CYBER-ATTACK RESILIENT DESIGN OF WIDE AREA MEASUREMENT SYSTEM IN SMART GRID

ASTHA CHAWLA

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY DELHI

October 2022

CYBER-ATTACK RESILIENT DESIGN OF WIDE AREA MEASUREMENT SYSTEMS IN SMART GRID

by

ASTHA CHAWLA

Department of Electrical Engineering

Submitted
in the fulfilment of the requirements of the degree of Doctor of Philosophy
to the

Indian Institute of Technology Delhi

October 2022

Dedicated

to

Mumma and Papa

CERTIFICATE

This is to certify that the thesis entitled **"Cyber-Attack Resilient Design of Wide Area Measurement Systems In Smart Grid"** submitted by **Ms. Astha Chawla**, to Indian Institute of Technology Delhi for the award of degree of **Doctor of Philosophy (Ph.D.)** 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.

Dr. Bijaya Ketan Panigrahi

Professor

Department of Electrical Engineering

Indian Institute of Technology Delhi

New Delhi-110016, India.

Date: 26th OCTOBER 2022

Acknowledgements

I would like to express my sincere gratitude to my Supervisor, Prof. B.K. Panigrahi, for providing me the opportunity to work in this area and for this constant guidance, encouragement, patience, and consistent direction during my Ph.D. journey at IIT Delhi. It has been an honor to work under his supervision and as part of his working group.

I am grateful to the members of my doctoral research committee, Prof. N. Senroy, Prof. A R. Abhyankar, and Prof. Ashu Verma, for their constructive suggestions and examination of my work.

I am extremely grateful to Prof. B. R. Bhalja for introducing me to the world of research and for his continual mentoring and insightful suggestions throughout my research work. I would also like to thank Prof. K. Paul for his expert advice and constructive pointers, which have been incredibly helpful.

I am thankful to Animesh and Prakhar for being so cooperative and wonderful to work with. I am grateful to industry professionals, particularly Mr. Santosh Kumar, Mr. Vivek Singh, Mr. Ashwin Damle, and Mr. Ankur Gulati, for patiently addressing my doubts and providing technical assistance in setting up the experimental testbed setup.

I am eternally grateful to my mother, Mrs. Rajni Chawla, and my father, Mr. Ashok Chawla, for being my greatest strength during this journey and for always believing in me and motivating me. I am grateful to my husband, Mohit Chandra, for sticking with me through the highs and lows of this journey and for being unbelievably patient and supportive. I am wholeheartedly thankful to my sister Malvika Chawla, and my brother Akshit Chawla, for being my constant listeners and biggest cheerleaders. I am grateful for their incredible support and constant encouragement during this journey. I am also thankful to my parents-in-law, Mrs. Rekha Saxena and Mr. Rakesh Saxena, and my brother-in-law Rohit Chandra for their continuous support and co-operation.

I am thankful to all my seniors, particularly Dr. Rishi Sharma, Dr. Deep Kiran, Dr. Sayari Das, Dr. Abdul Saleem Mir, Dr. Manas Jena, Mr. Debasis Mishra, Dr. Siva Raman, Dr. Kush Khanna, Dr. Rajiv Jha, Dr. Megha Gupta, Dr. Deepak Pullagurram for providing a warm, encouraging research atmosphere, and sharing their learnings and experiences. I am also thankful to all my friends and juniors, especially Vibhuti, Pankaj, Swagata, Arpan, Debargha, Geeta, Vijay, Samriddhi, Diptak, Kirti, Upasana, Arup for making my Ph.D. journey at IIT Delhi much more memorable. I am also thankful to IIT Delhi and its staff members, particularly Mr. Gaurav Kumar, Mr. Satish Sah, Mr. Yatindra Mani Tripathi and Mr. Anand Sansanwal for continual support.

Finally, I would also like to thank the Ministry of Human Resource and Development, India, for the scholarship grant for the research program.

Dated: 26th October 2022

Astha Chawla

Abstract

Advances in information, communication, and computer technologies and their subsequent application in power system infrastructure have resulted in the emergence of new technologies such as the Wide Area Measurement System (WAMS). Fast, highly accurate, and timestamped data from the Phasor Measurement Units (PMUs) have made real-time wide area situational awareness possible. They have also solved many complex power systems problems like preventing relay maloperations. However, the IEEE C37.118 PMU data's vulnerability to cyber-attacks can paralyze the working of such applications. While denial-of-service (DoS) attacks can blind the system operator about the grid's condition, data manipulation attacks can mislead the decision-making at the control center, compromising the power system's operation. Thus, it is crucial to secure PMU data against these attacks and avoid their adverse effect on the end applications. Further, for wide area protection and control applications (WAPAC) which involve sending a decision signal from the control center (based on PDC data) to the intelligent electronic devices (IEDs) in the substation, secure communication of such critical messages is also important for overall attack resiliency of such applications.

In this regard, the work in this thesis focuses on ensuring the availability, confidentiality, and integrity of synchrophasor data (IEEE C37.188) from PMUs (in substations) to the PDC (in the control center). It also discusses ways to secure critical decision signals, which can be communicated using IEC 61850-90-5 R-GOOSE protocol from protection schemes (in the control center) to the IEDs (Relays or BCUs) in the substation. The approach used in this work is inspired by the guidelines provided by the National Institute of Standard and Technology (NIST) for the cybersecurity of critical infrastructures. In this context, a cyber-physical WAMS testbed is developed for risk assessment, and then attack resiliency of PMU data based wide area monitoring and protection application (WAMAP) applications is enhanced by redesigning the WAMS framework with attack prevention, detection and mitigation strategies as discussed below:

- Cyber-physical WAMS testbed is developed for vulnerability assessment and studying the impact of cyber-attacks. The testbed includes industry-standard hardware, software, and communication protocols (IEEE C37.118 and IEC 61850-90-5).
- DoS attack prevention strategy is developed for PMU data in the WAMS framework using concepts of redundancy and randomness. Thereafter, unique fingerprints based attack

detection strategy is suggested for determining the root cause of data unavailability in terms of communication issues or DoS attacks. The detection strategy also identifies different types of DoS attacks.

- DoS attack mitigation approach is developed for PMU data using machine learning imputation techniques and deep learning networks to ensure attack resiliency of wide area monitoring and protection applications (situational awareness and adaptive relaying) during PMU data unavailability.
- A methodology for data manipulation attack detection in the WAMS framework for wide area monitoring and offline applications is suggested. The approach is based on the intrinsic properties of WAMS infrastructure and the existing strong and synchronized power grid. Further, to enhance attack resiliency of time-critical wide area applications against data manipulation attacks, a detection, and mitigation approach using deep learning networks is also developed.
- For overall attack resiliency of wide area protection applications like adaptive relaying, security of supervisory decision messages (IEC 61850-90-5 R-GOOSE messages) from the control center to the IEDs in the substation is enhanced using Cryptography technique and Blockchain concepts.

Keywords: Cyber Security**,** Wide Area Measurement Systems, Wide Area Situational Awareness, Adaptive Relaying, IEEE C37.118, IEC 61850-90-5 R-GOOSE, Denial-of-Service Attacks, Data Manipulation Attacks, Cryptography

सार

सूचना, संचार और कंप्यूटर प्रौद्योगिकियों में प्रगति और बिजली प्रणाली के बुनियादी ढांचे में उनके बाद के अनुप्रयोग के परिणामस्वरूप वाइड एरिया मेजरमेंट सिस्टम (WAMS) जैसी नई तकनीकों का उदय हुआ है। फेजर मेजरमेंट यूनिट्स (पी.एम.यू) के तेज, अत्यधिक सटीक और टाइमस्टैम्प्ड डेटा ने रीयल-टाइम वाइड एरिया सिचुएशनल अवेयरनेस को संभव बनाया है। उन्होंने रिले की खराबी को रोकने जैसी कई जटिल बिजली प्रणालियों की समस्याओं को भी हल किया है। हालाँकि, आईईईई C37.118 पी.एम.यू डेटा की साइबर हमलों के प्रति संवेदनशीलता ऐसे अनुप्रयोगों के कार्य को पंगु बना सकती है। जबकि डिनायल-ऑफ-सर्विस (DoS) हमले ग्रिड की स्थिति के बारे में सिस्टम ऑपरेटर को अंधा कर सकते हैं, डेटा हेरफेर हमले बिजली व्यवस्था के संचालन से समझौता करते हुए, नियंत्रण केंद्र में निर्णय लेने को गुमराह कर सकते हैं। इस प्रकार, इन हमलों के खिलाफ पीएमयू डेटा को सुरक्षित करना और अंतिम अनुप्रयोगों पर उनके प्रतिकूल प्रभाव से बचना महत्वपूर्ण है। इसके अलावा, विस्तृत क्षेत्र संरक्षण और नियंत्रण अनुप्रयोगों (डब्ल्यूएपीएसी) के लिए, जिसमें सबस्टेशन में बुद्धिमान इलेक्ट्रॉनिक उपकरणों (आई.ई.डी) को नियंत्रण केंद्र (पी.डी.सी डेटा के आधार पर) से निर्णय संकेत भेजना शामिल है, ऐसे महत्वपूर्ण संदेशों का सुरक्षित संचार भी महत्वपूर्ण है ऐसे अनुप्रयोगों की समग्र हमले की लचीलापन।

इस संबंध में, इस थीसिस में काम पीएमयू (सबस्टेशनों में) से पीडीसी (कंट्रोल सेंटर में) तक सिंक्रोफैसर डेटा (आईईईई C37.118) की उपलब्धता, गोपनीयता और अखंडता सुनिश्चित करने पर केंद्रित है। यह महत्वपूर्ण निर्णय संकेतों को सुरक्षित करने के तरीकों पर भी चर्चा करता है, जिसे आई.ई.सी 61850-90-5 R-GOOSE प्रोटोकॉल का उपयोग करके सुरक्षा योजनाओं (नियंत्रण केंद्र में) से सबस्टेशन में आई.ई.डी (रिले या BCU) तक संचार किया जा सकता है। इस काम में इस्तेमाल किया गया दृष्टिकोण महत्वपूर्ण बुनियादी ढांचे की साइबर सुरक्षा के लिए राष्ट्रीय मानक और प्रौद्योगिकी संस्थान (एनआईएसटी) द्वारा प्रदान किए गए दिशानिर्देशों से प्रेरित है। इस संदर्भ में, जोखिम मूल्यांकन के लिए एक साइबर-भौतिक WAMS परीक्षण बिस्तर विकसित किया गया है, और फिर पी.एम.यू डेटा आधारित व्यापक क्षेत्र निगरानी और सुरक्षा अनुप्रयोग (WAMAP) अनुप्रयोगों के हमले के लचीलेपन को हमले की रोकथाम, पता लगाने और शमन रणनीतियों के साथ WAMS ढांचे को फिर से डिजाइन करके बढ़ाया जाता है, जैसा कि चर्चा नीचे की गई है:

- साइबर-भौतिक WAMS टेस्टबेड को भेद्यता मूल्यांकन और साइबर हमलों के प्रभाव का अध्ययन करने के लिए विकसित किया गया है। टेस्टबेड में उद्योग-मानक हार्डवेयर, सॉफ्टवेयर और संचार प्रोटोकॉल (आईईईई C37.118 और आईईसी 61850-90-5) शामिल हैं।
- अतिरेक और यादृच्छिकता की अवधारणाओं का उपयोग करते हुए डब्ल्यूएएमएस ढांचे में पीएमयू डेटा के लिए DoS हमले की रोकथाम रणनीति विकसित की गई है। इसके बाद, संचार मुद्दों या डीओएस हमलों के संदर्भ में डेटा की अनुपलब्धता के मूल कारण को निर्धारित करने के लिए अद्वितीय फिंगरप्रिंट आधारित हमले का पता लगाने की रणनीति का सुझाव दिया जाता है। पता लगाने की रणनीति विभिन्न प्रकार के DoS हमलों की भी पहचान करती है।
- पीएमयू डेटा की अनुपलब्धता के दौरान व्यापक क्षेत्र की निगरानी और सुरक्षा अनुप्रयोगों (स्थितिजन्य जागरूकता और अनुकूली रिलेइंग) की हमले की लचीलापन सुनिश्चित करने के लिए मशीन लर्निंग इंप्यूटेशन तकनीकों और डीप लर्निंग नेटवर्क का उपयोग करके पीएमयू डेटा के लिए डीओएस अटैक शमन दृष्टिकोण विकसित किया गया है।
- विस्तृत क्षेत्र निगरानी और ऑफ़लाइन अनुप्रयोगों के लिए डब्ल्यूएएमएस ढांचे में डेटा हेरफेर हमले का पता लगाने के लिए एक पद्धति का सुझाव दिया गया है। दृष्टिकोण डब्ल्यूएएमएस बुनियादी ढांचे के आंतरिक गुणों और मौजूदा मजबूत और सिंक्रनाइज़ पावर ग्रिड पर आधारित है। इसके अलावा, डेटा हेरफेर हमलों के खिलाफ समय-महत्वपूर्ण व्यापक क्षेत्र अनुप्रयोगों की हमले की लचीलापन बढ़ाने के लिए, गहन शिक्षण नेटवर्क का उपयोग करके एक पहचान और शमन दृष्टिकोण भी विकसित किया गया है।
- व्यापक क्षेत्र सुरक्षा अनुप्रयोगों जैसे अनुकूली रिलेइंग, पर्यवेक्षी निर्णय संदेशों की सुरक्षा (आईईसी 61850-90-5 R-GOOSE संदेशों) की सुरक्षा के लिए नियंत्रण केंद्र से सबस्टेशन में आई.ई.डी तक क्रिप्टोग्राफी तकनीक और ब्लॉकचैन अवधारणाओं का उपयोग करके बढ़ाया जाता है।

कीवर्ड: साइबर सुरक्षा, वाइड एरिया मेजरमेंट सिस्टम, वाइड एरिया सिचुएशनल अवेयरनेस, एडेप्टिव रिलेइंग, आईईईई C37.118, आईईसी 61850-90-5 R-GOOSE, डेनियल-ऑफ-सर्विस अटैक, डेटा मैनिपुलेशन अटैक, क्रिप्टोग्राफी

Content

Certificate i

Acknowledgements ii

Abstract iii

Contents vii

List of Figures xiii

List of Tables xvii

List of Abbreviations and Symbols xix

CHAPTER 1: Introduction 1

1.1 Cybersecurity of Power Grid: Research Motivation 1

1.2 Initiatives to Secure the Power Grid 1

1.3 Cybersecurity of Wide Area Measurement System: Research Motivation: 2

1.3.1 Wide Area Measurement System: Background 2

1.3.2 Importance of Wide Area Measurement Systems 4

1.3.3 Research Motivation 4

1.4 Approach used for Cybersecurity of Wide Area Measurement System 5

1.4.1 Guidelines for Cybersecurity 5

1.4.2 Time Complexities Related to WAMS Framework 7

1.5 Existing Research Work and Research Gaps 9

1.6 Summary of the Research Gaps in Existing Works 14

1.7 Thesis Objectives 14

1.8 Brief Overview of the Research Work 15

1.8.1 Development of Cyber-Physical WAMS testbed and its Risk Assessment 15

1.8.2 Prevention and Detection of Denial-of-Service Attacks on PMU data 15

1.8.3 Mitigation of Denial-of-Service Attacks on PMU data 16

1.8.4 Detection and Mitigation of Data Manipulation Attacks on PMU data17

1.8.5 Cybersecurity of IEC 61850-90-5 R-GOOSE Messages in Wide Area Protection Application 18

1.9 Major Contributions 18

1.10 Assumptions Considered in the Research Work 19

1.11 Industrial Feasibility and Scalability of the Suggested Solutions 20

1.12 Thesis Organization 21

CHAPTER 2 : Development of Wide Area Measurement System Testbed And Risk Assessment 223

2.1 General 23

2.2 Importance of WAMS Testbed with both IEEE C37.118 and IEC 61850 Communication 23

2.3 WAMS Testbed Developed at IIT Delhi 24

2.3.1 Physical layer 26

2.3.2 Network layer 27

2.3.3 Control Center 28

2.3.4 Communication Protocols 28

2.4 Demonstration of Communication Capabilities of RT-HIL WAMS Testbed...32

2.4.1 Physical Layer to Control Center Communication 32

2.4.2 Control Center to Physical Layer Communication 34

2.5 Applications of WAMS Testbed 35

2.6 Risk Assessment 35

2.6.1 Threat 35

2.6.2 Vulnerability Analysis 36

2.6.3 Cyber-Attack Model 37

2.6.4 Impact Analysis of DoS attack on Wide Area Protection Application.40

2.7 Conclusion 44

CHAPTER 3: Prevention And Detection of Denial-of-Service Attacks 45

3.1 General 45

3.2 Proposed DoS Pre-emptive and Detection Framework……46

3.2.1 Module 1: PDC Data-Based Anomaly Detector (DBAD) 47

3.2.2 Module 2: Random Data Path Selector (RDPS)……50

3.2.3 Module 3: ARP Spoofing Detector (ASD) 50

3.2.4 Module 4: Denial-of-Service Fingerprint Detector (DFD) 51

3.3 Working of DoS Pre-Emptive Modules in the Proposed Framework..... 53

3.4 Hardware Implementation of the Proposed Framework 54

3.5 Results and Discussions 55

3.5.1 Performance of the Proposed Framework during DoS Cyber-Attack on PMUi – PDC-X Connection 55

3.5.2 Performance of the Adaptive Relaying Protection Scheme with the Proposed Framework 60

3.5.3 Time Complexities 61

3.5.4 Scalability..... 62

3.6 Conclusion..... 63

CHAPTER 4: Mitigation of Denial-of-Service Attacks..... 64

4.1 General 64

4.2 Proposed DoS Mitigation Strategy for WAMS Framework 65

4.2.1 Design and Working of Proposed Framework……..65

4.2.2 DoS Mitigation Module 67

4.3 Hardware Implementation of the Proposed Framework 70

4.3.1 Hardware Implementation of Proposed WAMS Framework with DoS Mitigation Approach 70

4.3.2 Data Generation..... 72

4.3.3 ML/DL Model Implementation in Mitigation Module 73

4.4 Results and Discussion: Proposed Framework with KNN Imputation/K-Means Clustering based Mitigation Module 74

4.4.1 Performance Evaluation of KNN Imputation and K-Means Clustering in Mitigating DoS Impact on Wide Area Protection Application 74

4.4.2 Time Complexities 76

4.4.3 Scalability 76

4.5 Results and Discussion: Proposed framework with ODAE based Mitigation Module 77

4.5.1 Performance Evaluation of Data Reconstruction Capability of ODAE77

4.5.2 Enhancement of Wide Area Situational Awareness during DoS attacks on PMUs 80

4.5.3 Scalability 82

4.5.4 Performance Evaluation on Synchrophasor Data Captured from Northern Region of Indian Power Grid (NRIPG) 83

4.5.5 Time Complexities 84

4.5.6 Discussion 85

4.6 Limitation and Future Scope: Performance Evaluation of Proposed Framework during Data Manipulation Attack on PMU 85

4.7 Conclusion 86

CHAPTER 5: Detection And Mitigation of Data Manipulation Attacks on PMU Data 88

5.1 General 88

5.2 Synchronized Frequency Phasors based Attack Detection Approach: Conceptual Background 89

5.3 Synchronized Frequency Phasors Based Attack Detection Approach: Design and Working 92

5.3.1 WAMS Control Center Operation in General 92

5.3.2 Design and Working of the Proposed Approach 92

5.3.3 Salient Features and Advantages 94

5.4 Observations and Case Studies 95

5.4.1 Ramp attack on Phasor Data from PMU Installed at Allahabad in Northern

Region of Indian Power Grid 96

5.4.2 Replay attack on phasor data from PMU Installed at Kanpur in Northern Region of Indian Power Grid 97

5.4.3 Weak Step Attack on Different PMUs in Northern Region of Indian Power Grid 98

5.4.4 Time Complexities 100

5.5 Limitations and Related Discussion 100

5.6 Deep Learning Based Data Manipulation Attack Detection and Mitigation Strategy-Approach to Solution 101

5.6.1 Long Short-Term Memory (LSTM) for Predicting Time-Series PMU data 102

5.6.2 Generative Adversarial Imputation Nets (GAIN) for PMU Data Imputation 103

5.7 Deep Learning Based Data Manipulation Attack Detection and Mitigation Strategy-Design and Working 105

5.7.1 LSTM based Anomaly Detection Module 106

5.7.2 GAIN based Mitigation Module 109

5.7.3 Working of the Proposed Framework in Different Scenarios 112

5.8 Hardware Implementation of the Proposed Framework 113

5.8.1 Hardware Implementation of Proposed WAMS framework with Attack Detection and Mitigation Modules 113

5.8.2 LSTM and GAIN Deployment 113

5.8.3 Time Complexities 114

5.8.4 Scalability 114

5.9 Results and Discussions 114

5.9.1 Normal Working (No Cyber-Attack) 115

5.9.2 During Step, Replay and Ramp Attacks 117

5.10 Conclusion 121

CHAPTER 6: Cybersecurity and HIL Implementation of IEC 61850-90-5 Routable GOOSE based in Wide Area Protection Applications 123

6.1 General 123

6.2 Need of IEC 61850-90-5 R-GOOSE in Wide Area Protection Applications 124

6.3 RT-HIL Implementation of Adaptive Relaying Protection Scheme using IEEE C37.118 Phasors and IEC 61850-90-5 R-GOOSE 125

6.3.1 Adaptive Relaying Protection Scheme 125

6.3.2 Implementation of Adaptive Relaying Scheme on HIL WAMS Testbed ..... …….125

6.4 Cybersecurity of R-GOOSE Message 129

6.4.1 AEAD Algorithm based Security for R-GOOSE: Background 129

6.4.2 Implementation of AEAD Security Mechanism 130

6.4.3 Performance Evaluation 131

6.5 Way Forward: Securing R-GOOSE using Blockchain Technology 132

6.6 Conclusion 133

CHAPTER 7: Conclusion and Future Scope 134

7.1 Summary of the Work 134

7.2 Future Scope 136

References 137

Publications from the Thesis 146

Bio-Data 147

LIST OF FIGURES

Figure 1.1 (a)Conventional WAMS framework (b) Standard IEEE C37.118 frames between PMU and PDC captured in Wireshark 3
Figure 1.2 NIST Cybersecurity Framework 6
Figure 1.3 The CIA Triad 7
Figure 1.4 Industrial implementation of the suggested attack prevention, detection and mitigation solutions 20
Figure 2.1 Cyber-Physical RT-HIL WAMS Testbed showing connections between components and data communication 25
Figure 2.2 Picture of Cyber-Physical Wide Area Measurement Systems Testbed at IIT Delhi... 26
Figure 2.3 Communication between the data source (PMU) and destination (PDC) at 30 fps captured in Wireshark 30
Figure 2.4 Communication stack of different IEC 61850 messages……..31
Figure 2.5 (a) IEC 61850-90-5 R-SV messages in Wireshark (b) IEC 61850-90-5 R-GOOSE messages 31
Figure 2.6 IEEE C37.118 Synchrophasor communication from PMUs from the physical layer to SEL PDC at the control center 32
Figure 2.7 IEC 61850-90-5 R-SV published from GTNET-x2 SV-6 module at physical layer and subscribed at the INFO TECH SV receiver at the control center 33
Figure 2.8 IEC 61850-90-5 R-GOOSE published from RTDS GTNET-x2 GSE-v7 and subscribed at INFO TECH R-GOOSE receiver at control centre 34
Figure 2.9 IEC 61850-90-5 R-GOOSE published from INFO TECH Tool at the control center and subscribed at RTDS GTNET-x2 GSE-v7 at the physical Layer 34
Figure 2.10 Bird Eye view of cyber vulnerabilities in WAMS infrastructure 36
Figure 2.11 DoS Attack creates NAN corresponding to attacked PMU in the PDC datastream . 37
Figure 2.12 Wireshark snapshot of unsecured R-GOOSE frames published from RTDS GTNET-x2 GSE card 40
Figure 2.13 WSCC 9-Bus System model in RSCAD 41
Figure 2.14 Confusion matrices (a) Without DoS attack on any PMU (b) With DoS attack on PMU7 43
Figure 3.1 WAMS framework design with DoS attack pre-emptive and detection strategy 46

Figure 3.2 Flowchart of PDC data-based anomaly detector (DBAD) module 48
Figure 3.3 Flowchart of ARP spoofing detector (ASD) module 51
Figure 3.4 Flowchart of Denial of Service fingerprint detector (DFD) module 52
Figure 3.5 WAMS experimental testbed with proposed DoS prevention and detection modules 54
Figure 3.6 The output of the ARP spoofing detector 56
Figure 3.7 (a) DBAD's output for PMU7 (b) The input signal (S) to RDPS from DBAD 56
Figure 3.8 Communication failure fingerprint 58
Figure 3.9 Reset DoS attack fingerprint 59
Figure 3.10 Slowloris DoS attack fingerprint 59
Figure 3.11 SYN flood DoS attack fingerprint 60
Figure 4.1 Proposed WAMS framework design with DoS attack mitigation strategy 66
Figure 4.2 Structure of Overcomplete Denoising Autoencoder (ODAE)…….69
Figure 4.3 WAMS experimental testbed with proposed modules and ODAE model in the mitigation module 71
Figure 4.4 Confusion matrices depicting Normal Scenario (0), 3-phase faults (1), line outage (2), and generator outage (3) (a) Without DoS attack (b) With DoS attack on one PMU in conventional WAMS framework, (c) After mitigation of DoS attack through K- means Clustering in proposed framework and (d) After mitigation of DoS attack through KNN in proposed framework 75
Figure 4.5 During No-Attack (a) Plot showing original and reconstructed phasors at t^{th} timestamp (b) RE^t of all phasors at t^{th} timestamp 78
Figure 4.6 During DoS attack on PMU4 (a) Plot showing original and reconstructed phasors at t^{th} timestamp (b) RE^t of all phasors at t^{th} timestamp 79
Figure 4.7 $|I1_{94}|$ from PMU9 indicating line trip event on line4 81
Figure 4.8 $|I1_{75}|$ from PMU7 indicating load switch ON at Bus8 81
Figure 4.9 $|V1_4|$ from PMU4 indicating line faults event during severe DoS attacks for longer duration 82
Figure 4.10 |VR_AGRA| from PMU at AGRA location indicating line fault at Agra-Unnao Transmission line 84
Figure 4.11 During Data Manipulation attack on PMU7 (a) Plot of original and reconstructed phasors at t^{th} timestamp (b) RE of all phasors at t^{th} timestamp 86
Figure 5.1 Coherent and synchronized timestamped frequency phasors from PDC 89

Figure 5.2 Frequency phasors as observed from Northern Region PDC before and after the generation trip event 90
Figure 5.3 Frequency measurements from WAMS and SCADA [107] 91
Figure 5.4 Proposed WAMS framework design with synchronized frequency phasors based data manipulation attack detection methodology 93
Figure 5.5 Frequency phasors from different PMUs in Northern Region of Indian Power Grid during Ramp attack on data from PMU located at Allahabad 96
Figure 5.6 Frequency Phasors from different PMUs in Northern Region of Indian Power Grid during Replay attack on data from PMU located at Kanpur 97
Figure 5.7 Frequency phasors from different PMUs in Northern Region of Indian Power Grid during Step attack of 0.1% intensity on PMU located at Allahabad 98
Figure 5.8 Frequency phasors from different PMUs in Northern Region of Indian Power Grid during Step attack of 0.03% intensity on PMU located at Agra 99
Figure 5.9 Frequency phasors from different PMUs in Northern Region of Indian Power Grid during Step attack of 0.01% intensity on PMU located at Singrauli 100
Figure 5.10 Typical LSTM cell architecture 103
Figure 5.11 Proposed WAMS framework design with data manipulation attack detection and mitigation modules 106
Figure 5.12 The architecture of the LSTM based attack detection module 107
Figure 5.13 The architecture of the GAIN based attack mitigation module 109
Figure 5.14 Original and imputed (a) Voltage magnitude and (b) Voltage angle phasors without cyber-attack 116
Figure 5.15 Original, manipulated and imputed phasors of (a) Voltage magnitude and (b) Voltage angle during strong Step attack 118
Figure 5.16 Original, manipulated and imputed phasors of (a) Voltage magnitude and (b) Voltage angle during moderate Step attack 118
Figure 5.17 Original, manipulated and imputed phasors of (a) Voltage magnitude and (b) Voltage angle during weak Step attack 119
Figure 5.18 Original, manipulated and imputed phasors of (a) Voltage magnitude and (b) Voltage angle during Replay attack 120
Figure 6.1 Adaptive Relaying concept 126

Figure 6.2 Implementation of Dependability/Security Adaptive Relaying protection scheme on HIL WAMS testbed 127
Figure 6.3 Wireshark snapshot of (a) IEEE C37.118 PMU data (b) IEC 61850-90-5 R-GOOSE messages (c) IEC 61850 GOOSE messages 128
Figure 6.4 R-GOOSE packets (a) Before implementing security mechanism (b) After implementing AEAD security..... 131

LIST OF TABLES

Table 1.1 Allowed latencies in various WAMS applications 8
Table 2.1 Denial-of-Service attacks executed on the WAMS Testbed 38
Table 3.1 Working of DoS pre-emptive modules in the framework 53
Table 3.2 Performance of Security/Dependability Adaptive Relaying protection scheme in conventional WAMS framework and proposed WAMS framework 61
Table 4.1 Working of the proposed DoS mitigation framework 67
Table 4.2 Phasors from each PMU in PDC datastream 72
Table 4.3 Best combination of ODAE model hyperparameters 73
Table 5.1 Working of the proposed attack detection and mitigation methodology in different scenarios 112

LIST OF ABBREVIATIONS AND SYMBOLS

ICS-CERT	:	Industrial Control Systems Cyber Emergency Response
DoE	:	Department of Energy
NATO	:	North Atlantic Treaty Organization
CCDCOE	:	Cooperative Cyber Defense Center of Excellence
NIST	:	National institute of Standard and Technology
OT	:	Operational Technology
ISO	:	International Organization for Standardization
CEA	:	Central Electricity Authority
SCADA	:	Supervisory Control and Data Acquisition
WAMS	:	Wide area measurement systems
PMU	:	Phasor Measurement Units
PDC	:	Phasor Data Concentrators
GPS	:	Global Positioning System
IEEE	:	Institute of Electrical and Electronics Engineers
IEC	:	International Electrotechnical Commission
TCP	:	Transmission Control protocol
UDP	:	User Datagram Protocol
fps	:	Frames Per Second
WAMPAC	:	Wide Area Monitoring, Protection And Control
WAPAC	:	Wide Area Protection And Control
IED	:	Intelligent Electronic Devices
GOOSE	:	Generic Object-Oriented Substation Events
R-GOOSE	:	Routable Generic Object-Oriented Substation Events
R-SV	:	Routable Sample Values
FDIA	:	False Data Injection Attacks
NASPI	:	North American SynchroPhaser Initiative
WAN	:	Wide Area Network
DoS	:	Denial-of-Service
CIA	:	Confidentiality Integrity Availability

FISMA	:	Federal Information Security Modernization Act
IT	:	Information Technology
BCU	:	Bay Control Unit
WAMAP	:	Wide Area Monitoring And Protection
WECC	:	Western Electricity Coordinating Council
NERC	:	North American Electric Reliability Council
DFT	:	Digital Fourier Transform
HIL	:	Hardware-in-Loop
MPTCP	:	Multi-Path Transmission Control Protocol
ML	:	Machine Learning
DL	:	Deep Learning
CNN	:	Convolutional Neural Network
DAE	:	Denoising Autoencoders
SVM	:	Support Vector Machine
HTT	:	Hilbert Huang Transform
VMD	:	Variational Mode Decomposition
HVDC	:	High Voltage Direct Current
MAC	:	Message Authentication Code
IIT	:	Indian Institute of Technology
RTDS	:	Real-Time Digital Simulator
NaN	:	Not a Number
RF	:	Random Forest
ARP	:	Address Resolution Protocol
KNN	:	K-Nearest Neighbors
ODAE	:	Overcomplete Denoising Autoencoder
ReLU	:	Rectified Linear Unit
CPU	:	Central Processing Unit
RAM	:	Random Access Memory
NRIPG	:	Northern Region of the Indian Power Grid
LSTM	:	Long Short-Term Memory
GAN	:	Generative Adversarial Network

GAIN	:	Generative Adversarial Imputation Nets
LAN	:	Local Area Network
AEAD	:	Authenticated Encryption with Associated Data
SLDC	:	State Load Dispatch Center
RLDC	:	Regional Load Dispatch Center
ICS	:	Industrial Control System
GTAO	:	Giga-Transceiver Analogue Output
GTNET	:	Giga-Transceiver Network
SEL	:	Schweitzer Engineering Laboratories
IRIG	:	Inter-Range Instrumentation Group
BNC	:	Bayonet Neill–Concelman
CB	:	Circuit Breaker
SCL	:	Substation Configuration Language
ICD	:	IED Capability Description
CID	:	Configured IED Description
TVE	:	Total Vector Error
UTC	:	Coordinated Universal Time
LD	:	Logical Device
LN	:	Logical Node
DO	:	Data Object
ACSI	:	Abstract Communication Service Interface
MMS	:	Manufacturing Message Specification
OSI	:	Open System Interconnection
VPN	:	Virtual Power Network
PDU	:	Protocol Data Unit
BER	:	Basic Encoding Rules
DBAD	:	PDC Data Based Anomaly Detector
RDPS	:	Random Data Path Selector
ASD	:	ARP Spoofing Detector
DFD	:	DoS Fingerprint Detector
MUX	:	Multiplexer

spyder	:	Scientific Python Development Environment
UP	:	Uttar Pradesh
MSE	:	Mean Squared Error
SoE	:	Sequence of Events
DR	:	Disturbance Recorder
ARIMA	:	Autoregressive Integrated Moving Average
RNN	:	Recurrent Neural Networks
DT	:	Decision Tree
HMAC	:	Hash Message Authentication Code
GMAC	:	Galois Message Authentication Code
SHA	:	Secure Hash Algorithm
AES	:	Advanced Encryption Standard
APDU	:	Application Protocol Data Unit
sqNum	:	Sequence Number
stNum	:	Status Number
T_{sol}	:	Total time involved in all the modules in suggested cybersecurity solutions
T_C	:	Communication delay in conventional WAMS Framework
s	:	seconds
ms	:	milliseconds
μs	:	microseconds
dB	:	Decibel
KV	:	Kilovolt
f	:	Frequency
I	:	Current
V	:	Voltage
δ	:	Phase angle
P	**:**	PDC Datastream
N	:	Total Number of PMU