, the global control objectives are derived for the resilient DC microgrid operation. A localized attack detection based on the error between sensor measurement value and artificial neural net-

work (ANN) estimated value is used to detect the FDI attack. Further, an event-driven resiliency is developed to mitigate the attack, where the attacked measurements are replaced with ANN-based estimated values.

Further, the resiliency of the microgrid can be enhanced by decreasing the number of variables communicated in the communication links, so the number of attack-prone elements is effectively reduced. However, it is a challenge to realize the distributed control with a reduced number of variables while achieving the average voltage restoration and proportionate power-sharing simultaneously in the DC microgrid. For this, a distributed control with reduced communication variables is proposed, along with event-based resiliency for communication variable attacks.

In AC microgrids, any false data injection (FDI) in the communicated variables used in distributed secondary control leads to frequency and voltage deviations. A steady-state FDI attack impact analysis on the conventional distributed controller is carried out to determine the deviations in attack magnitude and controller parameters. Further, to mitigate the deviations, the auxiliary variables are incorporated into the conventional cooperative active and reactive power loops. The cooperative errors derived from the auxiliary variables are used to nullify the attack impacts on frequency and voltages. A steady state impact analysis is also presented for the proposed distributed control with an FDI attack to show the convergence of frequency and average voltage of the AC microgrid to its nominal values. The presented impact analysis, proposed detection, and mitigation strategies throughout the thesis have been validated in simulations and hardware experimental setups for various case studies showing satisfactory performance. Finally, the significant findings and proposed method implications are concluded, along with the future scope that can pave the way forward for this thesis.

Key Words: Cyber-Physical Systems, Distributed Secondary Control, False Data Injection Attack, Microgrids, Resilient Control.

सारांश

संवेदक प्रतिक्रिया और वितरित संचार के कारण वितरित नियंत्रित माइक्रोग्रिड अत्यधिक साइबर हमलों के अधीन होते हैं। हालांकि वितरित नियंत्रित माइक्रोग्रिड में साइबर हमले एक कम संभावना वाली घटना है, वे माइक्रोग्रिड संचालन और नियंत्रक के उद्देश्यों को महत्वपूर्ण रूप से बाधित करते हैं और कभी-कभी तेजी से काम करने वाले पावर इलेक्ट्रॉनिक कन्वर्टर और संबंधित नियंत्रण प्रणाली के कारण कुल सिस्टम शटडाउन का कारण बन सकते हैं। माइक्रोग्रिड्स में साइबर हमलों के खिलाफ लचीलापन समय की आवश्यकता बन गया है। यह थीसिस माइक्रोग्रिड्स में परिष्कृत गलत डेटा इंजेक्शन (एफडीआई) साइबर हमलों को मॉडलिंग, पता लगाने और कम करने पर केंद्रित है। सबसे पहले, डीसी माइक्रोग्रिड्स में डिस्ट्रीब्यूटेड एनर्जी रिसोर्स (डी. ई. आर.) के आउटपुट करंट मेजरमेंट पर एक स्टीथ एफ. डी. आई. अटैक मॉडलिंग प्रस्तुत की जाती है जहाँ हमलावर की उपस्थिति सिस्टम ऑपरेटर से छिपी होती है। वितरित नियंत्रित डीसी माइक्रोग्रिड्स में वैश्विक सूचना निगरानी की कमी के कारण, गुप्त एफडीआई हमलों का पता लगाना एक चुनौती बन गया है। यह थीसिस हमला किए गए नोड्स का पता लगाने के लिए एक विसंगत तत्व-आधारित हमले का पता लगाने का प्रस्ताव करता है। प्रस्तावित पहचान विधि को लागू करना सरल है और डिवाइस स्तर नियंत्रण से स्थानीय और पड़ोसी डी. ई. आर. प्रेरक वर्तमान संदर्भों का उपयोग करता है।

कभी-कभी, साइबर-हमलावर सिस्टम ऑपरेटर की सूचना के बिना माइक्रोग्रिड संचालन या नियंत्रण उद्देश्यों को बाधित करने के लिए लक्षित कर सकते हैं। इसके लिए, थीसिस के दूसरे अध्याय में वितरित नियंत्रित डीसी माइक्रोग्रिड को एफडीआई हमलों के खिलाफ लचीला बनाने के लिए स्थानीयकृत हमले का पता लगाने और घटना-संचालित शमन का प्रस्ताव है। एफ. डी. आई. हमले के कारण इसके पूर्व-हमला किए गए मूल्यों के कारण औसत वोल्टेज और आउटपुट करंट में विचलन को निर्धारित करने के लिए एक आक्रमण प्रभाव विश्लेषण प्रस्तुत किया जाता है। विश्लेषण के आधार पर, लचीला डीसी माइक्रोग्रिड संचालन के लिए वैश्विक नियंत्रण उद्देश्य प्राप्त किए जाते हैं। एफ. डी. आई. हमले का पता लगाने के लिए संवेदक माप मूल्य और कृत्रिम तंत्रिका नेटवर्क (ए. एन. एन.) अनुमानित मूल्य के बीच त्रुटि के आधार पर एक स्थानीयकृत हमले का पता लगाने का उपयोग किया जाता है। इसके अलावा, हमले को कम करने के लिए एक घटना-संचालित लचीलापन विकसित किया जाता है, जहां हमला किए गए माप को ए एन एन-आधारित अनुमानित मूल्यों से बदल दिया जाता है।

इसके अलावा, संचार लिंक में संचारित चर की संख्या को कम करके माइक्रोग्रिड के लचीलेपन को बढ़ाया जा सकता है, इसलिए हमले-प्रवण तत्वों की संख्या को प्रभावी रूप से कम किया जाता है। हालांकि, डीसी माइक्रोग्रिड में एक साथ औसत वोल्टेज बहाली और आनुपातिक बिजली-साझाकरण प्राप्त करते हुए कम संख्या में चर के साथ वितरित नियंत्रण का एहसास करना एक चुनौती है। इसके लिए, कम संचार चर के साथ एक वितरित नियंत्रण प्रस्तावित किया गया है, साथ ही संचार चर हमलों के लिए घटना-आधारित लचीलापन।

एसी माइक्रोग्रिड्स में, डिस्ट्रीब्यूटेड सेकेंडरी कंट्रोल में उपयोग किए जाने वाले स्टेट वेरिएबल्स में कोई भी फाल्स डेटा इंजेक्शन (एफडीआई) फ्रीक्वेंसी और वोल्टेज विचलन की ओर ले जाता है। हमले के परिमाण और नियंत्रक मापदंडों के संदर्भ में विचलन निर्धारित करने के लिए पारंपरिक वितरित नियंत्रक पर एक स्थिर-राज्य एफडीआई हमले के प्रभाव का विश्लेषण किया जाता है। इसके अलावा, विचलन को कम करने के लिए, सहायक चर को पारंपरिक सहकारी सक्रिय और प्रतिक्रियाशील पावर लूप में शामिल किया जाता है। सहायक चर से प्राप्त सहकारी त्रुटियों का उपयोग आवृत्ति और वोल्टेज पर हमले के प्रभावों को समाप्त करने के लिए किया जाता है। एसी माइक्रोग्रिड की आवृत्ति और औसत वोल्टेज के इसके नाममात्र मूल्यों में अभिसरण को दिखाने के लिए एफडीआई हमले के साथ प्रस्तावित वितरित नियंत्रण के लिए एक स्थिर स्थिति प्रभाव विश्लेषण भी प्रस्तुत किया जाता है।

प्रस्तुत प्रभाव विश्लेषण, डिटेक्शन का उपयोग करके प्रस्तावित लचीला नियंत्रण, और पूरे थीसिस में शमन रणनीतियों को MATLAB/सिमुलिक में और विभिन्न केस स्टडी के लिए हार्डवेयर प्रयोगात्मक सेटअप पर मान्य किया गया है।

मुख्य शब्द: साइबर-फिजिकल सिस्टम, डिस्ट्रिब्यूटेड सेकेंडरी कंट्रोल, फाल्स डेटा इंजेक्शन अटैक, माइक्रोग्रिड्स, रेजिलिएंट कंट्रोल

Contents

Certificate	i
Acknowledgments	ii
Abstract	v
Contents	viii
List of Figures	xiii
List of Tables	xviii
Nomenclature	xix
1 Introduction	1
1.1 Introduction	1
1.2 Cyber Security in Power and Energy Systems	3
1.3 Existing Literature and Major Research Gaps	7
1.3.1 Attack modeling and detection schemes in DC microgrids	7
1.3.2 Attack mitigation strategies in DC microgrids	9
1.3.3 Distributed secondary control with fewer communication variables	11
1.3.4 Distributed control strategies for AC microgrid against communication FDI attacks	12

1.4	Research Objectives	14
1.5	Summary of Research Works	14
1.5.1	Stealth attack modeling and detection in DC microgrids	14
1.5.2	Resilient event-driven distributed secondary control for DC microgrids	15
1.5.3	Resiliency enhanced distributed controller for DC microgrids	16
1.5.4	Resiliency integrated distributed secondary control for AC microgrids under cyber-attacks	17
1.6	Thesis Outline	18
2	Modeling and Detection of Stealth Attacks in DC Microgrids	20
2.1	Introduction	20
2.2	DC Microgrid System Description	22
2.2.1	Preliminaries of consensus algorithms	23
2.2.2	Distributed secondary control for DCMG	24
2.3	FDI Attack Modeling in A Cyber-Physical DCMG System	25
2.3.1	Case study	27
2.4	Proposed Discordant Element (DE) Detection Method	28
2.5	Simulation Results	33
2.5.1	Simulation validation of proposed DE detection for stealth attacks in single DER and associated links	33
2.5.2	Validation of proposed DE detection for stealth attack in multiple DERs	34
2.5.3	Validation of proposed detection scheme for sinusoidal FDI attacks	35
2.5.4	Validation of proposed detection scheme for ramp FDI attacks	36
2.5.5	Validation of proposed detection for FDI attack on all DERs	37
2.5.6	Validation of proposed detection for FDI attack with plug and play (PnP) of DER	38
2.6	Hardware Validations	40
2.6.1	Validation of DE detection for single DER FDI attack	41

2.6.2	Validation of DE detection for FDI attack on all DERs	42
2.6.3	Validation of DE detection for communication link out	43
2.7	Chapter Summary	45
3	Event-Driven Resilient Distributed Secondary Control for DC Microgrids	47
3.1	Introduction	47
3.2	Steady-State Impact Analysis of DCMG under Sensor Measurement FDI Attacks .	48
3.2.1	Impact of single-point attacks on DCMG	50
3.2.2	Steady-state impact analysis for zero-sum attacks	51
3.2.3	Global control objectives for resilient operation of DSC DCMG	53
3.2.4	Case study	54
3.3	Proposed ANN-based Event-Driven Resilient DSC for DCMG	56
3.3.1	Output current estimation using ANN	57
3.3.2	Proposed event-driven resilient control for DCMG	58
3.3.3	Design guidelines for ζ and τ_{od}	60
3.4	Simulation Results	62
3.4.1	ANN training for output current estimation	64
3.4.2	Simulation results for single-point attacks	65
3.4.3	Comparison of DSC performance under zero-sum attacks	66
3.4.4	Simulation results of proposed resilient DSC against SPC and ZSC attacks	67
3.4.5	Validation of proposed resilient control under multiple attacks	69
3.4.6	Validation of proposed resilient control under communication delay	71
3.4.7	Validation of proposed resilient control on larger DCMG system under multiple attacks	72
3.5	Experimental Results	72
3.5.1	Experimental validation under single-point attacks	73
3.5.2	Experimental validation under zero-sum attacks	74

3.5.3	Experimental validation of proposed event-driven control under SPC and ZSC attacks	75
3.5.4	Experimental validation of DCMG under multiple attack locations and magnitudes	76
3.6	Chapter Summary	77
4	Enhanced Resilient Distributed Secondary Control for DC Microgrids	80
4.1	Introduction	80
4.2	Vulnerability and Impact Analysis of DC Microgrid	81
4.2.1	Control objectives for DCMG system	82
4.2.2	Conventional distributed control for DCMG	82
4.2.3	Vulnerability and impact analysis	83
4.3	Proposed Enhanced Resilient Distributed Control for DC Microgrids	86
4.3.1	Resiliency enhancement using event-based mitigation for DSC DCMG against communication link attacks	87
4.4	Simulation Results	88
4.4.1	Validation of proposed control for DCMG under large transient disturbances	90
4.4.2	Validation of proposed resilient control under communication link attacks .	93
4.5	Experimental Results	95
4.6	Chapter Summary	97
5	Integrated Resilient Distributed Secondary Control for AC Microgrids	99
5.1	Introduction	99
5.2	System Description and Objectives of DSC AC microgrid	100
5.2.1	Cyber-physical AC microgrid description	100
5.2.2	Preliminaries of dynamic consensus with reference tracking	102
5.2.3	Conventional DSC for AC microgrid	102
5.2.4	Objectives of DSC for AC microgrid	104

5.3	FDI Cyber-Attack Modeling and Impact on Frequency and Voltage of AC Microgrid	105
5.3.1	Impact of communication link attack on AC microgrid frequency and average voltage	106
5.3.2	Impact of local measurement attack on AC microgrid frequency	109
5.4	Proposed Resiliency Integrated DSC for AC Microgrids	110
5.4.1	Resilient DSC for frequency restoration of AC microgrid	111
5.4.2	Resilient DSC for average voltage restoration of AC microgrid	112
5.4.3	Steady-state analysis of proposed resilient distributed controller	113
5.5	Simulation Results and Discussion	116
5.5.1	Performance validation of proposed distributed control for load disturbances	117
5.5.2	Validation of proposed resilient control for frequency restoration during FDI attacks	118
5.5.3	Validation of proposed resilient control for voltage restoration during FDI attacks	119
5.5.4	Validation of proposed resilient control under plug and play of DER	121
5.5.5	Validation of proposed resilient control under communication link out . . .	122
5.6	Experimental Results	124
5.6.1	Validation of impact analysis for communication link attacks	127
5.6.2	Validation of proposed resiliency integrated distributed control for communication link FDI attacks	127
5.7	Chapter Summary	129
6	Conclusions and Future Scope	131
6.1	Conclusions	131
6.2	Future Scope	134
	Bibliography	136

Contents	xiii
List of Publications	143
Biodata	145

List of Figures

1.1	Timeline of major cyber-physical attacks on power and energy systems [1]	3
1.2	Different attack locations in a microgrid with secondary controller	6
2.1	N DER based cyber-physical model of DC microgrid system	21
2.2	Case study of DSC DCMG under destabilization attack and stealth attack	28
2.3	Overall control for i th DER with proposed discordant element(DE) detection	29
2.4	Performance evaluation of discordant theory under stealth attack in DER1 with $\phi_1^{fd} = 1A$. (a) Output currents were received in DSC. (b) Inductor current reference.	31
2.5	Validation of proposed DE detection for stealth attack with a false data of 3.6 A in DER1 sensor measurement.	34
2.6	Simulation results of output voltage(top), output current received in DSC(middle), and DE values of DERs under stealth attack in multiple DERs.	35
2.7	Simulation results of output voltage(top), output current received in DSC(middle), and DE values of DERs under sinusoidal attack in DER2 with false data of $\phi_2^{fd} = 2 + 0.8\sin(0.4\pi t)$	36
2.8	Simulation results of output voltage(top), output current received in DSC(middle), and DE values of DERs under ramp FDI attack in DER2 with false data of $\phi_2^{fd} = 1.5t$	37
2.9	Simulation results of output voltage(top), output current received in DSC(middle), and DE values of DERs for all DERs FDI attack in the DCMG.	38

2.10	Simulation results of output voltage(top), output current received in DSC(middle), and DE values of DERs for plug and play of DER3 and FDI attack in the DER2. . .	39
2.11	Hardware setup of DC microgrid with $N=3$ DERs.	40
2.12	Single line diagram of DC microgrid hardware setup	41
2.13	Validation of proposed DE detection for stealth FDI attack on DER1 with false data of 2 A.	42
2.14	Validation of proposed DE detection for stealth FDI attack on all DERs. The false data injected is 1 A in DER2, 1 A in DER3, and 1.5 A in DER1, in sequence. . . .	43
2.15	Validation of DE Detection for FDI attack in DER1 with Communication link13 out	43
2.16	Validation of DE Detection for FDI attack in DER3 with Communication link13 out	44
3.1	Cyber-physical model of DC microgrid system with N DERs	49
3.2	Case study showing impact of SPC and ZSC attacks on DCMG steady-state operation	55
3.3	Proposed event-driven resilient DSC for the i th DER in the DCMG	56
3.4	ANN diagram with input, hidden, and output layers	57
3.5	(a) Output current and ANN estimated current with ripple and noise (b) Normal distribution of ripple and noise of I_o and I_o^{ann} (c) I_o and I_o^{ann} comparison during a load increment	61
3.6	Flowchart of proposed event-driven resiliency for DSC DCMG under local measurements attacks	62
3.7	ANN training performance in terms of regression plot	63
3.8	Simulation results of DCMG for attacks on voltage measurements in terms of output voltages, estimated average voltages, and output currents. (a) under SPV attack (b) under ZSV attack	64
3.9	Simulation results of DCMG under SPC attacks with responses of output current, output voltages, AD value, and RCS with and without proposed method	67
3.10	Simulation results of DCMG under ZSC attacks with responses of output current, output voltages, AD value, and RCS with and without proposed method	68

3.11	Validation of proposed resilient event-driven control under different FDI attacks . . .	69
3.12	Validation of proposed resilient event-driven control for FDI attacks at different locations and magnitudes	70
3.13	Validation of proposed method under communication delay in multiple links and FDI attacks	71
3.14	Validation of proposed method on 8 DER DCMG system under FDI attacks	72
3.15	Experimental results for attacks on voltage measurements under SPV attack and ZSV attack	74
3.16	Experimental results for attacks on current measurement under SPC attack and ZSC attack	75
3.17	Experimental results of proposed event-driven resilient DSC for DCMG against SPC attack.	76
3.18	Experimental results of proposed event-driven resilient DSC for DCMG against ZSC attack.	77
3.19	Experimental validation of proposed resilient DSC for DCMG against SPC attack at different locations and magnitudes.	78
4.1	Cyber-physical DCMG system with N DERs under study	81
4.2	Proposed reduced communication variable distributed secondary control for the i th DER	86
4.3	Flowchart of proposed event-based resiliency for DSC DCMG with communica- tion link attacks	89
4.4	Simulation validation of proposed distributed control under multiple load distur- bances with the responses of output voltages and output currents	90
4.5	Simulation validation of conventional distributed control in [2] under stealth at- tacks with the responses of output voltages and output currents	92
4.6	Simulation validation of proposed distributed control under stealth attacks with the responses of output voltages and output currents	92

4.7	Validation of proposed event-based mitigation distributed control under FDI attack communication link41	93
4.8	Validation of proposed distributed control under ZSC communication link FDI attacks	93
4.9	Experimental validation of DCMG with proposed distributed control under the multiple load disturbances.	95
4.10	Experimental validation of proposed control under SPV attack	96
4.11	Experimental validation of proposed distributed control under ZSV attacks	96
5.1	Cyber-physical distributed AC microgrid model consists of N DERs	101
5.2	Proposed resiliency integrated DSC structure for i th DER	110
5.3	Impact of communication FDI attack on state variable $\bar{P}_{o23}^{fd} = 4 \text{ rad/s}$ in CDC AC microgrid in terms of cooperative error in $\bar{P}_o$ (top) and cooperative error in ω (bottom). [$c_P = 15, c_\omega = 20$]	112
5.4	Impact of FDI attack on proposed resilient DSC for frequency restoration showing $L\bar{P}_o^a$ (top), output of active power controller (middle) and cooperative error in α_p (bottom) with a false data of 4 rad/s in $\bar{P}_{o23}$	113
5.5	Impact of communication link FDI attack on state variable $\bar{Q}_{o14}^{fd} = 4 \text{ V}$ in CDC AC microgrid in terms of cooperative error in $\bar{Q}_o$ (top) and error in cooperative voltage (middle) and output of the reactive power controller.	114
5.6	Impact of FDI attack on proposed resilient DSC for voltage restoration showing $L\bar{Q}_o^a$ (top), output of reactive power controller (middle) and cooperative error in α_q (bottom) with a false data of 4 V in $\bar{Q}_{o23}$	115
5.7	Simulations results of proposed distributed secondary controlled AC microgrid. (a) Active power (b) Frequency (ω) (c) Reactive powers (d) Peak Voltage (V^{od}) . .	116
5.8	Performance of CDC AC microgrid under link23 attack on $\bar{P}_o$ variable with a false data of 4 rad/s. (a) Frequency (ω) (b) Active power of DERs. [$c_P = 15, c_\omega = 20$] .	118

5.9	Validation of proposed resilient DSC for AC microgrid under link23 attack on $\bar{P}_o$ variable a false data of 4 rad/s. (a) Frequency (ω) (b) Active power of DERs.	119
5.10	Performance of CDC AC microgrid under link14 attack on $\bar{Q}_o$ variable with false data of 4 V. (a) Voltages, (V_{od}) (b) Reactive power of DERs. [$c_Q = 20$]	120
5.11	Validation of proposed resilient DSC for AC microgrid under link FDI attack on $\bar{Q}_o$ variable with false data of 4 V. (a) Voltages, (V_{od}) (b) Reactive power of DERs.	121
5.12	Validation of proposed resilient distributed secondary controlled AC microgrid for plug and play operation of DER3. (a) Frequency, (ω) (b) Active power of DERs.	121
5.13	Validation of proposed resilient distributed secondary controlled AC microgrid for plug and play operation of DER3. (a) Voltages, (V_{od}) (b) Reactive power of DERs.	122
5.14	Validation of proposed distributed secondary controlled AC microgrid under communication link out.	123
5.15	(a) Single line diagram of hardware ACMG setup	124
5.16	Hardware AC microgrid setup consisting of 3 GFM inverters with loads	125
5.17	Hardware validation of CDC ACMG against FDI attacks on $\bar{P}_o$ data in communication link	126
5.18	Hardware validation of CDC ACMG against FDI attacks on $\bar{Q}_o$ data in communication link	126
5.19	Hardware validation of proposed resilient frequency control against FDI attacks on $\bar{P}_o$ data in communication link	128
5.20	Hardware validation of proposed resilient voltage control against FDI attacks on $\bar{Q}_o$ data in communication link	128

List of Tables

1.1	Major cyber-physical attacks on power and energy systems.	4
3.1	Impacts of FDI attacks on DCMG steady-state average voltage and output currents	53
3.2	ANN and training details for simulation and hardware	65
4.1	Impacts of communication link FDI attacks on CDC DCMG steady-state average voltage and output currents	85
4.2	Simulation and experimental setup parameters	91

Nomenclature

Acronyms/Abbreviations

ACMG Alternating Current Microgrid

AD Attack Disclosure

AI Attack Index

CDC Conventional Distributed Control

DCMG Direct Current Microgrid

DE Discordant Element

DER Distributed Energy Resource

DoS Denial of Service

DSC Distributed Secondary Control

FDI False Data Injection

GFL Grid Following

GFM Grid Forming

ICS Industrial Control Systems

IT	Information Technology
OT	Operational Technology
PLC	Programmable Logic Controller
RCS	Resilient Control Signal
RES	Renewable Energy Sources
SCADA	Supervisory Control and Data Acquisition
SPC	Single Point Current
SPV	Single Point Voltage
ZSC	Zero Sum Current
ZSV	Zero Sum Voltage