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.

Gupta

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 serves 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 scheme are capable to distinguish 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 DLAAs 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.

सारांश

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 इंटिग्रिटी 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 सिंक्रोनाइज़ेशन 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

List of Figures

List of Tables

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
$\mathrm{m}_j^{\mathrm{p}}$ & $\mathrm{n}_j^{\mathrm{q}}$	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
$\mathbf{E}$	Edge connecting agents
$\mathbf{L}$, $\mathbf{D}_{\text{in}}$ & $\mathbf{A}_{\text{G}}$	Laplacian matrix, Incoming information matrix & Adjacency matrix
$\Delta\omega_{\mathrm{sec}j}$ & $\Delta\mathrm{V}_{\mathrm{sec}j}$	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^* & $\bar{\mathrm{V}}_j^{\mathrm{dc}}$	Local reference voltage & average voltage of j^{th} PGM
$\mathrm{R}_j^{\mathrm{vir}}$	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