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

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. Shubhendu 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 Tripati and Mr. Satish, for all their support during all these years.

I am profoundly grateful to my parents, Mrs. Sujatha and Mr. Ramachamdraiah, 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 कन्वर्टर्स 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 स्टील्थ 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, डिस्ट्रिब्यूटेड 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/सिमुलिंक में और विभिन्न केस स्टडी के लिए हार्डवेयर प्रयोगात्मक सेटअप पर मान्य किया गया है।

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

Contents

List of Figures

List of Tables

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