Application-Based Measures for Developing Cyber-Resilient Control and Protection Schemes in Power Networks

by

Amir Ameli

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2019

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

Supervisor	Ehab F. El-Saadany Professor
Co-supervisor	Ramadan El-Shatshat Lecturer
External Examiner	Deepa Kundur Professor
Internal Member	Magdy Salama Professor
Internal Member	Kankar Bhattacharya Professor
Internal-external Member	Paul Fieguth Professor

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Electric power systems are a part of the most-crucial infrastructure on which societies depend. In order to operate efficiently and reliably, the physical layer in large electric power networks is coupled with a cyber system of information and communication technologies, which includes compound devices and schemes, such as Supervisory Control and Data Acquisition (SCADA) systems and Intelligent Electronic Devices (IEDs). These communication-base schemes and components are mainly a part of protection and control systems, which are known as the backbones of power networks, since the former detects abnormal conditions and returns the system to its normal state by initiating a quick corrective action, and the latter preserves the integrity of the system and stabilizes it following physical disturbances. This dissertation concentrates on the cyber-security of protection and control systems in power networks by unveiling a vulnerable protective relay, i.e., the Line Current Differential Relay (LCDR), and a susceptible controller, i.e., the Automatic Generation Control (AGC) system, and proposing application-based measures for making them robust against cyber threats.

LCDRs are a group of protective relays that are highly dependent on communication systems, since they require time-synchronized remote measurements from all terminals of the line they are protecting. In AC systems, this type of relay is widely used for protecting major transmission lines, particularly higher voltage ones carrying giga-watts of power. On the other hand, due to the limitations of other protection schemes, LCDRs has been identified as a reliable protection for medium-voltage lines in DC systems. Therefore, the cyber-security of LCDRs is of great importance. On this basis, this dissertation first shows the problem in both AC and DC systems and reveals the consequences and destructiveness of cyber-attacks against LCDRs through case studies. Then, it presents three solutions to address his problem, two for AC networks and one for DC grids. For AC systems, this dissertation presents two methods, one that can be used for Sampled Value (SV)-based LCDRs, and another one that works for both SV-based and phasor-based relays. Both methods are initiated after LCDRs pickup, to confirm the occurrence of faults and differentiate them from cyber-attacks. To detect attacks, the first method compares the estimated and locally-measured voltages at LCDR's local terminal during faults for both Positive-Sequence (PS) and Negative-Sequence (NS). To estimate the local voltage

for each sequence, the proposed technique uses an Unknown Input Observer (UIO), the state-space model of the faulty line, and remote and local measurements, all associated with that sequence. The difference between the measured and estimated local voltages for each sequence remains close to zero during real internal faults because, in this condition, the state-space model based on which the UIO operates correctly represents the line. Nevertheless, the state-space model mismatch during attacks leads to a large difference between measured and estimated values in both sequences.

The second proposed method for an AC LCDR detects attacks by comparing the calculated and locally-measured superimposed voltages in each sequence after the relay picks up. A large difference between the calculated and measured superimposed voltages in any sequence reveals that the remote current measurements are not authentic. Given that local measurements cannot be manipulated by cyber-attacks, any difference between the calculated and measured superimposed voltages is due to the inauthenticity of remote current measurements.

The proposed method for DC LCDRs is comprised of Passive Oscillator Circuits (POCs) installed in series with each converter. During faults, the resultant RLC circuit causes the POCs to resonate and generate a damped sinusoidal component with a specific frequency. However, this specific frequency is not generated during cyber-attacks or other events. Thus, LCDRs' pickup without detecting this specific frequency denotes a cyber-attack. Given that the frequency extraction process is carried out locally by each LCDR, the proposed approach cannot be targeted by cyber-attacks.

On the other hand, an AGC system, which is the secondary controller of the Load Frequency Control (LFC) system, is a communication-dependent vulnerable controller that maintains tie-lines' power at their scheduled values and regulates grid frequency by adjusting the set-points of a power plant's governors. This dissertation proves the destructiveness of cyber-attacks against AGC systems by proposing a Stealthy Hybrid Attack (SHA) that disrupts the normal operation of the AGC system quickly and undetectably. Afterwards, two methods are proposed for detecting and identifying intrusions against AGC systems. Both methods work without requiring load data in the system, in contrast to other methods presented in the literature. To detect attacks, the first method estimates the LFC system's states using a UIO, and calculates the UIO's Residual Function (RF), defined

as the difference between the estimated and measured states. In normal conditions, the estimated and measured values for LFC states are ideally the same. Therefore, an increase in the UIO's RF over a predefined threshold signifies an attack. This method also identifies attacks, i.e., determines which system parameter(s) is (are) targeted, by designing a number of identification UIOs.

The general idea behind the second proposed method for detecting and identifying attacks against AGC systems is similar to the first one; yet, the second one takes into account the effect of noise as well. Therefore, instead of a UIO, the second method utilizes a Stochastic Unknown Input Estimator (SUIE) for estimating the states of the LFC system and minimizing the effect of noise on the estimated states. Similarly, increasing the SUIE's RF over a predefined threshold indicates the occurrence of an attack.

Acknowledgments

First and foremost, I would like to express my sincere gratitude to my supervisor, professor *Ehab El-Saadany*, for his continuous support, patience, encouragement, enthusiasm, and immense knowledge. During my PhD studies, whenever I came out of his office, I was more determined, confident, and motivated than when I had entered that office. Additionally, I would like to deeply thank *Dr. Ramadan El-Shatshat* for being my co-supervisor.

I would like to sincerely thank my colleague and friend, *Dr. Ali Hooshyar*, for his endless support. He was always reachable and never hesitated to help me out. I count myself lucky to have had Dr. Hooshyar on board during my PhD studies, and I treasure my collaboration with him.

My heartfelt appreciation also goes to Dr. Amr Youssef from the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, for his constantly-available help and support during my research.

I am honored that this dissertation has been examined by Dr. Magdy Salama, Dr. Kankar Bhattacharya, Dr. Deepa Kundur, and Dr. Paul Fieguth. I owe respect and thanks to them for their time and insight.

Special thanks to my colleague, soon-to-be Dr. Ameen Yazdavar, for the fruitful technical discussions and collaborations we had over these years. Additionally, I appreciate the help and support of my other colleagues, Dr. Khaled Saleh, and Mr. Aram Kirakosyan.

I will always be indebted to Ms. Mary McPherson, from the Writing and Communication Center, who spent her, often personal, time helping me with sheer benevolence. I have been learning a lot from her.

I owe a lot to my parents, whose clear trace of devotion and dedication is visible in all of my accomplishments to date. I always fall short of words when it comes to describing their support. I am also thankful to my sister, Somaieh—may she rest in peace—and my brother, Soroush, for their support and love.

Last but not least, I wish to express my deepest gratitude to my beloved *Parisa*, my wife and my best friend. Traces of her encouragement, patience, and love can be found behind whatever I have achieved in the last five years. It is really unfair that my Parisa's

name does not appear on the first page of this dissertation, since her contribution is by no means less than mine.

to
Maman, Baba
& My beloved Parisa

Table of Contents

List of Tables xiii

List of Figures xv

List of Abbreviations xxi

List of Symbols xxv

1 Introduction 1

1.1 Line Current Differential Relay, a Vulnerable Protection Scheme 3

1.2 Automatic Generation Control System, a Vulnerable Control Scheme . . . 5

1.3 Research Objectives 6

1.4 Dissertation Outline 8

2 Vulnerability of LCDRs to Cyber-Attacks: Background and Problem Statement 10

2.1 Working Principal of LCDRs 11

2.1.1 AC LCDRs 11

2.1.2 DC LCDRs 13

2.2 Vulnerability of LCDRs to Cyber-Attacks 14

2.2.1 Communication and Time-Synchronization Media, Protocols, and Susceptibilities . . . 14
2.3 Tripping AC Lines by Targeting LCDRs . . . 16
2.3.1 Targeting Phasor-Based AC LCDRs by Cyber-Attacks . . . 16
2.3.2 Targeting SV-Based AC LCDRs by Cyber-attacks . . . 21
2.3.3 Activating the DD Elements of Target LCDRs . . . 22
2.4 Tripping DC Lines by Targeting LCDRs . . . 24
2.5 Attack Model and Analysis . . . 25
2.5.1 Attackers' Motives and Objectives . . . 25
2.5.2 Assumptions and Attackers' Capabilities and Constraints . . . 26
2.6 Case Studies . . . 27
2.6.1 Case Study 1 . . . 27
2.6.2 Case Study 2 . . . 32
2.6.3 Case Study 3 . . . 35
2.7 Conclusion . . . 42

3 Attack Detection Method for SV-based AC LCDRs 43
3.1 State-Space Model of AC Transmission Lines During Internal Faults . . . 44
3.2 A UIO for State Estimation in the Presence of Unknown Inputs . . . 47
3.2.1 Accuracy of UIO . . . 49
3.2.2 Stability of UIO . . . 52
3.3 Attack Diagnosis Using UIO . . . 55
3.3.1 State-space Model of AC Lines During FDIAs and TSAs . . . 56
3.3.2 Attack Detection Scheme . . . 57
3.4 Performance Evaluation . . . 60

3.5 Determining tr^+ and tr^- . . . 61
3.6 Evaluation Scenarios . . . 64
3.7 Conclusion . . . 71

4 Attack Detection Method for SV-based and Phasor-based AC LCDRs 73
4.1 System Model . . . 74
4.2 Proposed Attack Detection Method . . . 78
4.2.1 OTI between LCDR's terminals and fault location . . . 78
4.2.2 Calculating Local Superimposed Voltage . . . 80
4.2.3 Detecting Attacks . . . 81
4.3 Performance Evaluation . . . 83
4.3.1 Off-line Simulations . . . 83
4.3.2 Real-Time Simulation . . . 88
4.4 Conclusion . . . 92

5 Attack Detection Method for DC LCDRs in Medium-Voltage DC Systems 94
5.1 The Proposed Attack Detection Method for DC LCDRs . . . 95
5.1.1 Augmenting DC LCDRs with POCs . . . 95
5.1.2 Selection Criteria for f_d . . . 97
5.1.3 Relation between f_d and f_0 . . . 98
5.1.4 f_d Detection for Attack Diagnosis . . . 103
5.2 Performance Evaluation . . . 104
5.3 Conclusion . . . 112

6 Vulnerability of AGC systems to Cyber-Attacks: Background, Problem Statement, and System Modeling 114

6.1 AGC System's Operating Principal and Alarms . . . 115

6.2 Attack Model and Analysis . . . 116

6.2.1 Attackers' Motives and Objectives . . . 117

6.2.2 Assumptions and Attackers' Capabilities and Constraints . . . 117

6.3 FDIAs against AGC Systems . . . 118

6.3.1 Over-/under-compensation attacks . . . 118

6.3.2 Negative-compensation attacks . . . 120

6.3.3 Formulation of an SHA . . . 122

6.4 LFC System Modeling . . . 126

6.4.1 The State-Space Model of an N-Area LFC System During Normal Condition . . . 127

6.4.2 The State-Space Model of an N-Area LFC system during FDIAs . . . 133

6.5 Conclusion . . . 135

7 Attack Detection and Identification for Automatic Generation Control Systems 136

7.1 Development of a UIO for LFC Systems . . . 137

7.2 Proposed Detection and Identification Schemes . . . 140

7.2.1 Attack Detection Scheme . . . 140

7.2.2 Type Identification Scheme . . . 142

7.3 Performance evaluation . . . 145

7.3.1 Three-Area Test System . . . 145

7.3.2 39-Bus New England Test System . . . 148

7.4 Conclusion . . . 154

8 Attack Detection and Identification for Automatic Generation Control Systems in the Presence of Noise 155

8.1 Development of a SUIE for LFC system 156

8.1.1 Development of a SUIE for ALFCS 161

8.1.2 Relation Between ALFCS and OLFCS 167

8.2 FDIA Diagnosis Using SUIE 167

8.2.1 FDIA Detection 167

8.2.2 FDIA Type Identification 170

8.3 Performance Evaluation 172

8.3.1 Off-line Simulation 172

8.3.2 Real-Time Simulation 178

8.3.3 Comparative Analysis 182

8.4 Conclusion 184

9 Conclusions 186

9.1 Summary 186

9.2 Contributions 189

9.3 Directions for Future Work 190

References 191

APPENDICES 206

A Description of the 39-bus new England Test System in Chapters 2, 3, 4, and 7 207

B Description of the DC Test System in Chapters 2 and 5 211

C Description of the Three-Area Test System in Chapters 6, 7, and 8 **213**

D Proof of Theorem 5 **215**

E Feasibility of Stealthy FDIAs Against AGC Systems **222**

F List of Publications **225**

F.1 Peer-Reviewed Journal Articles 225

F.2 Submitted Journal Articles 226

F.3 Under-Preparation Journal Articles 226

F.4 Conference Proceedings 226

List of Tables

5.1 Maximum obtained $V^{+}_{FFT,5}$, $V^{+}_{FFT,2}$, $V^{-}_{FFT,5}$, and $V^{-}_{FFT,2}$ during various faults in Scenario 3 (all in volts). 109

5.2 Maximum obtained $V^{+}_{FFT,5}$ during PPG and PP faults, and captured $V^{-}_{FFT,5}$ during NPG faults of Scenario 4 (all in volts). 109

5.3 Comparison between the peak current of Bus 5's VSC during faults, with and without installing POCs. 111

6.1 Area i's Frequency Deviation and ACE Signal During Over-/Under-/Negative-Compensation Attacks 120

6.2 Area i's ACE and frequency deviation during an SHA 123

7.1 UIOs for Area 1 of the Three-Area Power System 144

7.2 Identification Logic for Area 1 of The Three-Area Test System 144

8.1 AISUIEs for Area 1 of The Three-Area Power System 171

8.2 Identification Logic for Area 1 of The Three-Area Test System 172

A.1 Generators' voltage and power in 39-bus New England system 208

A.2 Transmission line characteristics of 39-bus New England system 209

A.3 Load characteristics of 39-bus New England system 210

C.1 Generator Specifications for the Three-Area Test System 214

C.2 LFC System Parameters in Each Area of the Three-Area Test System . . . 214
C.3 Generated and Consumed Powers in the Three-Area Test System 214

List of Figures

1.1 Diagram of Research Objectives. 7

2.1 LCDR characteristic [1]. 12

2.2 39-bus new England system. 17

2.3 Operating point trajectory of LCDRs during MMAs. 18

2.4 LCDR I's trajectory during the MMA, PMA, and TSA. 19

2.5 The locus of solutions of (2.21) for Line 6-11 of the test system. 21

2.6 PS current measured by LCDR I after switching the shunt capacitor bank installed on Bus 12, (a) magnitude, (b) angle. 23

2.7 PS current measured by LCDR I after switching the series capacitor bank installed in Line 5-8, (a) magnitude, (b) angle. 23

2.8 PS current measured by LCDR I after 20% load change at bus 8, (a) magnitude, (b) angle. 24

2.9 IEEE 14-bus test systems used for simulations. 28

2.10 Attack tree showing intrusions that lead to voltage collapse and Small signal instability. 29

2.11 PS current entering Line 2-5 from Bus 5 after switching on the shunt capacitor bank installed at Bus 5 at $t = 20$ ms, (a) magnitude, (b) angle. 30

2.12 The trajectory of targeted LCDR of Line 2-5 during the FDIA. 31

2.13 PS current entering Line 2-4 from Bus 2 after the tripping of Line 2-5 at $t = 45$ ms, (a) magnitude, (b) angle. 31
2.14 PV curves at Bus 5 during case study 1. 32
2.15 Eigenvalues of the system when Lines 2-5 and 2-4 are tripped. 32
2.16 PV curve at Bus 5 after tripping Line 1-5. 33
2.17 The trajectory of targeted LCDR of Line 6-11 during the FDIA. 34
2.18 PS current entering Line 13-14 from Bus 14 after Line 6-11 is tripped at $t = 45$ ms, (a) magnitude, (b) angle. 34
2.19 PS current entering Line 2-3 from Bus 2 after Line 13-14 is tripped at $t = 70$ ms, (a) magnitude, (b) angle. 35
2.20 Over-loaded lines and their currents after the coordinated attacks. 36
2.21 Frequencies of generators after the coordinated attacks, (a) over-frequency, (b) under-frequency (Generator 2). 36
2.22 DC test system. 37
2.23 (a) Current of Line 4-3 after tripping of Line 2-5, (b) differential current of LCDR installed at Bus 4. 38
2.24 (a) Current of Line 2-3 after tripping of Line 2-5, (b) differential current of LCDR installed at Bus 2. 38
2.25 Current of Line 1-5 after tripping of Lines 2-5 and 3-4. 40
2.26 Voltage at Bus 1 after tripping Line 1-5, and the effect of load shedding scheme on voltage stability. 40
2.27 Line 1-2's current after tripping Line 1-5 and disconnecting the load on Bus 1. 40
2.28 Voltage at Bus 5 after tripping Line 1-2. 41

3.1 A two-terminal transmission line during internal faults. 45
3.2 A two-terminal transmission line during FDIAs. 56
3.3 Tripping logic of LCDRs after implementing the proposed method. 60

3.4 Added noise to voltage and current waveforms. 62
3.5 Primary and secondary currents of CTs installed at Buses 6 and 11 for different levels of saturation, (a) VFS, (b) FS, (C) MS. 63
3.6 Equivalent model for utilized CCVTs. 63
3.7 PS results for the case in which maximum $r^{+}[k]$ occurred, (a) Estimated and measured voltages for Bus 11, (b) RF. 64
3.8 NS results for the case in which maximum $r^{-}[k]$ occurred, (a) Estimated and measured voltages for Bus 11, (b) RF. 64
3.9 The location of the fault obtained by the utilized fault location technique. 65
3.10 Estimated and measured voltages for Bus 11 in Scenario 1, (a) PS, (b) NS. 66
3.11 RFs of Scenario 1, (a) PS, (b) NS. 66
3.12 PS results obtained for Scenario 2, (a) Estimated and measured voltages for Bus 11, (b) RF. 67
3.13 Estimated and measured voltages for Bus 11 in Scenario 3, (a) PS, (b) NS. 67
3.14 RFs of Scenario 3, (a) PS, (b) NS. 68
3.15 PS results obtained for Scenario 4, (a) Estimated and measured voltages for Bus 11, (b) RF. 68
3.16 PS results obtained for Scenario 5, (a) Estimated and measured voltages for Bus 11, (b) RF. 69
3.17 Estimated and measured voltages for Bus 11 in Scenario 6, (a) PS, (b) NS. 70
3.18 RFs of Scenario 6, (a) PS, (b) NS. 70
3.19 Estimated and measured voltages for Bus 11 in Scenario 7, (a) PS, (b) NS. 71
3.20 RFs of Scenario 7, (a) PS, (b) NS. 71

4.1 The equivalent model of the test system. 75
4.2 Model of the test system during internal faults (a) PS, (b) NS. 76

4.3 Tripping logic of LCDRs after implementing the proposed method. 82
4.4 Flowchart of the proposed method 83
4.5 Superimposed voltages at bus 11 during Scenario 1, (a) PS, (b) NS. 85
4.6 Superimposed voltages at bus 11 during Scenario 2, (a) PS, (b) NS. 85
4.7 PS Superimposed voltages at bus 11 during (a) Scenario 3, (b) Scenario 4. 86
4.8 PS superimposed voltages at bus 11 during Scenario 5, (a) PMA, (b) TSA. 87
4.9 Superimposed voltages at bus 11 during Scenario 6, (a) PS, (b) NS. 87
4.10 Primary and secondary currents of the CT installed at Bus 6 for different levels of saturation, (a) VFS, (b) FS, (C) MS. 89
4.11 Superimposed voltages at bus 11 during Scenario 7, (a) PS, (b) NS. 90
4.12 HIL setup. 90
4.13 Superimposed voltages at bus 11 obtained from RTS during Scenario 1, (a) PS, (b) NS. 91
4.14 Superimposed voltages at bus 11 obtained from RTS during Scenario 6, (a) PS, (b) NS. 91
4.15 Superimposed voltages at bus 11 obtained from RTS during Scenario 8, (a) PS, (b) NS. 92

5.1 Attack Detection scheme for LCDRs of a DC Line after including POCs. . 95
5.2 System model during capacitor discharge stage, (a) PG fault, (b) PP fault. 96
5.3 Eigenvalues of the system during capacitor discharge stage when a fault with $R_f = 0\ \Omega$ happens on Line 2-5 of the test system at $x = 0.25$. 99
5.4 f_d generated during PG faults when, (a) only x and R_f change, (b) x, R_f, and line length ($\mathcal{L}_{dc}$) change, (c) x, R_f, and converters' capacitors (C_{c1} and C_{c2}) change, and (d) x, R_f, and f_0 change. 100
5.5 f_d generated during PP faults when, (a) only x and R_f change, (b) x, R_f, and line length ($\mathcal{L}_{dc}$) change, (c) x, R_f, and converters' capacitor (C_{c1} and C_{c2}) change, and (d) x, R_f, and f_0 change. 102

5.6 Tripping logic for each pole after implementing the proposed method. . . . 104

5.7 $v^+_{POC,5}$ and $V^+_{FFT,5}$ during Scenario 1 (a) $v^+_{POC,5}$, (b) $V^+_{FFT,5}$. 106

5.8 $V^+_{FFT,4}$ and $V^-_{FFT,4}$ during Scenario 2 (a) $V^+_{FFT,4}$, (b) $V^-_{FFT,4}$. 106

5.9 $v^+_{POC,5}$ and $v^+_{POC,2}$ during a PPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5. 107

5.10 $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during a PPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$. 107

5.11 $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during an NPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$. 108

5.12 $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during a PP fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$. 108

5.13 $V^+_{FFT,5}$ during (a) PP faults with $R_f = 200\ \Omega$, (b) PPG faults with $R_f = 1\ \Omega$. 110

5.14 Current and voltage of Bus 5's VSC during a bolted PP fault at $x = 0.1$ from Bus 5 on Line 5-2, (a) Positive pole's current (b) voltage. 111

5.15 Magnitude of frequency component oscillating with f_d in Scenario 6: (a) $V^+_{FFT,5}$, (b) $V^-_{FFT,5}$, (c) $V^+_{FFT,2}$, and (d) $V^-_{FFT,2}$. 112

6.1 AGC system architecture. 116

6.2 Single-line diagram of the three-area test system. 119

6.3 System frequency during over-/under-/negative-compensation attacks. . . . 121

6.4 ACE signal of Area 1 during over-/under-/negative-compensation attacks. 121

6.5 The real and manipulated frequencies during an SHA. 126

6.6 ACE signal of Area 1 during an SHA that increase the frequency. 126

6.7 Linearized model of LFC system for area i. 127

7.1 Main UIO's RF, (a) Without noise, (b) With noise. 146

7.2 Scenario 1's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C. 147

7.3 Scenario 2's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C. 148

7.4 Scenario 3's RFs, (a) Main UIO, (b) UIO *A*, (c) UIO *B*, (d) UIO *C*. 149
7.5 Scenario 4's RFs, (a) Main UIO, (b) UIO *A*, (c) UIO *B*, (d) UIO *C*. 150
7.6 Single-line diagram of 39-bus New England test system. 151
7.7 Scenario 5's RFs, (a) UIO *E*, (b) UIO *F*, (c) UIO *G*, (d) UIO *H*. 152
7.8 Scenario 6's RFs, (a) UIO *E*, (b) UIO *F*, (c) UIO *G*, (d) UIO *H*. 153
7.9 Scenario 7's RFs, (a) UIO *E*, (b) UIO *F*, (c) UIO *G*, (d) UIO *H*. 153
7.10 RF of UIO *I* during Scenario 7. 154

8.1 Flowchart of state estimation for the ALFCS using a SUIE. 166
8.2 Main SUIE's RF considering noise and parameter uncertainties. 174
8.3 Main SUIE's RF, (a) Scenario 1, (b) Scenario 2. 174
8.4 Scenario 3 RFs, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*.175
8.5 Scenario 4 RFs, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*.176
8.6 Scenario 5 RFs, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*.177
8.7 RF of AISUIE *G* during Scenario 5. 178
8.8 Scenario 6 RFs, (a) AISUIE *A*, (b) AISUIE *B*, (c) AISUIE *C*, (d) AISUIE *G*.178
8.9 HIL setup. 179
8.10 Scenario 4 RFs obtained by RTS, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*. 180
8.11 Scenario 7 RFs obtained by RTS, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*. 181
8.12 Load and wind generation profiles used for comparative analysis (a) Load, (b) Wind generation. 182
8.13 Parameters of the method proposed by [2] obtained for Scenario 7, (a) ACE_{max} and ACE_{min}, (b) δ_2. 183
8.14 Main SUIE's RF during Scenario 7. 184
8.15 System frequency during Scenario 8. 184

List of Abbreviations

ACE	Area Control Error.
AGC	Automatic Generation Control.
AISUIE	Attack Identification Stochastic Unknown Input Estimator.
ALFCS	Augmented LFC system.
AVR	Automatic Voltage Regulator.
CCVT	Coupling Capacitor Voltage Transformer.
CEO	Chief Executive Officer.
CT	Current Transformer.
DD	Disturbance Detector.
DG	Distributed Generation.
DNP3	Distributed Network Protocol Version 3.0.
DoSA	Denial of Service Attack.
ESTE	External System Thevenin Equivalent.
FDIA	False Data Injection Attack.
FFT	Fast Fourier Transform.
FS	Fast Saturation.
GPS	Global Positioning System.

HB	Hopf Bifurcation.
HIL	Hardware-In-The-Loop.
IED	Intelligent Electronic Device.
IGBT	Insulated-Gate Bipolar Transistor.
IRIG-B	Inter-Range Instrumentation Group Code B.
LAN	Local Area Network.
LCDR	Line Current Differential Relay.
LFC	Load Frequency Control.
LSM	Least Square Method.
MMA	Magnitude Modification Attack.
MS	Mild Saturation.
NERC	North American Electric Reliability Corporation.
NPG	Negative Pole-to-Ground.
NS	Negative-Sequence.
OFR	Over Frequency Relay.
OTI	Open-Circuit Transfer Impedance.
PG	Pole-to-Ground.
PMA	Phase Modification Attack.
POC	Passive Oscillator Circuit.
PP	Pole-to-Pole.
PPG	Positive Pole-to-Ground.

PS	Positive-Sequence.
PTP	Precision Timing Protocol.
PV	Photovoltaic.
RF	Residual Function.
RISI	Repository for Industrial Security Incidents.
ROCOF	Rate-of-Change-of-Frequency.
RTS	Real-Time Simulator.
SCADA	Supervisory Control and Data Acquisition.
SDH	Synchronous Digital Hierarchy.
SHA	Stealthy Hybrid Attack.
SNB	Saddle-Node Bifurcation.
SNR	Signal-to-Noise Ratio.
SONET	Synchronous Optical Network.
SUIE	Stochastic Unknown Input Estimator.
SV	Sampled Value.
TSA	Time Synchronization Attack.
UFLS	Under Frequency Load Shedding.
UFR	Under Frequency Relay.
UIO	Unknown Input Observer.
VFS	Very Fast Saturation.
VSC	Voltage-Source Converter.
WAN	Wide Area Network.

ZS Zero-Sequence.

List of Symbols

B_i	Area i's frequency bias.
C_p	Capacitance of passive oscillating circuits.
C_{conv}	Capacitance of converters.
D	Duty-cycle of converters.
D_{e_i}	Equivalent damping coefficient of Area i.
G_i	Number of generators in Area i.
H_i	Equivalent inertia constant of Area i.
I_b	Breaking point in differential-restraining characteristic of line current differential relays.
I_t	Voltage vector including all terminals voltage phasors.
I_{d0}	Minimum pickup current in differential-restraining characteristic of line current differential relays.
$I_{diff,dc}[k]$	Differential current of DC line current differential relays.
I_{diff}	Differential current.
I_{inj}	Injection current to terminal buses.
$I^s_{k,pp}$	Fault current phasor in sequence s.
I_{nom}	Nominal current of lines.
$I_n[k]$	The current phasor entering the n-th terminal of a line at time-step k.
I_{op}	Operating function of line current differential relays.

I_{res}	Restraining current.
$I_{res}[k_0]$	Restraining current before the initiation of an attack.
L_p	Inductance of passive oscillating circuits.
L_{conv}	Inductance of converters.
N	Total number of terminals of a line.
R_f	Fault resistance.
$R_{g,i}$	Governor's time constant of the g-th generator of Area i.
T	Transpose operator.
T_s	Discretization time step.
T_{AGC}	Interval between two successive operations of AGC.
$T_{ch_{g,i}}$	Turbine's time constant of generator g n Area i.
$T_{g_{g,i}}$	Droop coefficient of the g-th generator of Area i.
T_{ij}	Synchronizing power coefficient between areas i and j.
V_t	Current vector including all terminals current phasors.
$V^p_{FFT,b}$	Magnitude of the component with the frequency of f_d obtained from the voltage across the POC installed at Bus b on pole p.
Y_L	Admittance matrix of the line.
ΔP_{L_i}	Mismatch between the load and generation of Area i.
$\Delta V^s_{n,c}$	Calculated superimposed voltages for the sequense s.

$\Delta V^s_{n,m}$	Measured superimposed voltages for the sequense s.
Δf^*	Attacker's target frequency.
$\Delta P_{c_{g,i}}$	Power generation set point of Generator g in Area i.
ΔP_{m_i}	Sum of Area i's generators' mechanical power deviations.
$\Delta P_{m_{g,i}}$	Mechanical power deviation of the g-th generator in Area i.
ΔP_{tie_i}	Sum of Area i's tie-lines' power deviations.
$\Delta P_{tie_{i,j}}$	Active power deviation of the tie-line that connects areas i and j.
$\Delta P_{v_{g,i}}$	Deviation of valve position of Generator g's turbine in Area i.
$\Delta\dot{\omega}_i$	Derivative of frequency deviation with respect to time.
$\Delta\omega_i$	Angular frequency deviation of Area i.
$\Delta f_{\max}$	Maximum frequency deviation that does not raise an alarm.
Φ	Any voltage or current whose instantaneous positive- or negative-sequence components is required.
Φ_i	Number of generators controlled by AGC in Area i.
α	Unknown input observer's delay.
δ^s_n	Difference between the measures and calculated superimposed voltages at terminal n in percent for sequence s.

η	Required number of time steps for an attack.
γ	Maximum permissible slope of the frequency curve.
$\hat{v}_1^s[k]$	Estimated local voltage at time-step k.
κ	Reliability coefficient of DC line current differential relays.
λ	Maximum permissible ACE curve's slope.
$\overline{\mathbb{A}}$	Descritized state matrix during attacks.
$\overline{\mathbb{A}}_c$	Continuous state matrix during attacks.
$\overline{\mathbb{B}}_{c,ca}$	Continuous attack matrix.
$\overline{\mathbb{U}}_{ca}[k]$	Attack input vector at time step k.
$\mathbb{A}_c$	Continuous state matrix.
$\mathbb{B}_u$	Discretized unknown input matrix.
$\mathbb{B}_{c,n}$	Continuous known input matrix.
$\mathbb{B}_{c,u}$	Continuous unknown input matrix.
$\mathbb{C}$	Output matrix.
$\mathbb{Q}[k]$	Descritized process noise covariance matrix at time step k.
$\mathbb{Q}_c(t)$	Continuous process noise covariance matrix at time t.
$\mathbb{R}[k]$	Descritized measurement noise covariance matrix at time step k.
$\mathbb{R}_c(t)$	Continuous measurement noise covariance matrix at time t.
$\mathbb{U}_n^s$	Known input vector.
$\mathbb{V}_c(t)$	Measurement noise vector at time t.
$\mathbb{W}_c(t)$	Process noise vectors at time t.
$\mathbb{X}^s$	State vector for sequence s.
$\mathbb{X}^s[k]$	Estimate for system states.

$\mathbb{Y}_i(t)$	Output vector of state-space model at time t.
$\overline{\mathbb{B}}_{c,n}$	Continuous known input matrix during attacks.
$\overline{\mathbb{B}}_{ca}$	Descritized attack matrix.
$\overline{\mathbb{B}}_n$	Descritized state matrix during attacks.
$\mathcal{C}$	Set of all complex numbers.
$\mathcal{L}$	Gain of unknown input observers.
$\mathcal{L}_{dc}$	Length of the DC line.
ζ	Damping factor.
bp	Subscript denoting before-pickup values.
$e^s\left[k+1\right]$	Error of unknown input observers for sequence s.
f	System frequency.
f_0	Natural frequency.
f_d	Resonance frequency of passive oscillating circuits.
f_s	Sampling frequency.
h_i^s	Attack vector targeting remote current measurements.
h_v^s	Attack vector targeting remote voltage measurements.
$i_{POC,m}^+$	Current of the inductor of the POCs installed on the terminal of converter m on the positive-pole.
$i_{POC,n}^+$	Current of the inductor of the POCs installed on the terminal of converter n on the positive-pole.
i_{cm}	Currents of DC link capacitor of converter m.
i_{cn}	Currents of DC link capacitor of converter n.

$i_n[k]$	Sampled value of the current entering the n-th terminal of a line at time-step k.
k_1	The lower percentage restraining settings of line current differential relays.
k_2	The lower percentage restraining settings of line current differential relays.
$k_{\phi,i}$	Gain of ϕ-th AGC.
m_i^{k+s}	Time-variant attack multiplier at time-step k after the initiation of the attack.
p	Superscript denoting positive-pole or negative-pole.
pp	Subscript denoting post-pickup values.
$r^s[k]$	Residual function associated with submodule of sequence s at time-step k.
$r_j[k]$	Residual function of the j-th identification UIO at time sep k.
tr^*	Threshold of the UIO.
tr^s	Detection threshold for sequence s.
tr_b^p	Attack detection threshold of Bus b for pole p.
tr_j^*	Threshold of the j-th identification UIO.
tr_{neg}	Deactivation threshold for the negative-sequence submodule.
$v_{POC,m}^+$	Voltage of POCs installed on the terminal of converter m on the positive-pole.
$v_{POC,n}^+$	Voltage of POCs installed on the terminal of converter n on the positive-pole.
v_{cm}	Voltage of DC link capacitor of converter m.
v_{cn}	Voltage of DC link capacitor of converter n.
δ_i	Set of areas to which Area i is connected.
$\mathbb{Y}^s$	Output vector for sequence s.

$\overline{\mathcal{Y}}^{s}_{ca}[k:k+\alpha]$	Output vector during attacks from time-step k to $k+\alpha$.
$i^{s}_{f}(t)$	Sampled value of the fault current.
$i_{n,dc}[k]$	DC current sample at the n-th terminal of a line at time step k.

Chapter 1

Introduction

In an article published by the Associated Press in March 2016, Duke Energy Chief Executive Officer (CEO) stated that "If I were to share with you the number of [cyber-]attacks that came into Duke Network everyday, you will be astounded. It is from nation-states that are trying to penetrate systems" [3]. A cyber-attack is a kind of intrusion, defined as "an event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, and acceptable use policies" [4]. Recently, cyber-related problems have raised new concerns regarding the security vulnerabilities of smart grids and their large-scale effects on critical power system infrastructure. Some of the significant issues reported are directly related to either cyber-attacks or malfunctions of the cyber-layer of power systems. For example, the 2011 annual report of the Repository for Industrial Security Incidents (RISI) states that about 35% of industrial control system security issues were initiated by remote access through cyber systems. This report also indicates that between years 2004 and 2008, twelve cyber-attacks targeted the power sector, which is 20% more than in the previous four years [5]. So far, in total, 800 total cyber-attacks globally have been documented since 1980 [6]. Three examples of recent cyber-attacks that targeted power systems are:

- On December 17th, 2016, a power cut due to cyber-attacks occurred in the Ukrainian

capital, Kiev. The blackout started before midnight and lasted for one hour. This cyber-attack de-energized about one-fifth of Kiev's consumers [7].

- On January 25th, 2016, Israel's Electricity Authority was under a "severe cyber-attack". The attack was carried out by a virus, delivered to the Electric Authority over Email, and spread over computers on the network. There was no loss of power in Israel's case, since the attack was identified and thwarted quickly before it affected computers of the electric company or distribution sites [8].

- On December 23rd, 2015, the first successful cyber-attack was carried out against the Ukraineian power grid. Hackers manipulated the information systems of three power distribution companies and temporarily disrupted the electricity supply to 230,000 end consumers for a period of one to six hours. This cyber-attack switched off 30 substations [9].

Power systems became vulnerable to cyber-attacks mainly after the integration of communication infrastructure, which gave rise to the emergence of compound protection and control schemes, such as the SCADA system, IEDs used for controlling circuit breakers, transformers, capacitor banks and other equipment, voltage/frequency/power control monitors, sensors, or device status indicators. These communication-base schemes and devices are mainly a part of protection and control systems, which are known as the backbones of power networks (since the former detects abnormal conditions and returns the system to its normal state by initiating a quick corrective action, and the latter preserves the integrity of the system and stabilizes it following physical disturbances). Although the integration of communication infrastructure and the above-mentioned schemes were to improve the reliability, service continuity, flexibility, and efficiency of power networks, they introduced new concerns in terms of proneness to cyber-attacks. Therefore, in addition to the physical security of a power network, the cyber-security of its protection and control schemes should be improved as well [10]. The following identifies two vulnerable protection and control schemes, and discusses their related research gaps and motivations.

1.1 Line Current Differential Relay, a Vulnerable Protection Scheme

The cyber-attack targeting the Ukrainian power system in 2015 involved opening and closing circuit-breakers without any input from the control centers [11]. This cyber-attack sparked off a renewed debate over restricting remote access to circuit breakers and instead controlling them locally. However, limiting direct remote access to breakers does not necessarily prevent a cyber-attack from sending malicious commands to them. Breakers can be controlled locally by protective relays, and relays often rely on communication networks, which are potentially vulnerable to cyber-attacks [12]. Therefore, if an attack can manipulate the data transmitted to a relay such that the relay issues a false trip command, the respective breaker has been indirectly targeted.

A successful attack on a protection system can involve tampering with the measurements obtained and decisions made by a remote relay communicating with a local relay [13]. LCDRs are a group of communication-dependent relays that are increasingly used to protect AC transmission lines, particularly for critical lines carrying large amounts of power [14], and are highly reliable for medium-voltage DC lines [15, 16, 17, 18, 19].

An LCDR must be equipped with a high-bandwidth communication channel to receive the synchronized currents measured at the other line terminal. Thus, the operation of LCDRs depends crucially on the integrity of the utilized communication channel and the Global Positioning System (GPS) [20]. This dependence makes LCDRs potential targets for cyber-attacks, as will be explained in Chapter 2.

Research on the cyber-security of protection systems in AC and DC systems is generally in its early stages, and can be divided into three main groups. Studies in the first group—such as [21], [22], [23], and [24]—have focused on attack modeling and risk assessment in protection systems. In [21], a framework is presented for modeling coordinated switching attacks over circuit breakers and relays. In [22], the impact of bus and transmission line protection schemes on power system cyber-security has been evaluated. In [23], a resilience and assessment metric is proposed to quantify the ability to and the cost required for the system to recover from an attack. Moreover, the authors of [24] have proposed a game-theoretic graph-coloring technique to determine the optimal allocation of security

mechanisms diversity that minimizes the impact of vulnerabilities to the grid. It is also shown that this technique provides a Nash equilibrium solution.

In the second group, studies have concentrated on the cyber-security of substations. In [25], a method is proposed to detect and mitigate cyber-attacks on substation automation systems. In this method, protection devices collaboratively defend against cyber-attacks against substations, even if information and communication technology (ICT)-based techniques are compromised. To avoid malfunctions due to substations receiving fake data packages, the authors of [26] have proposed a method whereby a substation identifies vicious attacks by using context information, such as its own voltages and currents. This method collects all measurements of the substation and feeds them to a probabilistic neural network. An event that differs from the known fault pattern is identified as an attack. Moreover, a distributed intrusion-detection system is proposed in [27] to monitor and detect anomalies in power systems and IEC-61850-based messages. A number of other studies, such as [28] and [29], have also proposed intrusion-detection systems for substations.

The third group of studies has developed attack detection or identification method for protection systems. In [13], a distributed scheme is proposed, that detects attacks and differentiates them from faults using both the cyber and physical properties of power networks. In [30], an anomaly detection approach, which works based on zone partition, is proposed for industrial cyber-physical systems. Moreover, the authors of [31] have presented an end-to-end attack-resilient cyber-physical security framework for wide-area monitoring, protection, and control (WAMPAC) applications. They also describe a defense-in-depth architecture and discuss several attack-resilient algorithms for WAMPAC systems.

All above-mentioned studies have focused on the cyber-security of protection systems. However, the cyber-security of LCDRs in both AC and DC networks has barely been investigated to date. The only work appearing in the literature about the cyber-security of LCDRs proposes a remedial pilot protection scheme in AC network, which works independently of timing information [32]. This remedial pilot protection scheme makes AC LCDRs independent of the GPS, and thus AC LCDRs can no longer be affected by GPS signal spoofing. However, even if LCDRs are resilient against GPS spoofing, they are still vulnerable to False Data Injection Attacks (FDIAs), since attackers can also break into communication systems (e.g., Wide Area Networks (WANs) and substations' Local Area

Networks (LANs)) in order to target LCDRs [33, 34, 35]. The research gap that remains in the area of line differential scheme cyber-security can be filled by the development of cyber-resilient LCDRs for both AC and DC systems.

1.2 Automatic Generation Control System, a Vulnerable Control Scheme

Power system controllers in the SCADA center process the collected data and send the required commands to pertinent actuators. AGC, one of these controllers, operates in a closed automated loop and greatly depends on communication infrastructure. AGC is the secondary LFC loop, and has the additional objective of economic dispatch [36]. By adjusting the load reference set-point, the AGC keeps the system frequency within acceptable bounds and regulates the power exchange between adjacent areas at scheduled levels. The inputs to the AGC are frequency and tie-lines power measurements, and its outputs are the load reference set-points for different generators. All inputs and outputs are sent and received through communication system. This dependence on the communication system, however, renders AGC systems vulnerable to cyber-attacks, as will be discussed in Chapter 6. Cyber-attacks can inject incorrect control or wrong measurements into the AGC data stream, and thus directly affect the frequency, stability, and economic operation of the grid [37]. As a result, an intrusion-resilient AGC is needed to prevent the consequences of such attacks on power system operation.

The targeting of AGC systems by cyber-attacks and the performance of LFC systems under intrusions have been studied in [38, 39, 40, 41, 42]. In [38], a model is developed to find the optimal and fastest series of FDIAs against AGC systems. In addition, [40] investigates the impact of time-delay switching attacks on an AGC system, and proposes a defense mechanism that augments the AGC with a time-delay estimator. In [42], an attack against AGC systems is proposed to destabilize the power system, and then a procedure is proposed to identify attacks. In [39], the risks faced by AGC systems are identified, and an attacker-defender game is modeled to find the most effective defensive actions during FDIAs. In [43], a series of FDIAs against an AGC system are devised to obtain an optimal

attack strategy that triggers the load-shedding or generation-tripping schemes.

In addition to theoretical analysis, [44] and [38] investigate AGC system vulnerability to FDIAs experimentally. In [44], testing of a system in Iowa, USA, shows FDIAs to be potential sources of under-frequency conditions and could result in unnecessary load shedding. In [38], a real 16-bus system is tested to practically demonstrate the possibility of attacks against AGC systems.

To detect FDIAs against an AGC system, the method developed in [2] forecasts the load, and then uses the forecasted values during real-time operation to validate the performance of the AGC system and to detect FDIAs. Additionally, [38] detects attacks targeting the AGC system by checking the consistency between observed and predicted frequency deviations. However, due to the unavailability of real-time values of loads in the system, both of the above-mentioned methods use estimated or forecasted load changes—which might not be perfectly accurate. Consequently, the accuracy of both of these methods depends strongly on the authenticity of forecasted or estimated loads. Moreover, none of the attack-detection methods proposed in the literature have considered the effect of noise. Noise can affect the operation of FDIA-detection methods adversely by increasing the number of false alarms, as discussed in Chapter 8. Therefore, developing an attack-detection method that works robustly against noise and does not require load data in the network has not received particular attention in the literature yet.

1.3 Research Objectives

Driven by the above-mentioned motivations and research gaps, this dissertation first unveils the potential consequences of cyber-attacks against AC and DC LCDRs and AGC systems. Additionally, it develops application-based measures for making AGC systems and LCDRs robust against cyber-attacks. The dissertation targets the following specific objectives, which are also shown in Fig. 1.1:

1. Unveiling the vulnerabilities of AC and DC LCDRs and investigating the consequences of cyber-attacks against this relay type.

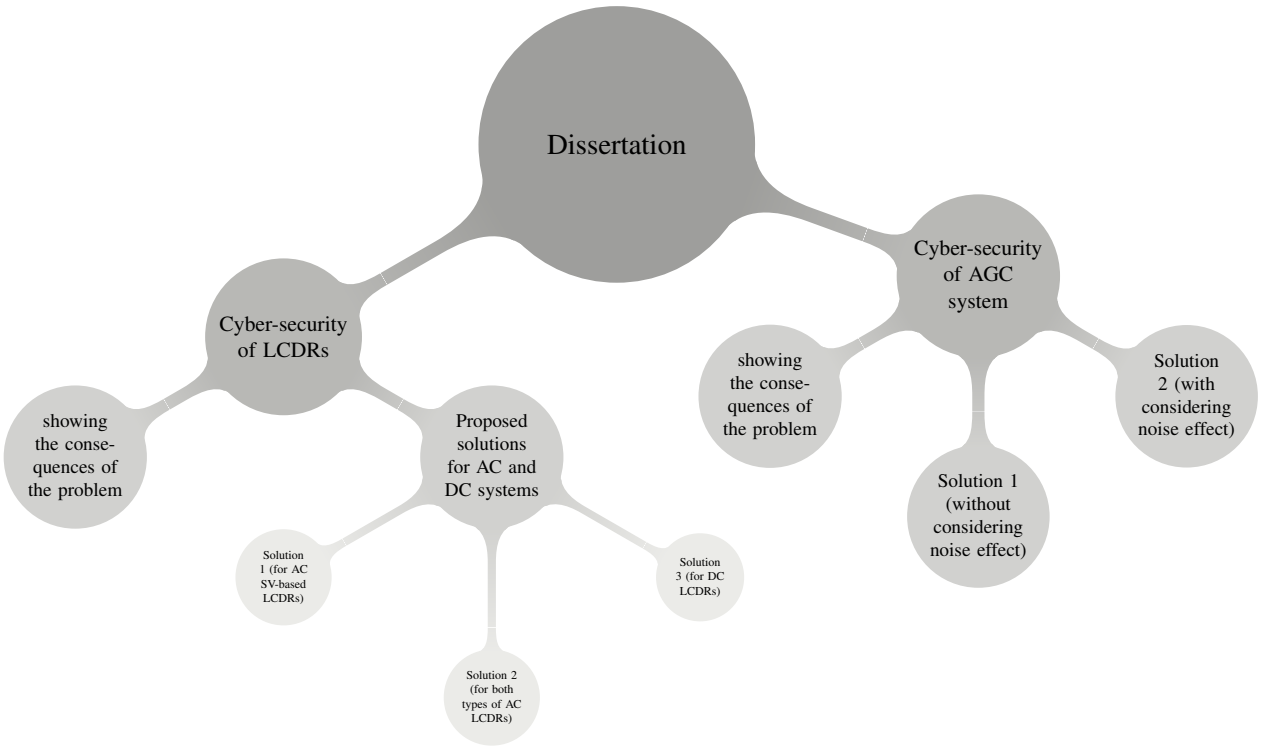


Figure 1.1: Diagram of Research Objectives.

2. Developing attack-detection techniques for SV-based and phasor-based AC LCDRs, with the goal of proposing techniques that are initiated when LCDRs pick up, in order to confirm faults and differentiate them from attacks.

3. Developing attack-detection techniques for DC LCDRs to confirm faults and differentiate them from attacks.

4. Revealing the vulnerabilities of AGC systems and investigating the consequences of cyber-attacks against this controller.

5. Developing an attack-detection and -identification techniques for AGC systems. The proposed methods should work independently from load-change data in the system, since this type of data is not normally available in real-time. Independence from noise is another feature that should be taken into account.

1.4 Dissertation Outline

This dissertation is divided into two main parts: the next four chapters, which concentrate on the cyber-security of LCDRs, and the subsequent three chapters, which focus on the cyber-security of AGC systems. The individual chapters are organized as follows:

Chapter 2 provides the necessary background on the working principals of AC and DC LCDRs, as well as on their communication and time-synchronization requirements and vulnerabilities. Additionally, this chapter formulates FDIAs against both AC and DC LCDRs, and presents three case studies to show the consequences of coordinated attacks against such relays.

Chapter 3 presents an attack-detection technique for AC SV-based LCDRs. To confirm the occurrence of faults and to differentiate them from attacks, the proposed method is initiated after LCDRs pick up. In this method, the estimated and locally-measured voltages at an LCDR's local terminal are compared during faults. To estimate the local voltage, the proposed technique uses a UIO, the state-space model of the faulty line, and remote and local measurements. The difference between the measured and estimated local voltage remains close to zero during real internal faults, because in this condition the state-space model based on which the UIO operates correctly represents the line. Nevertheless, the state-space model mismatch during attacks leads to a large difference, as will be shown in Chapter 3.

Chapter 4 develops an attack-detection technique that works for both SV-based and phasor-based AC LCDRs. The proposed technique is initiated when LCDRs pick up. The method confirms faults and differentiates them from attacks by comparing the calculated and locally-measured superimposed voltages at an LCDR's local terminal after the relay's pickup. A difference between the calculated and the measured superimposed voltages reveals that the remote measurements are not authentic, because local measurements cannot be manipulated by cyber-attacks. Thus any difference between the calculated and measured superimposed voltages is due to the inauthenticity of remote current measurements.

Chapter 5 presents an attack-detection method by which DC LCDRs can differentiate between cyber-attacks and faults using local measurements. The proposed method

installs a POC, which includes an inductor and a capacitor in parallel, at each converter's terminal. A POC thus resonates and generates a damped component with a specific frequency, i.e., f_d, only under fault conditions. Each LCDR detects f_d by applying Fast Fourier Transform (FFT) to the uncompromisable locally-measured voltage across each POC in real-time. Detecting f_d thus validates an LCDR's tripping decision. Accordingly, a cyber-attack is flagged if an LCDR picks up without detecting f_d.

Chapter 6 supplies the necessary background on the AGC system state-space model, operating principals, and alarms. To investigates the vulnerabilities of this controller and to demonstrate the destructiveness of FDIAs against AGC systems, this chapter formulates and optimizes an SHA to disrupt the normal operation of the AGC system quickly and undetectably. Additionally, it models the AGC system under FDIAs and develops its associated state-space equation.

Chapter 7 develops an attack-detection and -identification method for AGC systems. The proposed method detects FDIAs by estimating the LFC system's states and comparing them with measured ones. For estimating the LFC system's states, the proposed method uses a UIO that does not require load-related data in the system. This chapter also identifies attacks by using a number of identification UIOs.

Chapter 8 proposes a method for detecting and identifying FDIAs against AGC systems in the presence of measurement and process noise. This method uses a SUIE that estimates the LFC system's states without requiring real-time load changes in the grid. FDIAs are detected by comparing the estimated and measured states. Additionally, FDIAs are identified by using a number of Attack Identification Stochastic Unknown Input Estimators (AISUIEs).

Chapter 9 concludes the dissertation, highlights its contributions, and suggests topics for future research.

Chapter 2

Vulnerability of LCDRs to Cyber-Attacks: Background and Problem Statement

LCDRs are a group of communication dependent protection devices that are increasingly used to protect AC transmission lines, particularly for critical ones carrying gigawatts of power [45], and medium-voltage DC lines [15, 16, 17, 18, 19]. This type of relays perform well under conditions for which other protection schemes may malfunction, e.g., high-impedance faults, series-compensated lines, and lines connected to converter-interfaced wind and solar power plants [14]. LCDRs detect faults by comparing the synchronized current measurements at all of the line terminals. Therefore, the main requirements of LCDRs are reliable communication of measured currents between relays at a line terminals, as well as an external time reference, e.g., GPS, if the communication channel is not symmetrical [46]. However, this dependence on communication systems and the GPS renders LCDRs vulnerable to cyber-attacks. Thus, superior performance of LCDRs is achieved at the expense of exposing the protection system to cyber-threats.

On this basis, Section 2.1 briefly discusses the working principal of AC and DC LCDRs. Afterwards, Section 2.2 describes the vulnerabilities of LCDRs to cyber-attacks and elaborates on LCDRs' communication and time-synchronization requirements and vulnera-

bilities. Section 2.3 then formulates FDIAs against AC LCDRs, and proceeds with the procedure that must be carried out to trip AC lines protected by LCDRs. Additionally, Section 2.4 formulates FDIAs against DC LCDRs. Afterwards, Section 2.6 presents three case studies to show the consequences of coordinated attacks against AC and DC LCDRs. Finally, Section 2.7 presents the concluding remarks.

2.1 Working Principal of LCDRs

LCDRs detect internal faults based on Kirchhoff's current law, by comparing the currents going in or out of the line from all terminals. To this aim, LCDRs installed on different terminals of a line communicate with each other to share the time-synchronized current measurements [14]. The following explains how AC and DC LCDRs operate.

2.1.1 AC LCDRs

Some AC LCDRs exchange current phasors, while modern ones communicate the SVs of currents. Compared to phasor-based AC LCDRs, SV-based ones (i) share half amount data, because they share instantaneous values instead of the magnitude and angle of phasors, (ii) exchange data at higher rates (e.g. a few kilohertz), while phasor-based LCDRs exchange data every 4 ms [47], (iii) are not dependent on the GPS, as the SVs can be synchronized by measuring the communication link latency and interpolating the received data, and (iv) share more information—such as harmonics or rate of change of currents—with the remote relays, simplifying certain LCDR requirements, such as fast detection of Current Transformer (CT) saturation [14].

Some SV-based and phasor based commercial AC LCDRs issue the trip command only if they pick up, i.e., their operating point in the differential-restraining plane of Fig. 2.1 enters the trip zone [1]. In this figure, I_{diff} and I_{res} are the differential and restraining currents, which are formed differently for SV-based and phasor-based AC LCDR. Phasor-based relays compute these two currents from the shared phasor values using the following equations:

$$I_{diff}[k] = |I_1[k] + I_2[k] + \cdots I_N[k]| \tag{2.1}$$

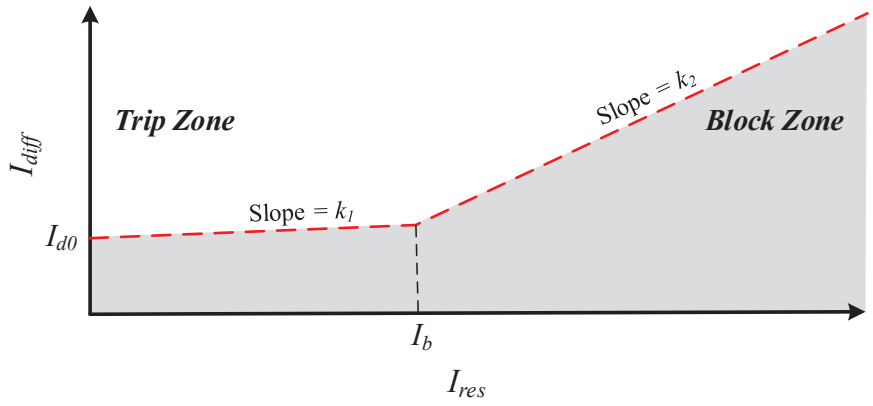


Figure 2.1: LCDR characteristic [1].

$$I_{res}[k] = |I_1[k]| + |I_2[k]| + \cdots |I_N[k]| \tag{2.2}$$

in which, $I_n[k] = |I_n| \angle \theta_n$ is the current phasor entering the n-th terminal of a line at time-step k, N is the total number of terminals, and $|.|$ denotes the absolute value operator. However, SV-based relays use following equations to obtain I_{diff} and I_{res}:

$$I_{diff}[k] = \|i_1[k] + i_2[k] + \cdots + i_N[k]\| \tag{2.3}$$

$$I_{res}[k] = \|i_1[k]\| + \|i_2[k]\| + \cdots + \|i_N[k]\| \tag{2.4}$$

in which, $i_n[k]$ is the SV of the current entering the n-th terminal of a line at time-step k, and $\|.\|$ denotes the operation of filtering and magnitude estimation. The operating points of both AC LCDR types enter the trip zone when

$$I_{diff}[k] \geqslant I_{op} \tag{2.5}$$

in which, I_{op} is a function of I_{res}, and is given by

$$I_{op}\left(I_{res}\right) = \begin{cases} I_{d0} + k_1 \times I_{res} & I_{res} \leqslant I_b \\ I_{d0} + k_1 \times I_b + k_2 \left(I_{res} - I_b\right) & I_{res} \geqslant I_b \end{cases} \tag{2.6}$$

where I_b, I_{d0}, k_1, and k_2 are the settings of the differential-restraining characteristic, and are shown in Fig. 2.1.

For further security, some other AC LCDRs additionally require that the Disturbance Detector (DD) element of the relay also picks up before a trip command is issued [47]. The DD element is a sensitive current disturbance detector that supervises current-based elements such as LCDRs to prevent their malfunction. Commercial LCDRs utilize various settings for detecting disturbances. These settings are chosen such that the DD element picks up even during small disturbances, e.g., high-resistance ground faults [14]. For example, the DD element of some LCDRs picks up if one of the these criteria are met in 1 cycle [47]:

- the magnitude of the Zero-Sequence (ZS) or PS currents changes by more than ± 0.02 p.u.
- the angle of the ZS or PS currents varies by more than $\pm 8^{\circ}$.

Any event meeting either or both of these criteria activates the DD element.

2.1.2 DC LCDRs

Unlike AC LCDRs, DC ones utilize only the magnitude of current measurements at all line terminals to detect faults in DC systems. Therefore, the differential current of DC LCDRs is obtained using

$$I_{diff,dc}[k] = |i_{1,dc}[k] + i_{2,dc}[k] + \cdots + i_{N,dc}[k]| \tag{2.7}$$

in which $i_{n,dc}[k]$ is the DC current sample at the n-th terminal of a line at time step k. In normal conditions, $I_{diff,dc}[k]$ is ideally zero. A fault is thus detected if

$$I_{diff,dc}[k] \geqslant \kappa I_{nom} \tag{2.8}$$

in which κ is a reliability coefficient whose value can be set to between 0.1 and 0.25, and I_{nom} is the nominal current of the line [16].

2.2 Vulnerability of LCDRs to Cyber-Attacks

Intrusions against LCDRs can be categorized into three main groups: Denial of Service Attacks (DoSAs), FDIAs, and Time Synchronization Attacks (TSAs). DoSAs cause a break in the normal transmission of real-time protection messages and disable the primary line current differential element of LCDRs [48]. However, as most commercially available LCDRs, e.g., [1], [47], and [49], include other protection schemes, such as over-current and directional comparison elements in the same device, the line remains still protected by other elements if the differential element is disabled [48]. Additionally, some relays, such as in [49], include redundant communication links [50]. During FDIAs against LCDRs, however, the measurement values are manipulated. On the other hand, TSAs manipulate the time-tags of measurements [51, 32], e.g., by spoofing the GPS signal. Therefore, in the case of LCDRs, FDIAs and TSAs are more disruptive than DoSAs, since they are able to fool LCDRs into tripping lines [48]. In the rest of this chapter, the focus will be on these two types of cyber-attacks.

2.2.1 Communication and Time-Synchronization Media, Protocols, and Susceptibilities

To share time-synchronized measurements with relays installed on other terminals, an LCDR must be equipped with a high-bandwidth communication channel. Therefore, the operation of LCDRs depends crucially on the integrity of the communication channel and the authenticity of synchronization mechanism [20]. LCDRs' data can be transmitted via a dedicated fiber or multiplexed network [52]. Dedicated fiber channels communicate at the speed of light through the fiber, thus no extra delays are incurred due to encoding, buffering, (de)multiplexing, and converting to electrical signals. Additionally, direct point-to-point channels are symmetrical, i.e., the propagation times for transmitting and receiving data are equal. Therefore, no external time reference, e.g., the GPS, is required. However, the application of direct channels for long distances is limited, and they have no inherent redundancy, which results in the loss of the differential scheme when its associated fiber fails [46].

LCDRs' data can also be transmitted via multiplexed channels, which are widely used nowadays, due to their superiority over direct point-to-point fiber in terms of cost-efficiency, path redundancy, and wireless connectivity to remote locations. In multiplexed channels, the relay's communication interface is connected to a substation multiplexer—either T1/E1 or a Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH)—to transport data over a WAN [53, 52]. The availability of multiplexed channels, however, is adversely affected by the availability of devices and physical channels that transmit the data. On the other hand, unlike direct fiber, delays in multiplexed channels are longer due to signal conversion and buffering. Moreover, multiplexed channels are not symmetrical, requiring external time reference, e.g., GPS [46]. Therefore, LCDRs that utilize multiplexed channels receive timing information from the substation using a hardwired network-based protocol, e.g., Inter-Range Instrumentation Group Code B (IRIG-B), or packet-based time synchronization protocols, e.g., IEEE 1588 Precision Timing Protocol (PTP) [54].

In the case of both communication channels, FDIAs can target LCDRs by intruding into substations' LAN and accessing the control center facilities [55, 56]. This vulnerability has been proven by the attacks that paralyzed the substations of the Ukrainian power system in 2015 and 2016 [11]. On the other hand, the protocol that LCDRs use to communicate in substations, i.e. IEC 61850 [57], is also vulnerable to cyber-attacks. This has been shown experimentally in [35] and discussed in [58] and [59]. Multiplexed channels, however, can also be attacked by FDIAs targeting wide-area communication systems, as well as by TSAs [60, 61, 32]. To change the time reference in the whole substation, the GPS signal can be spoofed by a TSA, in which the authentic GPS signal is overwhelmed using noise of the same frequency and the GPS receiver is mislead by a counterfeit GPS signal [32]. TSAs can also be carried out by targeting synchronization protocols. The vulnerability of IRIG-B to TSAs is proven experimentally in [62]. The susceptibility of PTP and the required procedure to target this protocol by TSAs are also discussed in [32].

In conclusion, LCDRs are vulnerable to FDIAs and TSAs. These vulnerabilities can provide cyber-attackers with indirect access to circuit breakers through LCDRs, leading potentially to outages or blackouts [63]. The rest of this chapter shows how these vulnerabilities endanger the integrity of an tire system.

2.3 Tripping AC Lines by Targeting LCDRs

This section unveils how FDIAs and TSAs can fool AC LCDRs into tripping the line they are protecting. To this aim, this section considers the more secure type of AC LCDRs, which are also equipped with a DD element. As a result, this type of relays require (i) the pickup signal of the DD element, and (ii) the pickup signal of the relay to issue the trip signal.

This section uses the 39-bus new England system, shown in Fig 2.2, and the PSCAD/EMTDC program for simulations. The specifications of this test system are provided in Appendix A. As explained in this appendix, Lines 6-11, 4-14, 2-3, and 3-18 are critical, so they are protected by LCDRs, which are set based on the default settings of [1]. Additionally, a 100 MVAr capacitor banks has been installed on Bus 12 to supply the required reactive power by load connected to this bus, and Line 5-8 has been 60% compensated using series capacitors. The focus in this subsection is on LCDRs I and II in Fig. 2.2 protecting the 100 km line between buses 6 and 11. Following the default settings given in [1], the parameters of these LCDRs are set at $I_0 = 0.05$ kA, $I_b = 0.585$ kA, $k_1 = 0.2$, and $k_2 = 0.4$. During normal operation, the currents measured by LCDR I and II in Fig. 2.2 are $0.282\angle 111.2°$ kA and $0.262\angle -78°$ kA, respectively, and so $I_{op} = 0.158$ kA and $I_{res} = 0.544$ kA.

2.3.1 Targeting Phasor-Based AC LCDRs by Cyber-Attacks

To move the operating point trajectory of phasor-based AC LCDRs into the trip zone, an attacker can manipulate the magnitude, phase angle, and/or time stamp—altering the time stamps of an LCDR's measurements is equivalent to changing the measurements' phase angle [64]—of remote measurements. Therefore, during FDIAs or TSAs the remote measurements of terminal n are changed from $(|I_n|\angle\theta_n)$ to $(|I_n| + |\Delta I_n|\angle(\theta_n + \Delta\theta_n)$. The manipulated differential current during attacks thus becomes

$$I^m_{diff}[k] = \left| \sum_{j\in\{1,\cdots,N\}-\{n\}} (|I_j|\angle\theta_j) + ((|I_n| + |\Delta I_n|)\angle(\theta_n + \Delta\theta_n)) \right| \tag{2.9}$$

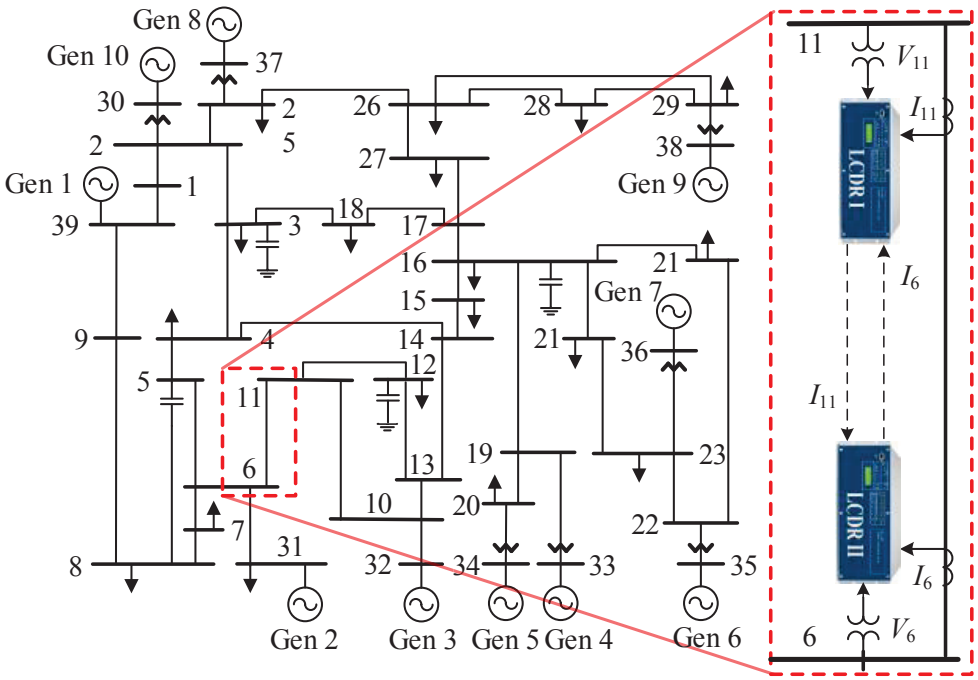


Figure 2.2: 39-bus new England system.

As I_{diff} in normal conditions is ideally zero, using (2.1), the following equation holds for any terminal n ($1 \leqslant n \leqslant N$):

$$\sum_{j \in \{1,\cdots,N\}-\{n\}} (|I_j| \angle \theta_j) = -(|I_n| \angle \theta_n) \tag{2.10}$$

Substituting (2.10) into (2.9) results in

$$I^m_{diff}[k] = |(|I_n| + |\Delta I_n|) \angle (\theta_n + \Delta\theta_n) - |I_n| \angle \theta_n| \tag{2.11}$$

Given that the restraining current before the initiation of the attack was $I_{res}[k_0]$, it changes to $I_{res}[k_0] + |\Delta I_n|$ when the attack starts. To trip the line, an attacker must select $\Delta\theta_n$ and $|\Delta I_n|$ such that the manipulated differential current, I^m_{diff}, becomes greater than I_{op}

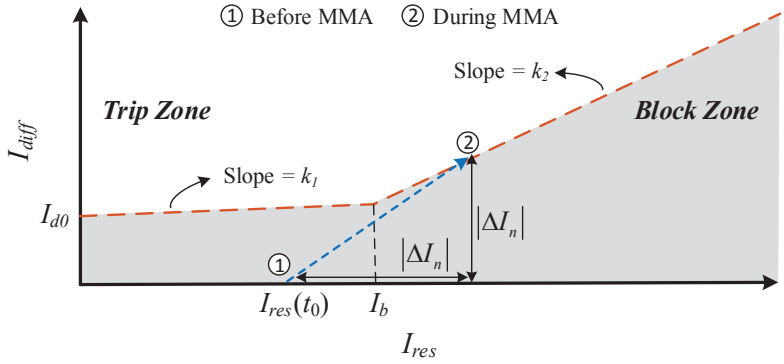


Figure 2.3: Operating point trajectory of LCDRs during MMAs.

in (2.6). Hence, an LCDR picks up during an attack if the following equation is satisfied:

$$|(|I_n| + |\Delta I_n|)\angle(\theta_n + \Delta\theta_n) - |I_n|\angle\theta_n| \geq I_{op}\,(I_{res}[k_0] + |\Delta I_n|) \tag{2.12}$$

Since all relays of a line share current measurements among each other, these current values—i.e., $|I_n|\angle\theta_n$ for $n \in \{1, 2, \cdots, N\}$—are available after intruding into the communication systems or substations. As a result, $I_{res}[k_0]$ is calculable at anytime for attackers during FDIAs or TSAs. To satisfy (2.12), the following attacks can be carried out:

- *Magnitude Modification Attack (MMA)*: An MMA is a kind of FDIA that involves manipulating the magnitude of the remote end current measurements before they are used by LCDRs for detecting faults. As shown in Fig. 2.3, when $|\Delta I_n|$ is injected into the n-th terminal's current measurements, the operating point of other terminals' LCDRs move from point ① to ②. Therefore, the operating point in Fig. 2.3 enters the trip zone if the MMA satisfies

$$|\Delta I_n| \geqslant I_M \tag{2.13}$$

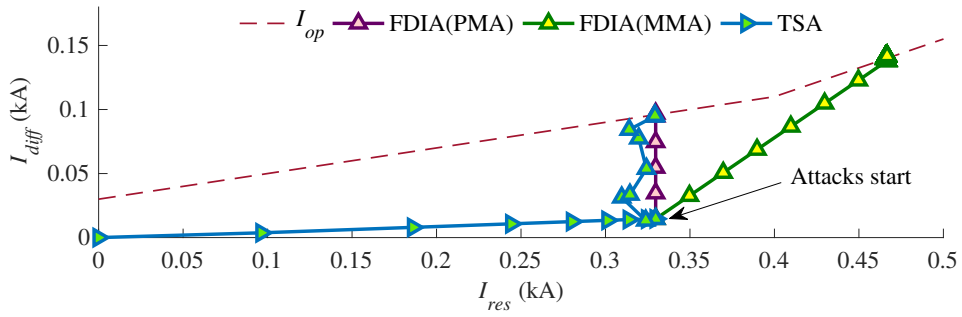


Figure 2.4: LCDR I's trajectory during the MMA, PMA, and TSA.

where, I_M is

$$I_M = \begin{cases} \dfrac{I_{op}\left(I_{res}[k_0]\right)}{1-k_1} & I_{res}[k_0] < (1-k_1)\, I_b - I_{d0} \\ \\ \frac{I_{op}(I_{res}[k_0])+(k_1-k_2)(I_b-I_{res}[k_0])}{1-k_2} & I_{res}[k_0] \geqslant (1-k_1)\, I_b - I_{d0} \end{cases} \tag{2.14}$$

In (2.14), $I_{res}[k_0]$ and $I_{op}\left(I_{res}[k_0]\right)$ can be calculated according to (2.2) and (2.6) using the measurements that an attacker can access through the communication network linking LCDRs.

Using (2.14) and the aforementioned current values for LCDR I, I_M is 0.251 kA for this relay. Therefore, LCDR I's operating point enters the trip zone during non-fault conditions if the $|\Delta I_6|$ associated with an MMA is greater than 0.251 kA. The trajectory of LCDR I's operating point during an MMA with $|\Delta I_6| = 0.251$ kA is illustrated in Fig. 2.4. Consequently, a false pickup signal is issued as soon as the operating point of the relay enters the trip zone.

• *Phase Modification Attack (PMA)*: A PMA is another kind of FDIA that involves manipulating the phase angle of the remote end current measurements from θ_n to $\theta_n + \Delta\theta_n$ before they are used by LCDRs for detecting faults. Thus PMAs change the differential current in (2.11) to

$$I^m_{diff}[k] = |I_n| \times |(1\angle\left(\theta_n + \Delta\theta_n\right)) - (1\angle\theta_n)| \tag{2.15}$$

During a PMA, $|\Delta I_n|$ is zero; thus I_{res} does not change. Therefore, using (2.6) and (2.15), an LCDR picks up if $\Delta\theta_n$ satisfies

$$|(1\angle(\theta_n + \Delta\theta_n)) - (1\angle\theta_n)| > \frac{I_{op}\left(I_{res}[k_0]\right)}{|I_n|} \tag{2.16}$$

Solving (2.16) indicates that $\Delta\theta_n$ must be selected from the following interval for an LCDR to trip:

$$\Delta\theta_n \in \left[2\arcsin\left(\frac{I_{op}\left(I_{res}[k_0]\right)}{2\,|I_n|}\right), 2\pi - 2\arcsin\left(\frac{I_{op}\left(I_{res}[k_0]\right)}{2\,|I_n|}\right)\right] \tag{2.17}$$

For (2.16) to be solvable, $I_{op}\left(I_{res}[k_0]\right)/2|I_n|$ must be inside the domain of arcsin(.) (i.e., [-1,1]) in (2.17). Thus, since $I_{op}\left(I_{res}[k_0]\right)/2|I_n|$ is positive, (2.16) is solvable for:

$$\frac{I_{op}\left(I_{res}[k_0]\right)}{2} \leqslant |I_n| \tag{2.18}$$

In conclusion, to trip a line, a PMA must target a line terminal whose current meets (2.18). During the PMA, $\Delta\theta_n$ must satisfy (2.17). For example, the aforesaid values for LCDR I in the test system indicate that $I_{op}\left(I_{res}[k_0]\right)/2$ is smaller than $|I_6|$ and $\Delta\theta_6$ must be within [35.1° 324.9°]. Fig. 2.4 shows that the trajectory of LCDR I's operating point enters the trip zone for a PMA with $\Delta\theta_6 = 35.1°$.

• *TSA*: A TSA manipulates the sampling time of measurements. This type of attack has been previously investigated for wide-area monitoring systems [64]. A TSA is equivalent to changing the measurements' phase angle. Therefore, to carry out a TSA, a $\Delta\theta_n$ that satisfies (2.17) must be selected, and the time stamps of current samples must be changed from t to $t + \Delta t$, where, Δt is

$$\Delta t = \frac{\Delta\theta_n}{2\pi f} \tag{2.19}$$

In this equation, f is the system frequency. For example, choosing $\Delta\theta_6 = 35.1°$ results in $\Delta t = 1.63$ ms. Fig. 2.4 illustrates the effect of this TSA on LCDR I's operating point.

• *Hybrid Attacks*: An LCDR can also be targeted by a combination of the above-discussed attacks. For example, if both θ_n and $|I_n|$ are changed to $\theta_n + \Delta\theta_n$ and $|I_n| + |\Delta I_n|$, I^m_{diff} becomes

$$I^m_{diff}[k] = |(|I_n| + |\Delta I_n|)\angle(\theta_n + \Delta\theta_n) - |I_n|\angle\theta_n| \tag{2.20}$$

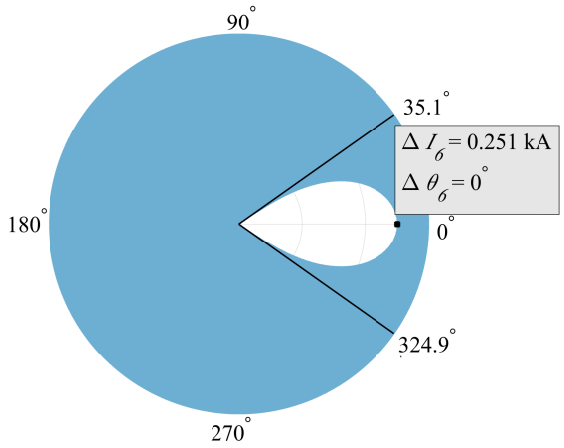


Figure 2.5: The locus of solutions of (2.21) for Line 6-11 of the test system.

and $I_{res}[k_0]$ changes to $I_{res}[k_0] + |\Delta I_n|$. Therefore, using (2.5) and (2.6), the following equation must be satisfied to trip the line:

$$|(|I_2| + |\Delta I_2|)\angle(\theta_2 + \Delta\theta_2) - |I_2|\angle\theta_2| > I_{op}\,(I_{res}[k_0] + |\Delta I_2|) \tag{2.21}$$

Fig. 2.5 shows the locus of solutions of (2.21) in the polar coordinates for Line 6-11. For any point in this figure, the magnitude indicates $|\Delta I_6|$, and the angle represents $\Delta\theta_6$. To trip the line, $\Delta\theta_6$ and $|\Delta I_6|$ must be selected from the shaded area. For example, for $\Delta\theta_6 \in [35.1°,\ 324.9°]$, the LCDR trips the line for any value of $|\Delta I_6|$. However, for $\Delta\theta_6 \in [324.9°,\ 35.1°]$, $|\Delta I_6|$ must be selected outside the white area, e.g., for $\Delta\theta_6 = 0$, $|\Delta I_6|$ must be greater than 0.251 kA. Therefore, hybrid attacks can gives the same results as MMAs and PMAs if $\Delta\theta_6 = 0$ and $|\Delta I_6| = 0$, respectively.

2.3.2 Targeting SV-Based AC LCDRs by Cyber-attacks

To cause malfunction of an SV-based AC LCDR that receives remote measurements from terminal n of a line, an attack must manipulate $i_n[k]$ such that (2.5) is met. Altering $i_n[k]$ to $I_n^m[k]$ by an FDIA or TSA at $k = k_0$ changes the differential current in (2.3) to $I_{diff}^m[k]$

as follows

$$I^m_{diff}[k] = \left\| \sum_{j\in\{1,\cdots,N\}-\{n\}} i_j[k] + i^m_n[k] \right\| \tag{2.22}$$

As I_{diff} in normal conditions is ideally zero, using (2.3), the following equation holds for terminal n:

$$\sum_{j\in\{1,\cdots,N\}-\{n\}} i_j[k] = -i_n[k] \tag{2.23}$$

Substituting (2.23) into (2.22) results in

$$I^m_{diff}[k] = \|-i_n[k] + i^m_n[k]\| \tag{2.24}$$

Additionally, the restraining current after the inception of the attack becomes

$$I_{res}[k] = I_{res}[k_0] - \|i_n[k]\| + \|i^m_n[k]\| \tag{2.25}$$

where $I_{res}[k_0]$ is the restraining current before the start of the attack. To trip the line, $i^m_n[k]$ must be selected such that $I^m_{diff}[k]$ becomes greater than $I_{op}(I_{res})$ in (2.5) for the new restraining current. Thus, to trip the line, $i^m_n[k]$ must be selected such that the following equation is satisfied for SV-based AC LCDRs:

$$\|-i_n[k] + i^m_n[k]\| \geq I_{op}\left(I_{res}[k_0] - \|i_n[k]\| + \|i^m_n[k]\|\right) \tag{2.26}$$

To satisfy this equation, cyber-attacks similar to those explained for phasor-based LCDRs can be carried out.

2.3.3 Activating the DD Elements of Target LCDRs

As explained in Section 2.1, any event that changes the PS or ZS current's magnitude by 0.02 p.u. activates the DD element of LCDRs. Additionally, DD elements can also pick up if the PS or ZS currents' angle change by more than $\pm 8^\circ$. Although these criteria are usually met during faults, other no-fault transients can pick up the DD element of LCDRs as well. For example, Fig. 2.6 illustrates the PS current measured by LCDR I in

Fig. 2.2 right after switching on the capacitor bank installed at Bus 12. The length of the no-disturbance zone in Fig. 2.6 is 1 cycle, and its width is 0.04 p.u. and 16 degrees in Figs 2.6a and 2.6b, respectively. The criteria for the pickup of LCDRs' DD element are thus satisfied if either the magnitude or its angle cross any horizontal side of the no-disturbance zone. As seen in 2.6, both the magnitude and phase angle of the measured current overstepped the no-disturbance zone from horizontal sides. Additionally, Fig. 2.7 illustrates the same variable after switching off the series capacitor bank installed in Line 5-8: in this case, however, only the magnitude of the measured current overstepped the no-disturbance zone. Thus, in both cases, the DD element of LCDR I picked up.

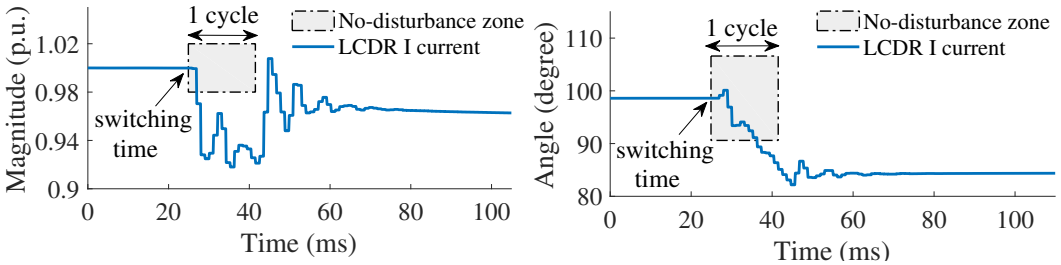


Figure 2.6: PS current measured by LCDR I after switching the shunt capacitor bank installed on Bus 12, (a) magnitude, (b) angle.

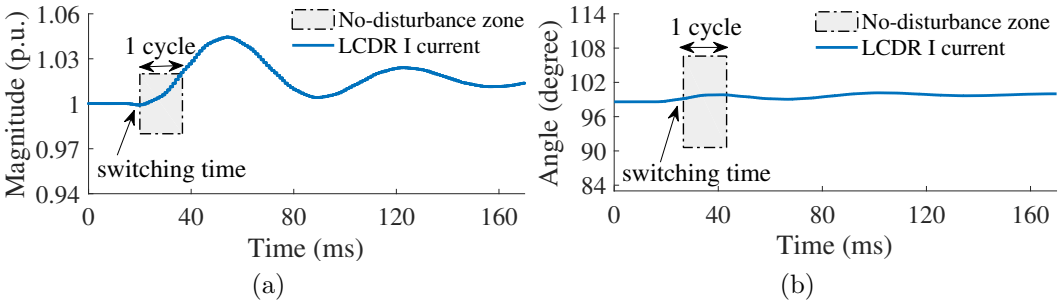


Figure 2.7: PS current measured by LCDR I after switching the series capacitor bank installed in Line 5-8, (a) magnitude, (b) angle.

Additionally, large load changes in the system, real faults, deliberate physical disturbances are other examples of events that can activate the DD element of LCDRs. For

instance, Fig. 2.8 shows the PS current measured by LCDR I after a 20% load change at Bus 8: once the load changes, the magnitude of the PS current overstepped the no-disturbance zone and thus the DD element picked up.

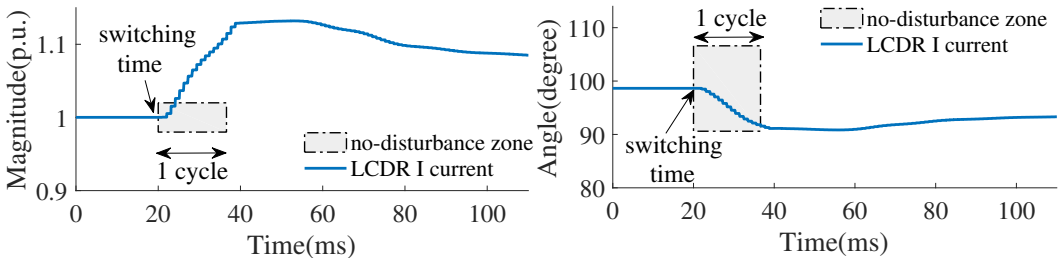


Figure 2.8: PS current measured by LCDR I after 20% load change at bus 8, (a) magnitude, (b) angle.

In conclusion, if a large-enough transient happens near an LCDR, the DD element of the LCDR picks up. Consequently, if an FDIA or TSA fools the LCDR after such a transient and moves its operating point into the trip zone, the line would be tripped.

2.4 Tripping DC Lines by Targeting LCDRs

To trip a DC line by FDIAs, an attacker must manipulate $i_{n,dc}[k]$ such that (2.8) is met. Altering $i_{n,dc}[k]$ to $i^m_{n,dc}[k]$ changes the differential current in (2.7) to

$$I^m_{diff,dc}[k] = \left| \sum_{j\in\{1,\cdots,N\}-\{n\}} i_{j,dc}[k] + i^m_{n,dc}[k] \right| \tag{2.27}$$

As $I_{diff,dc}[k]$ is ideally zero under normal conditions, the following equation holds for terminal n:

$$\sum_{j\in\{1,\cdots,N\}-\{n\}} i_{j,dc}[k] = -i_{n,dc}[k] \tag{2.28}$$

Substituting (2.28) into (2.27) yields

$$I^m_{diff,dc}[k] = \left|-i_{n,dc}[k] + i^m_{n,dc}[k]\right| \tag{2.29}$$

Given that $i_{n,dc}[k]$ is accessible by intruding into the communication system, $I^m_{diff,dc}$ can be calculated such that (2.8) is met. As a result, $i^m_{n,dc}[k]$ that satisfies (2.29) can be determined. On the other hand, to trip a line protected by a DC LCDR through a TSA, time-stamps of the LCDR's remote measurements are manipulated such that (2.29) is met. Assuming that a TSA changes the time stamps of remote measurements by Δt, (2.29) is satisfied and the line is tripped if an event, such as an external fault, changes the line's current by more than κI_{nom} over Δt.

2.5 Attack Model and Analysis

2.5.1 Attackers' Motives and Objectives

According to the North American Electric Reliability Corporation (NERC) standards, power systems must satisfy the $N-1$ security constraint, that is, the system is required to continue its normal operation after any single element failure. Additionally, NERC mandates operators to have contingency plans for all critical $N-2$ contingencies [65], and so the system can sustain a maximum of two critical failures at the same time. This situation might motivate attackers to carry out malicious activities, such as coordinated attacks, in which attackers can simultaneously target multiple components and potentially trip several critical lines at the same time—an event that the system is not normally designed to withstand. LCDRs are suitable choices to target by cyber-attacks, because they are highly dependent on the data received through the communication links [14, 61]. Therefore, coordinated attacks can impose severe consequences on the system, such as cascading failures, if they target the LCDRs of more than two lines in the system. An attacker's objectives in targeting power systems include, but are not limited to, (i) gaining financial benefit, (ii) causing maximal harm to the targeted power system without being detected, and (iii) satisfying curiosity/building reputation, e.g., to increase the attacker's

reputation in the hackers community. This section focuses on objective (ii) and shows that targeting LCDRs can lead to achieving such an objective, because LCDRs

- directly control lines' circuit breakers, so they can trip lines if they pick up [14];
- are vulnerable to cyber-attacks, since they highly rely on synchronized measurements received through communication links [14, 61];
- are increasingly used for protecting heavily loaded lines.

2.5.2 Assumptions and Attackers' Capabilities and Constraints

This dissertation considers the following resource constraints and capabilities for attackers who are aiming to achieve any of the above objectives by targeting LCDRs:

1. Attackers cannot physically trip transmission lines by opening circuit breakers. Without this constraint, it is a trivial exercise to trigger cascading failures across the power grid.
2. An attacker's resources are restricted, so a limited number of LCDRs can be targeted.
3. Only some of the lines in a power system are protected by LCDRs; thus, an attacker's options are limited.
4. For some AC LCDRs, the trip command relies only on the position of the operating point in the differential-restraining plane, shown in Fig. 2.24 [1]. For further security, some other AC LCDRs additionally require that the DD element of the relay also picks up before a trip command is issued [66]. The AC LCDRs considered in this section are the latter more-secure type.
5. Attackers can only tamper with remote measurements by intruding into the communication link between LCDRs, spoofing the GPS signal, or breaking into substations networks. However, local measurements are secure, since they are recorded by current and voltage transformers, located in substations' yard, and are sent directly to

LCDRs using copper wires. Therefore, LCDRs' local measurements are secure, reliable, and immune to cyber-attacks. The proposed attack detection methods in this dissertation work only if this assumption holds.

6. System data including loads, generation, and configuration are available for attackers. Additionally, the lines that are protected by LCDRs are known. Selecting the optimal attack strategy is dependent on accessing this information.

2.6 Case Studies

To corroborate the effectiveness of coordinated attacks against LCDRs and investigate their consequences, this section presents three case studies on the IEEE 14-bus and 39-bus new England networks and a 5-kV DC test system. In each case study, coordinated attacks target some LCDRs in the system and the results are studied. The consequences of cyber-attacks in all cases are indirect, i.e., cyber attacks only initiate a sequence of incidents. These case studies show that although attack strategies are system-dependent and might differ from one to another, the results are the same and a type of instability can happen. Additionally, these case studies demonstrate that different kinds of instability can occur as the consequences of coordinated attacks.

As will be explained and shown by attack trees, the attack strategies to achieve a certain goal are not unique, and there are several ways to reach that goal. Additionally, once the attack strategy is selected, any attack vectors that satisfy the selected strategy can be picked. Therefore, to prove the dimensions of the problem, each case study presents a selected attack strategy and its related attack vectors; however, there are lots of other ones that end up the same results.

2.6.1 Case Study 1

In this case study, the IEEE 14-bus test system (Fig. 2.9) [67] is chosen to investigate the consequences of coordinated attacks against AC LCDRs. Simulations are carried out using the PSCAD/EMTDC program. Additionally, to obtain the small-signal and voltage

instability margins, system Power-Voltage (PV) curves and eigenvalues are obtained using the Power System Analysis Toolbox (PSAT). The static data of the test system—used for obtaining PV curves—can be found in [68]. To obtain system eigenvalues, the data related to dynamic modeling of generators—including the exciters and Automatic Voltage Regulators (AVRs)—are chosen based on the typical data given in [69]. In this test system, a 30 MVAr capacitor bank is installed at bus 5 to supply the required reactive power. Lines 1-5, -5, 2-4, 6-13, and 13-14 of this system are designated as critical lines, as they supply critical loads or connect load centers to the generators; thus, they are protected by SV-based LCDRs. These LCDRs are set based on [1]. The trip logic of LCDRs is also considered to be similar to that of [1], in which the trip signals of differential, overcurrent, and distance elements are sent to an OR gate whose output is sent to breakers. Therefore, if any element detects a fault, the line would be tripped, regardless of other elements' output.

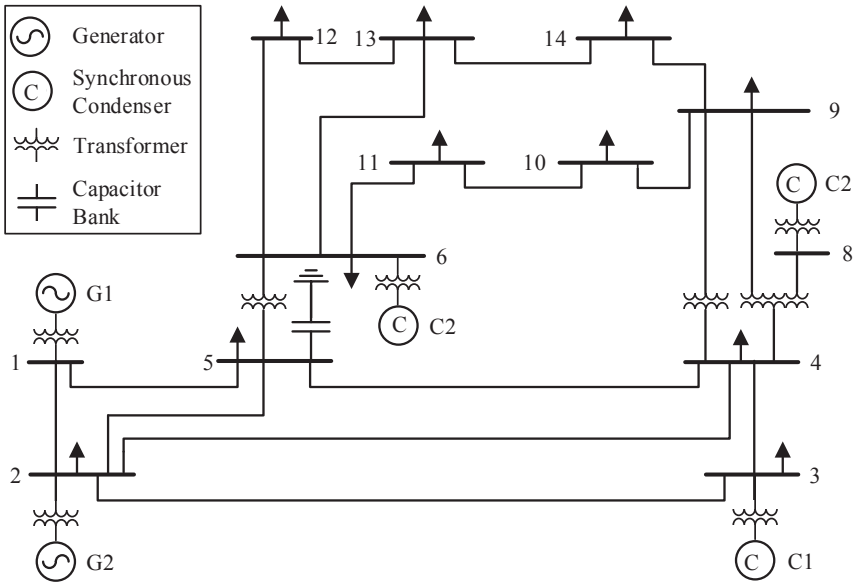


Figure 2.9: IEEE 14-bus test systems used for simulations.

The attack objective in this case study is considered to be a kind of instability, such as voltage collapse or small signal instability, that destabilizes the system or leads to a

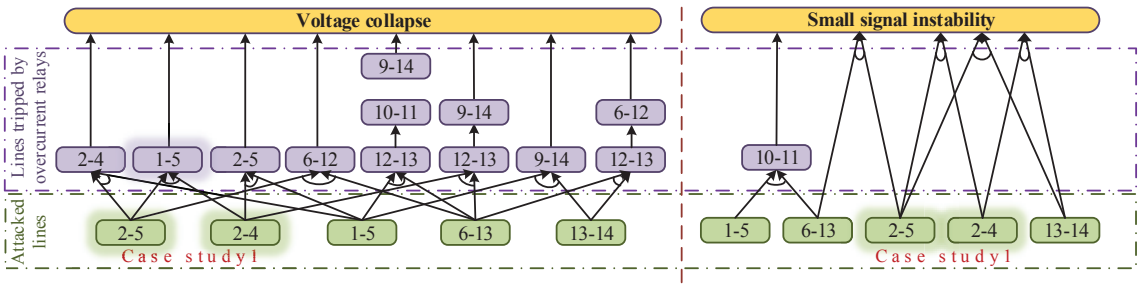


Figure 2.10: Attack tree showing intrusions that lead to voltage collapse and Small signal instability.

blackout. To this aim, attack trees have been used in this case study to assess the impact of cyber-attacks and to determine target LCDRs [70]. A main assumption considered here in obtaining attack trees is that attackers' resources are limited, so they can target and trip maximum only two lines for cyber-attacks. On this basis, all possible attack scenarios were simulated off-line, and the effect of each scenario was investigated. Fig. 2.10 illustrates attack trees for intrusions that lead to voltage collapse and small signal instability. In this figure, green and purple blocks show the targeted lines by cyber-attacks, and the lines that are tripped by the overcurrent element of protective relays after power flow are redirected due to the tripping of targeted lines. The rest of this study shows how targeting lines 1-5 and 2-5 can result in voltage collapse (and small signal instability as a byproduct).

The attack is initiated when the DD element of Line 2-5's LCDRs pick up after the capacitor bank installed at Bus 5 is switched on at $t = 20$ ms. Fig. 2.11 shows the magnitude and angle of the current of line 2-5: after this event, the magnitude and angle of the PS current increase by more than 0.02 p.u. and 8°, respectively, in 1 cycle. Therefore, the DD elements of Line 2-5's LCDRs pick up after the capacitor bank is switched on.

In the first step, the LCDRs of Line 2-5 should pick up by an FDIA to trip the line. Following the default settings given in [1], parameters I_0, I_b, k_1, and k_2 of this line's LCDRs are set at 0.03 kA, 0.4 kA, 0.2, and 0.4, respectively. During normal operation, the currents flowing into Line 2-5 from Buses 2 and 5 are $0.184\angle -90.3°$ kA and $0.164\angle 84.4°$ kA, respectively, so the restraining current is $I_{res}[k_0] = 0.348$ kA (where $[k_0]$ is 20 ms in this

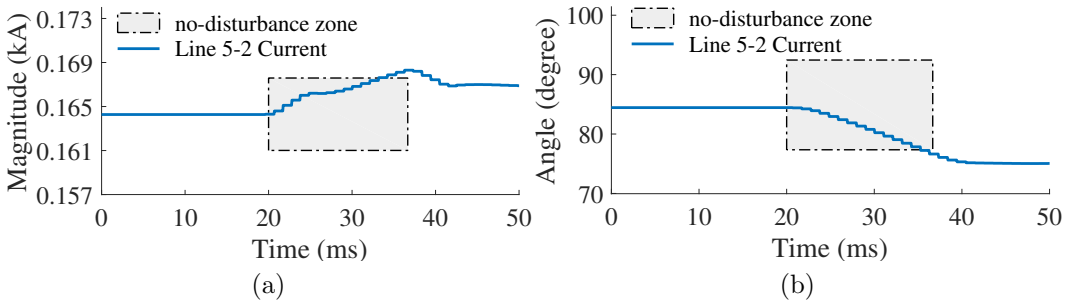


Figure 2.11: PS current entering Line 2-5 from Bus 5 after switching on the shunt capacitor bank installed at Bus 5 at $t = 20$ ms, (a) magnitude, (b) angle.

case study). During the FDIA, the current measurements sent from Bus 5 to Bus 2, i.e., $i_5[k]$, are going to be manipulated such that (2.26) is met. Any manipulation that satisfies this equation can be chosen for this FDIA. This case study, targets current measurements by an MMA, in which the true measurements are multiplied by a positive number, i.e., γ, resulting in $i_5^m[k] = \gamma \times i_5[k]$. Given that in this case study $\|i_5[k]\| = 0.164$ kA, the minimum γ that satisfies (2.26) is 1.83. Fig. 2.12 shows the trajectory of the LCDR installed at Bus 5 during an FDIA with $\gamma = 1.83$: once the attack starts, the estimated phasor of manipulated remote measurements, i.e., $i_5^m[k]$, increases, so the LCDR's trajectory moves toward the trip zone. It takes about 1 cycle for the estimated phasor to settle down at its final value. At this time, the operating point trajectory crosses I_{op}, and the line is tripped. The line could have been tripped in a shorter time, if a greater γ had been selected. In this case, the operating point would have been entered the trip zone before the phasor of the manipulated measurements reaches its final value.

After Line 2-5 is tripped, as shown in Fig. 2.13, the magnitude of Line 2-4's current increases by more than 0.02 p.u. per cycle, so the DD elements of LCDRs protecting this line also pick up. Thus, the second part of the coordinated attacks can be initiated to trip Line 2-4. Carrying out a procedure similar to that done for Line 2-5 and selecting a $\gamma \geq 1.92$, e.g., $\gamma = 2$, the trip signal is issued by the LCDRs of Line 2-4 in about 0.8 cycle.

To investigate the voltage stability of the network after the above-discussed attacks, and to determine the system's instability margin, the PV curves of Bus 5 during normal operation (base case), after tripping Line 2-5, and after tripping Line 2-4 are shown in

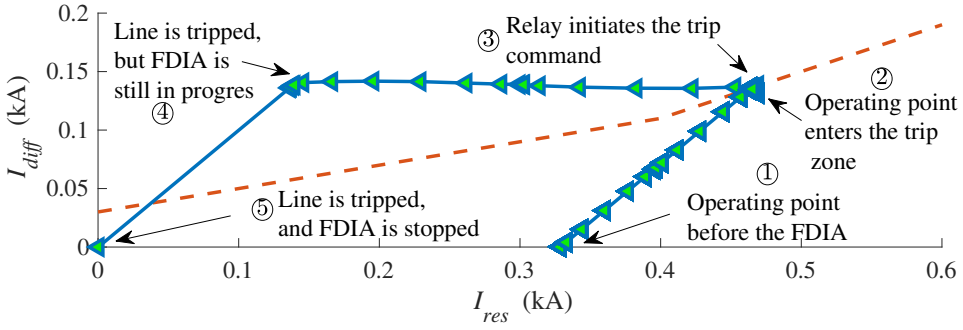


Figure 2.12: The trajectory of targeted LCDR of Line 2-5 during the FDIA.

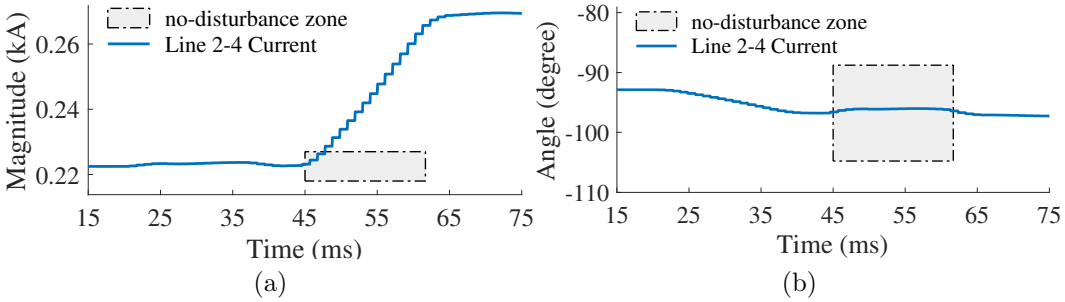


Figure 2.13: PS current entering Line 2-4 from Bus 2 after the tripping of Line 2-5 at $t = 45$ ms, (a) magnitude, (b) angle.

Fig. 2.14. In this figure, $\lambda = \frac{P}{P_0}$ is the loading factor, where P and P_0 denote the actual and nominal active powers of the system [71]. These curves indicate the voltage of Bus 5 at each operating point, as well as the Saddle-Node Bifurcation (SNB), i.e., the point at which a voltage collapse happens. In fact, at SNB and afterwards, the Jacobian and/or state matrix of the system becomes singular, resulting in no steady-state solution for power flow. Fig. 2.14 also illustrates the Hopf Bifurcation (HB) node, which is the onset of unstable poles. At HB point and beyond, the system parameters start to oscillate after any small perturbation [71]. As Fig. 2.14 illustrates, the operating point of the system is far enough from the SNB after tripping Lines 2-4 and 2-5. However, the HB node falls behind the operating point of the system, leading to small signal instability. This happens because, as shown in Fig. 2.15, the eigenvalues of the system after tripping these two lines contain two unstable poles, i.e., $1.468 \pm j7.781$. As a result, if a perturbation occurs, the

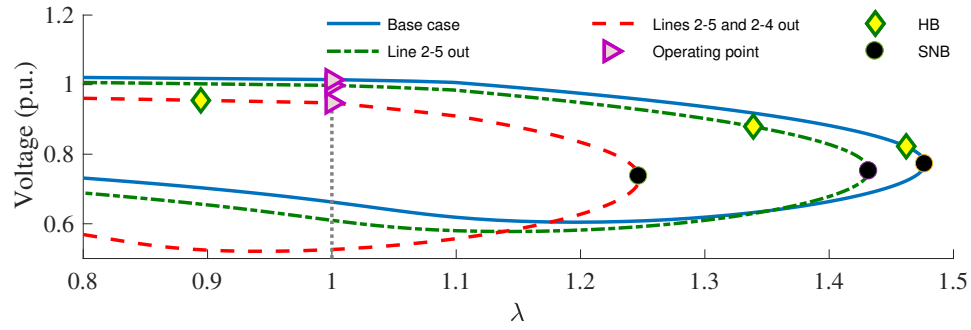


Figure 2.14: PV curves at Bus 5 during case study 1.

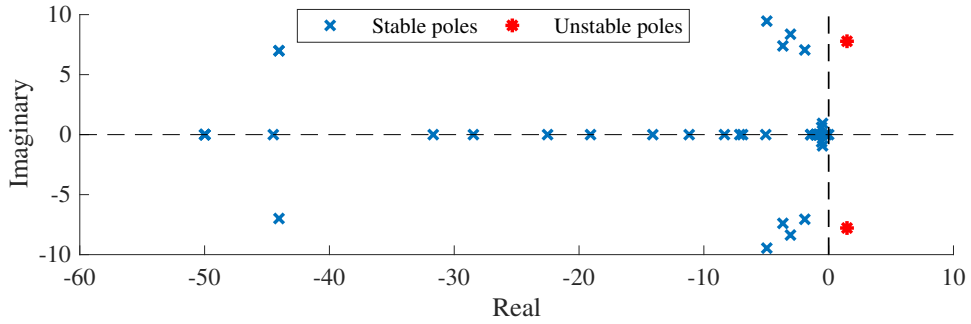


Figure 2.15: Eigenvalues of the system when Lines 2-5 and 2-4 are tripped.

system parameters start to oscillate. The small signal instability is not a major issue if the attack is detected on time, before oscillations become large enough to endanger the system integrity.

After tripping Lines 2-5 and 2-4, the current flowing into Line 1-5 becomes 2.45 p.u. This current is larger than the typical pickup current setting of this line's overcurrent elements. Consequently, Line 1-5 is also tripped. At this point, as shown in Fig. 2.16, the operating point of the system falls behind the SNB, resulting in a voltage collapse. As a result, coordinated attacks against LCDRs in this case study led to voltage instability.

2.6.2 Case Study 2

This case study also investigates the effect of coordinated attacks against AC LCDRs. In this case study, the 39-bus new England test system (Fig. 2.2) [72] is chosen as the

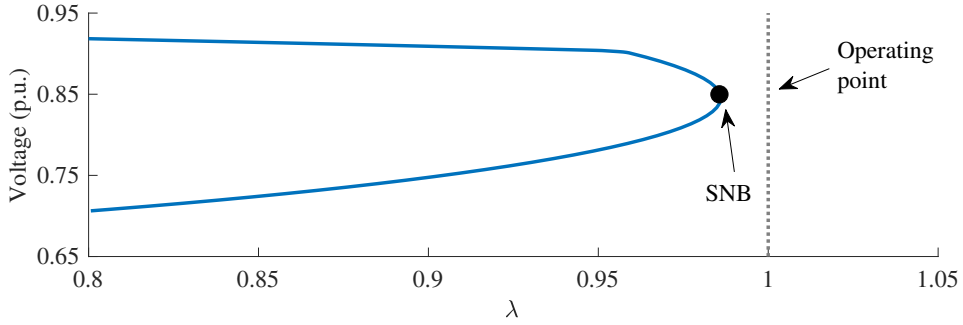


Figure 2.16: PV curve at Bus 5 after tripping Line 1-5.

target of coordinated attacks. The specifications of this test system are provided in Section 2.3 and Appendix A. The settings of frequency relays are also provided in Appendix A. Simulations are carried out using the PSCAD/EMTDC program. LCDRs in this case study are of phasor-based type and are set based on [1]. Additionally, he trip logic of LCDRs is considered to be similar to that of [1], in which the trip signals of differential, overcurrent, and distance elements are sent to an OR gate whose output is sent to breakers. Therefore, if any element detects a fault, the line would be tripped, regardless of other elements' outputs.

In this case study, the main objective is to create a frequency instability. Evaluating all possible attack scenarios and creating attack trees similar to Fig. 2.10 for this objective show that tripping Lines 6-11, 13-14, and 2-3 can achieve this objective. On this basis, an attacker starts the coordinated attacks at $t = 20$ ms, right after the DD element of LCDRs installed on Line 6-11 pick up due to a 20% load-change occurring at Bus 8. As it was shown in Fig. 2.8, the magnitude and angle of Line 6-11's current during one cycle satisfy the disturbance-detection criterion explained at the beginning of this section, so the DD element of Line 6-11's LCDRs picks up. At this moment, the attacker targets remote measurements received by the LCDR I installed on Bus 11 of Line 6-11 with the MMA explained in Section 2.3. Fig. 2.17 presents the trajectory of LCDR I during the MMA with $|\Delta I_6| = 0.251$ kA: once the attack starts, the trajectory of the LCDR moves toward the trip zone, so the trip signal is issued. When Line 6-11 is tripped at $t = 45$ ms, the angle and magnitude of the current flowing into Line 13-14 change about 2.4° and 0.13 p.u. in 1 cycle (as shown in Fig. 2.18), respectively, resulting in activation of the DD element

of Line 13-14's LCDRs. Similar to the MMA that was carried out for Line 6-11, at this time the attacker manipulates the current measurements received by the LCDR installed on Bus 14. As a result, the LCDR of Bus 14 also picks up, and Line 13-14 is tripped at $t = 70$ ms. Tripping of Line 13-14 changes the magnitude and angle of Line 2-3's current by 0.193 p.u. and 6.25° in 1 cycle, respectively, as illustrated in Fig. 2.19. Since in 1 cycle the magnitude of this line's current changes by more that 0.02 p.u., the DD element of LCDRs of Line 2-3 pick up. Thus, Line 2-3 is also tripped after the attacker modifies the phase angle of measurements sent from Bus 2 to Bus 3 by $\Delta\theta_2 = 40°$.

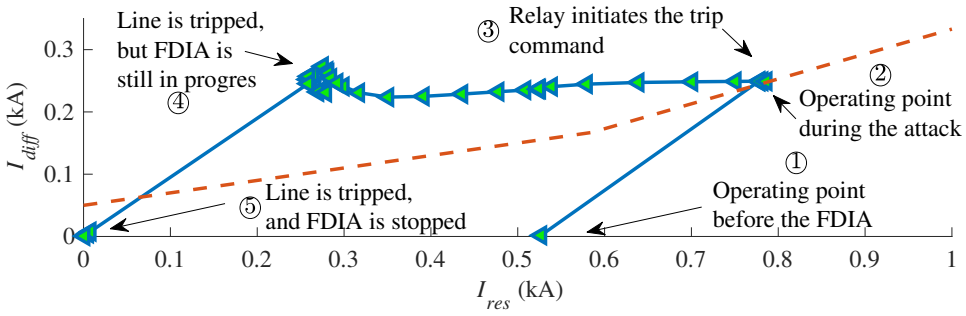


Figure 2.17: The trajectory of targeted LCDR of Line 6-11 during the FDIA.

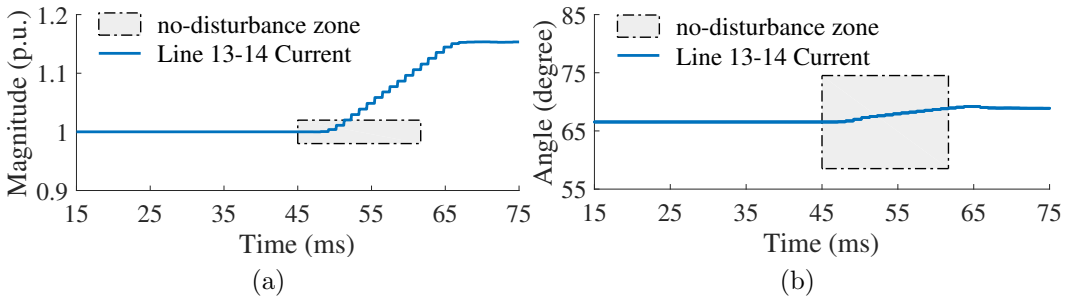


Figure 2.18: PS current entering Line 13-14 from Bus 14 after Line 6-11 is tripped at $t = 45$ ms, (a) magnitude, (b) angle.

Once the three above-mentioned lines are tripped by coordinated attacks, the power flow is redirected to healthy lines, resulting in the over-loading of some. Fig. 2.20 shows the current of over-loaded lines after the coordinated attacks (each line's current is normalized

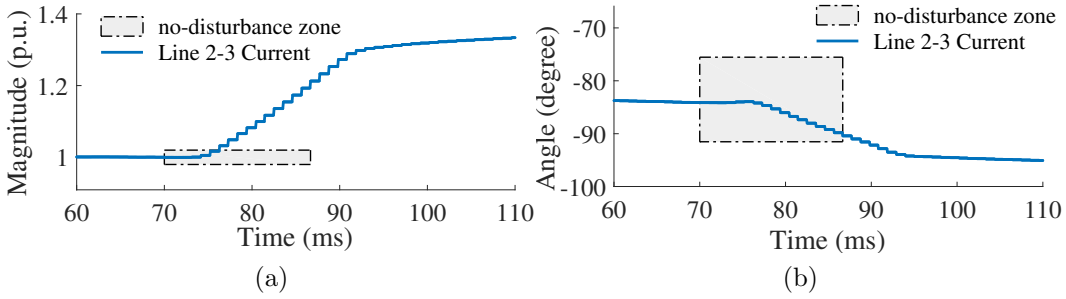


Figure 2.19: PS current entering Line 2-3 from Bus 2 after Line 13-14 is tripped at $t = 70$ ms, (a) magnitude, (b) angle.

based on its nominal current). As seen in this figure, the current of 13 lines become initially more than 2 p.u., and the situation even gets worse when the highly over-loaded ones (i.e., lines 17-27, 3-18, 25-26) are tripped by their overcurrent element or zone 3 of their distance elements. Therefore, the cascading failures of all 13 overloaded lines happen. As a result of these cascading failures, the system loses its synchronism and becomes unstable (Fig. 2.21). Consequently, the frequency of Generators 3, 4, 5, 8, and 10 reaches 61.8 Hz (Fig. 2.21a), so these generators are tripped by their Over Frequency Relays (OFRs). On the other hand, the frequency of Generator 2 decreases steeply after the attack, such that the Under Frequency Load Shedding (UFLS) scheme operates. However, UFLS cannot stop the frequency reduction, and the frequency of generator 2 reaches 57.8 Hz (Fig. 2.21b), so it is tripped by its Under Frequency Relay (UFR). In conclusion, the coordinated attacks in this case-study made the system unstable, tripped 6 generators, and disrupted energy supply to 69% of the load.

2.6.3 Case Study 3

This case study investigates the effect of coordinated attacks against DC LCDRs. In this case study, a 7-bus medium-voltage DC test system (Fig. 2.22), consisting of three Distributed Generations (DGs), is chosen as the target of coordinated attacks. The specifications of this test system are provided in Appendix B. The main protection of lines in the test system is the differential scheme. Accordingly, multiplexed channels and the GPS are utilized in this case study for the communication of LCDRs and for time synchronization,

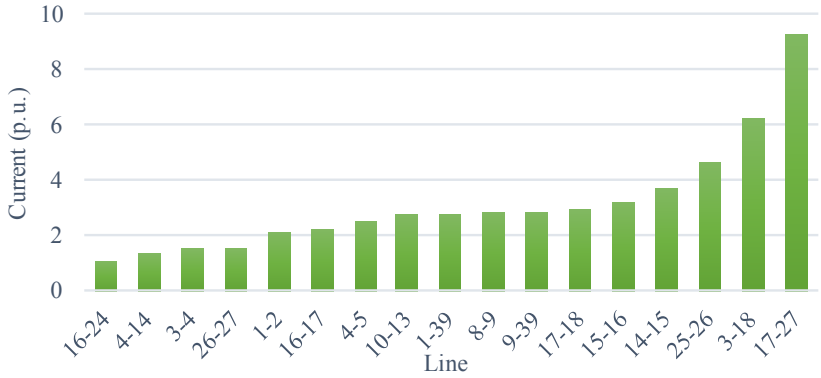


Figure 2.20: Over-loaded lines and their currents after the coordinated attacks.

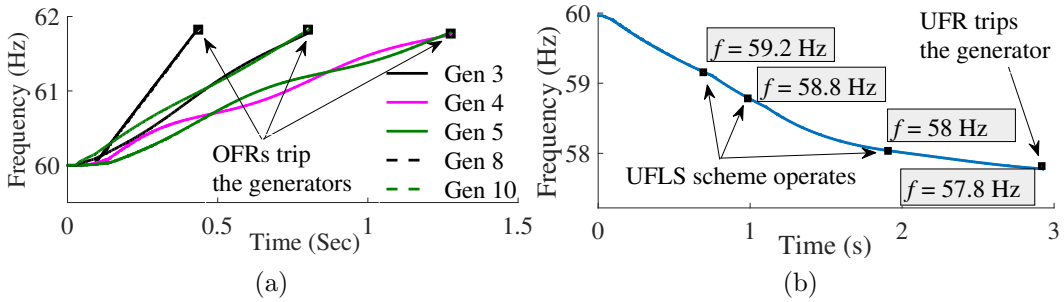


Figure 2.21: Frequencies of generators after the coordinated attacks, (a) over-frequency, (b) under-frequency (Generator 2).

respectively. The reliability coefficient of LCDRs is set at $\kappa = 0.2$ [16]. Given that LCDRs share their measurements every 1 ms [17], and that proactive DC hybrid circuit breakers trip the line in 1 ms [73], the fault detecting and clearing process takes at maximum 3 ms, including the relay process time. Additionally, overcurrent relays are utilized in the test system as the backup protection scheme [17]. The pickup current of each line's overcurrent relay is selected as the line's maximum current during normal operation plus a 50% security margin [74]. In this dissertation, 120% of the line's nominal current is considered as the maximum overcurrent during normal operation.

To prevent voltage collapse and ensure stable operation of the test system during power mismatch, a load management scheme is incorporated. This scheme sheds lower-priority loads to prevent total system collapse and ensure secure power supply to higher-priority

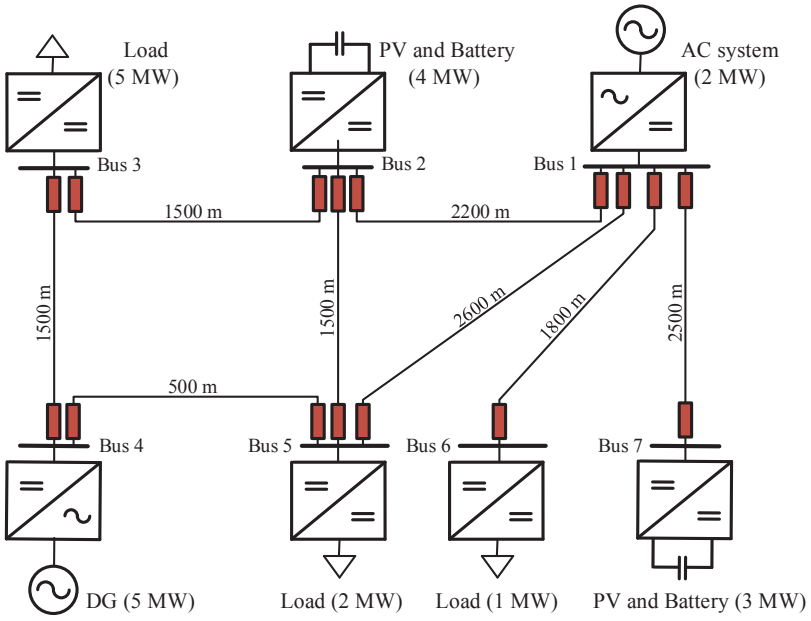


Figure 2.22: DC test system.

loads. This dissertation implements the load shedding scheme proposed in [75], in which the load on Bus 1 has the lowest priority and is shed immediately if its voltage drops by 15%; loads on Buses 5 and 6 are the next priorities and are shed if their voltages drop by 20% and 25%, respectively, and remain under this threshold for 0.5 s. The load on Bus 3 has the highest priority.

In this case study, the main objective is to create a voltage collapse. Evaluating all possible attack scenarios and creating attack trees similar to Fig. 2.10 for this objective show that tripping Lines 2-5, and 3-4 can achieve this objective. On this basis, an attacker starts coordinated attacks at $t = 9$ ms by spoofing the GPS signal of the substation installed at Bus 3. Given that LCDRs' measurements are sent every 1 ms, by changing time-stamps of measurements from t to $t + 1$ ms, remote LCDRs, i.e., LCDRs at Buses 2 and 4 on Lines 3-2 and 3-4, assume that the packet that was supposed to be sent at $t = 9$ ms has been lost, so they suspend their functioning for time $t = 9$ ms, and get back to normal operation at $t = 10$ ms, when both local and remote measurements are available

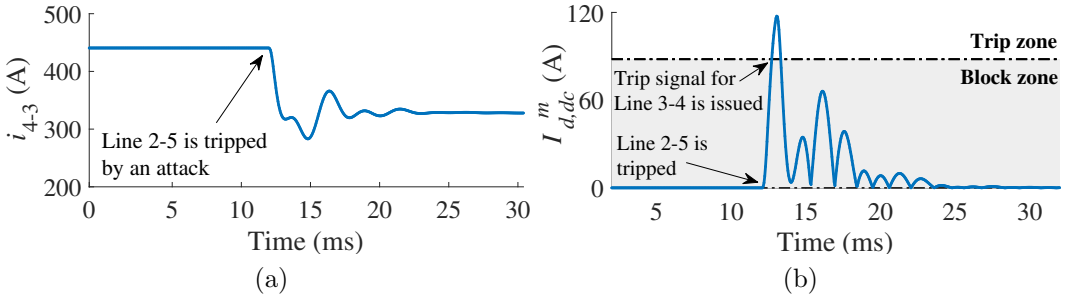


Figure 2.23: (a) Current of Line 4-3 after tripping of Line 2-5, (b) differential current of LCDR installed at Bus 4.

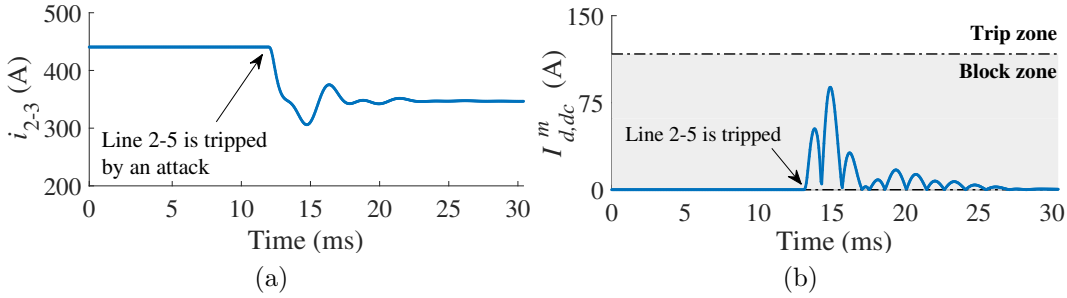


Figure 2.24: (a) Current of Line 2-3 after tripping of Line 2-5, (b) differential current of LCDR installed at Bus 2.

again. As a result, during this attack, the time stamps of Bus 3's measurements exceed the actual time by 1 ms. This attack can impact the operation of LCDRs of Lines 2-3 and 3-4 if a significant transient happens. During steady state, however, the differential currents of remote LCDRs installed at buses 4 and 2 are not affected, since the currents of Lines 2-3 and 3-4 are constant. Meanwhile, at $t = 10$ ms, the attacker intrudes into the communication system and manipulates remote measurements of Line 2-5, sent from Bus 2 to Bus 5. During this FDIA, the measurements are increased by 25%, so this line's trip criterion, expressed in (2.8), is met, and the line is tripped at $t = 13$ ms.

Tripping of Line 2-5 creates a transient in nearby buses and changes the power flow in neighboring lines, as shown in Figs. 2.23a and 2.24a. On the other hand, because the TSA is still in progress during this transient and the remote measurements sent from Bus 3 to LCDRs installed at buses 4 and 2 are incorrectly time-stamped, the differential currents of

these LCDRs rise, as shown in Figs. 2.23b and 2.24b. Since the current of Line 3-4 changes by a rate larger than κI_n, (2.8) is met and the operating point of the LCDR installed on Bus 4 enters the trip zone (Fig. 2.23b). Thus, Line 3-4 is tripped at $t = 16$ ms. However, the differential current of Bus 2's LCDR remains in the block zone (Fig. 2.24b).

When both Lines 2-5 and 3-4 are tripped, the power flow in healthy lines is redirected, overloading Line 1-5 (Fig. 2.25). In this figure, the current is normalized based on the nominal current of the line, and the pickup setting of this line's OCR is set at 1.8 p.u. As seen in Fig. 2.25, the current of Line 1-5 increases steeply, such that it exceeds the pickup setting at $t = 18$ ms. As a result, the relay issues the trip command, and the line is disconnected at $t = 19$ ms. Once this line is tripped, Buses 4 and 5 split from the rest of the grid, resulting in a separate island, called Island 1. This island continues its operation with the load on Bus 5 supplied by the DG on Bus 4. The DC grid, on the other hand, gets shortchanged of power, so the system voltage starts to collapse (Fig. 2.26). However, when the voltage at Bus 1 reaches 0.85 p.u. at $t = 340$ ms, the load on this bus—which has the lowest priority—is shed, and the system voltage becomes stable again, as shown in Fig 2.26. However, as shown in Fig. 2.27, the current of Line 1-2 increases after tripping the load on Bus 1. The increased current exceeds the pickup setting of this line's overcurrent relay at $t = 341$ ms; thus the trip signal of Line 1-2 is issued, and the line is tripped at $t = 342$ ms. At this time, the rest of the test DC grid splits up into two separate islands (i.e., Island 2 for Buses 1, 6 and 7, and Island 3 for Buses 2 and 3). In island 2, the load on Bus 6 is supplied by the Photovoltaic (PV) DG installed on Bus 7. However, the voltage in island 3 collapses due to the shortage in the generated power, as in Fig. 2.28, which happens because the total generation in Island 3 is one MW less than the total load. In conclusion, coordinated attacks in this case study resulted in the disruption of energy supply to 70% of loads, tripping of half of the lines, and splitting of the system into 3 islands.

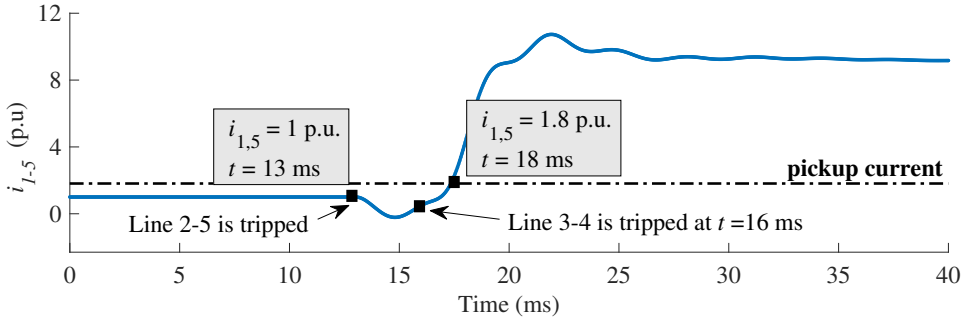


Figure 2.25: Current of Line 1-5 after tripping of Lines 2-5 and 3-4.

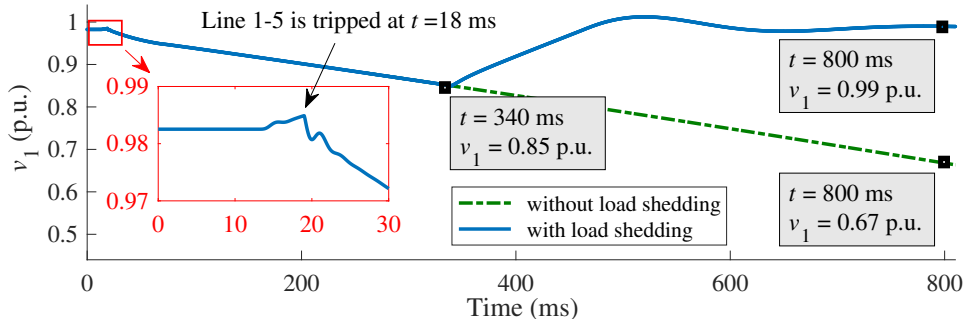


Figure 2.26: Voltage at Bus 1 after tripping Line 1-5, and the effect of load shedding scheme on voltage stability.

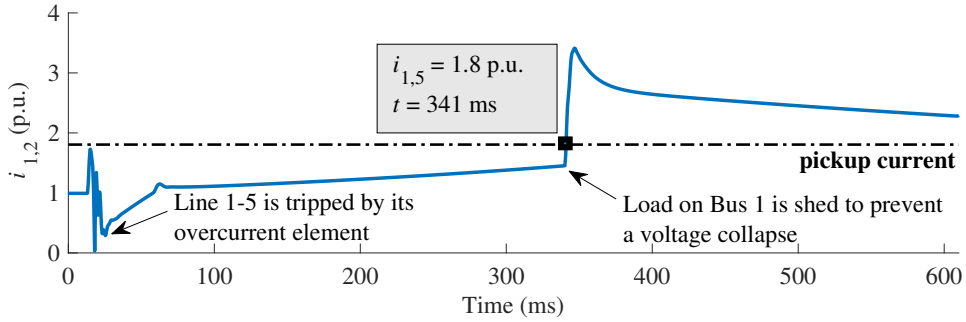


Figure 2.27: Line 1-2's current after tripping Line 1-5 and disconnecting the load on Bus 1.

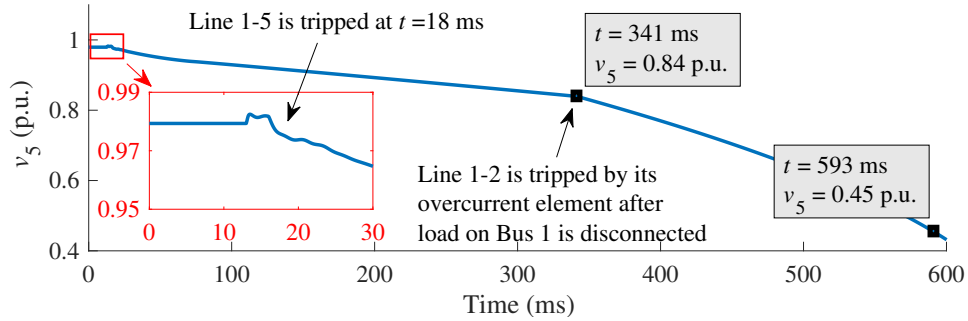


Figure 2.28: Voltage at Bus 5 after tripping Line 1-2.

2.7 Conclusion

This chapter first unveiled the vulnerabilities of AC and DC LCDRs to cyber-attacks, and discussed how these relays can be targeted by FDIAs or TSAs. Then, the mathematical formulation of cyber-attacks against both AC and DC LCDRs was presented. For AC LCDRs in particular, four attack strategies were proposed and simulated next to shown how cyber-attacks can move the operating point of AC LCDRs into the trip zone. It was also shown how the more secured type of AC LCDRs, which are equipped with DD elements, can be fooled into tripping the line they are protecting. Afterwards, through three case studies, this chapter demonstrated the consequences of coordinated attacks against AC and DC LCDRs. In all case studies, a kind of instability happened and the system integrity collapsed. As a result, the cyber-security of LCDRs against cyber-attacks is a crucial issue which must be addressed.

Chapter 3

Attack Detection Method for SV-based AC LCDRs

As shown in Chapter 2, AC LCDRs are vulnerable to FDIAs and TSAs. This vulnerability can potentially lead to an instability if several attacks are coordinated against several LCDRs in the system. To address this issue for SV-based AC LCDRs, this chapter proposes a method to detect FDIAs using UIOs and to distinguish them from internal faults. The proposed method is comprised of PS and NS submodules, each including a UIO to estimate the local PS and NS voltages based on the state-space model of the faulty line in each sequence. Immediately after an SV-based AC LCDR picks up, the proposed method calculates the fault location to obtain the state-space model of the potentially faulty line, and estimates each sequence's local voltages using UIOs. The RF for each submodule, i.e., the difference between the measured and estimated local voltage for the sequence associated with that submodule, remains close to zero during real internal faults, because in this condition the state-space model based on which the UIOs operate correctly represents the line. Nevertheless, the state-space model mismatch during FDIAs leads to large RFs. Thus, a rise in the RFs after an LCDR pickup signifies an FDIA or a TSA, so the trip signal of the LCDR is blocked.

The proposed method requires time-synchronized SVs of local and remote terminals, a communication platform, and a fast-enough processor. Given that the proposed method is

supposed to operate as a built-in function in SV-based microprocessor digital LCDRs, most of these requirements are already in place; that is, commercial SV-based LCDRs already share time-synchronized SVs of remote current measurements using a communication system and utilize state-of-the-art processors for analyzing received measurements to detect faults. Therefore, no extra hardware or communication equipment is required. Additionally, the fast communication platforms that are already being used for sharing SVs enable the proposed method to detect attacks and differentiate them from faults quickly, in less than two cycles, which is in the range of commercial LCDRs' operation time. However, the proposed method needs remote voltage SVs as well, which are not currently being shared by commercial LCDRs. Given that local voltage SVs are already available for LCDRs, sharing them along with current SVs is possible by increasing the communication bandwidth.

On this basis, Section 3.1 describes the state-space model of transmission lines for both PS and NS. Section 3.2 proceeds with a brief overview of UIOs and their design procedure. The FDIA and TSA diagnosis idea and procedure is covered in Section 3.3. Afterwards, the performance of the proposed method is evaluated and its effectiveness is corroborated in Section 3.4. Finally, Section 3.7 concludes this chapter.

3.1 State-Space Model of AC Transmission Lines During Internal Faults

This section presents the state-space representation of transmission lines for both PS and NS during internal faults. The model is obtained from the perspective of LCDR I installed at Terminal T_1 in Fig. 2.1. A similar model can be also achieved for LCDR II installed at Terminal T_2. The obtained state-space models are used later in Sections 3.2 and 3.3 for detecting FDIAs against LCDRs.

Fig. 2.1 shows the PS and NS models of a transmission line during an internal fault. The fault is modeled by a current source at the fault location [76], and has occurred at a distance of xL from terminal T_1, where L is the length of the line and $0 < x < 1$. To find x, the fault location technique suggested in [77] for LCDRs is used. PS and NS voltages and currents in this figure, i.e., $s \in \{+, -\}$, are instantaneous values, and are obtained

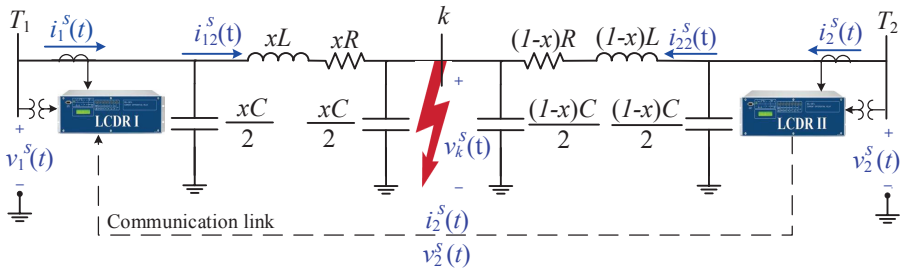


Figure 3.1: A two-terminal transmission line during internal faults.

from the sampled values using

$$\Phi^{+}(t) = \frac{1}{3}\left[\Phi_a(t) + \Phi_b\left(t - \frac{f_s}{3f}\right) + \Phi_c\left(t - \frac{2f_s}{3f}\right)\right] \tag{3.1a}$$

$$\Phi^{-}(t) = \frac{1}{3}\left[\Phi_a(t) + \Phi_b\left(t - \frac{2f_s}{3f}\right) + \Phi_c\left(t - \frac{f_s}{3f}\right)\right] \tag{3.1b}$$

where Φ denotes any voltage or current whose instantaneous PS or NS components is required; subscripts a, b, and c represent the three phases; and f_s and f are the sampling and fundamental frequencies. Therefore, the delays introduced by $f_s/3f$ and $2f_s/3f$ are 120° and 240°, respectively [78].

Using the circuit of Fig. 3.1, the differential equations that relate the voltages and currents of the line in each sequence are:

$$i^s_{12}(t) - i^s_1(t) + \frac{xC}{2}\frac{dv^s_1(t)}{dt} = 0 \tag{3.2a}$$

$$v^s_1(t) - xRi^s_{12}(t) - xL\frac{di^s_{12}(t)}{dt} - v^s_k(t) = 0 \tag{3.2b}$$

$$i^s_{22}(t) - i^s_2(t) + \frac{(1-x)C}{2}\frac{dv^s_2(t)}{dt} = 0 \tag{3.2c}$$

$$v^s_2(t) - (1-x)Ri^s_{22}(t) - (1-x)L\frac{di^s_{22}(t)}{dt} - v^s_k(t) = 0 \tag{3.2d}$$

$$i_{12}^s(t) + i_{22}^s(t) + i_f^s(t) - \frac{C}{2}\frac{dv_k^s(t)}{dt} = 0 \tag{3.2e}$$

where $i_f^s(t)$ is the current at the fault location, which is unknown. Using (3.2a)-(3.2e), the state-space model of the line in Fig. 3.1 is as follows for each sequence:

$$\underbrace{\begin{bmatrix} \dot{v}_1^s(t) \\ \dot{v}_2^s(t) \\ \dot{v}_k^s(t) \\ \dot{i}_{12}^s(t) \\ \dot{i}_{22}^s(t) \end{bmatrix}}_{\dot{\mathbb{X}}^s(t)} = \underbrace{\begin{bmatrix} 0 & 0 & 0 & \frac{-2}{xC} & 0 \\ 0 & 0 & 0 & 0 & \frac{-2}{(1-x)C} \\ 0 & 0 & 0 & \frac{2}{C} & \frac{2}{C} \\ \frac{1}{xL} & 0 & \frac{-1}{xL} & \frac{-R}{L} & 0 \\ 0 & \frac{1}{(1-x)L} & \frac{-1}{(1-x)L} & 0 & \frac{-R}{L} \end{bmatrix}}_{\mathbb{A}_c} \underbrace{\begin{bmatrix} v_1^s(t) \\ v_2^s(t) \\ v_k^s(t) \\ i_{12}^s(t) \\ i_{22}^s(t) \end{bmatrix}}_{\mathbb{X}^s(t)} +$$

$$\underbrace{\begin{bmatrix} \frac{2}{xC} & 0 & 0 & 0 & 0 \\ 0 & \frac{2}{(1-x)C} & 0 & 0 & 0 \end{bmatrix}^T}_{\mathbb{B}_{c,n}^T} \underbrace{\begin{bmatrix} i_1^s(t) \\ i_2^s(t) \end{bmatrix}}_{\mathbb{U}_n^s(t)} + \underbrace{\begin{bmatrix} 0 & 0 & \frac{2}{C} & 0 & 0 \end{bmatrix}^T}_{\mathbb{B}_{c,u}^T} i_f^s(t) \tag{3.3a}$$

$$\mathbb{Y}^s(t) = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}}_{\mathbb{C}} \mathbb{X}^s(t) \tag{3.3b}$$

where, $\mathbb{X}^s$ is the state vector for sequence s; $\mathbb{A}_c$, $\mathbb{B}_{c,n}$, and $\mathbb{B}_{c,u}$ are the continuous state, known input, and unknown input matrices; $\mathbb{C}$ is the output matrix; $\mathbb{U}_n^s$ is the known input vector, which includes current measurements from terminals T_1 and T_2 for sequence s; $\mathbb{Y}^s$ is the output vector for sequence s, which includes voltage measurements; and T is the transpose operator.

To make a pair of state-space equations, such as (3.3), suitable for numerical implementation, the continuous matrices A_c, $B_{c,n}$, and $B_{c,u}$ in (3.3) are discretized using

$$\mathbb{A} = e^{\mathbb{A}_c \times T_s} \tag{3.4a}$$

$$\mathbb{B}_n = \int_{\tau=0}^{T_s} e^{\mathbb{A}_c \times \tau} \mathbb{B}_{c,n} d\tau \tag{3.4b}$$

where T_s denotes the discretization time step [79]. $\mathbb{B}_{c,u}$ should also be discretized by

substituting it with $\mathbb{B}_{c,n}$ in (3.4b), resulting in $\mathbb{B}_u$. Therefore, the discretized model of the system in (3.3) is

$$\mathbb{X}^s[k+1] = \mathbb{A}\mathbb{X}^s[k] + \mathbb{B}_n\mathbb{U}_n^s[k] + \mathbb{B}_u i_f^s[k] \tag{3.5a}$$

$$\mathbb{Y}^s[k] = \mathbb{C}\mathbb{X}^s[k] \tag{3.5b}$$

where $\mathbb{X}^s[k] \in \mathbb{R}^n$, $\mathbb{U}_n[k] \in \mathbb{R}^m$, and $\mathbb{Y}[k] \in \mathbb{R}^p$ are the state, known input, and output vectors at time step k, respectively, and $i_s^f[k] \in R^1$ is the only unknown input. To deal with the unavailability of i_f^s, a UIO—which works independently from its unknown inputs—should be used, as explained in the next section.

3.2 A UIO for State Estimation in the Presence of Unknown Inputs

To estimate the states of the system in (3.3) accurately without requiring the value of i_f^s, a UIO can be used. A UIO estimates the states of a system by using its outputs $\mathbb{Y}^s$ and known inputs, i.e., $\mathbb{U}_n^s$, without requiring its unknown inputs [80]. Such observers are suitable for studying conditions that involve uncertain dynamics, faults, or attacks, as well as when real-time values of system inputs are unavailable [81]. Therefore, as the fault current i_f^s is not normally available, a UIO is an appropriate tool for estimating the states of the system.

As shown in [82], state estimation in the presence of unknown inputs is possible if a delay, denoted by α, is introduced to the UIO. The value of α depends on system parameters, as explained later. Thus, an $(\alpha+1)$-samples-long window from time step k to $k+\alpha$ is considered for estimating the states of the system at time step k. In this window, $k+\alpha$ is the most recent sampling instant. System outputs during this window, i.e., $\mathbb{Y}^s[k]$ to $\mathbb{Y}^s[k+\alpha]$, are used to estimate $\mathbb{X}^s[k]$.

To develop a UIO for (3.3), the system outputs given by this equation should be developed in a matrix form for the duration of the above window, i.e., from time step k to

$k+\alpha$, as follows

$$\mathcal{Y}^s\left[k:k+\alpha\right] = \mathcal{O}_\alpha \mathbb{X}^s\left[k\right] + \mathcal{J}_{n,\alpha}\mathcal{U}_n^s\left[k:k+\alpha\right] + \mathcal{J}_{u,\alpha} i_f^s\left[k:k+\alpha\right] \tag{3.6}$$

where,

$$\mathcal{Y}^s\left[k:k+\alpha\right] = \begin{bmatrix} \mathbb{Y}^s\left[k\right]^T & \mathbb{Y}^s\left[k+1\right]^T & \cdots & \mathbb{Y}^s\left[k+\alpha\right]^T \end{bmatrix}^T \tag{3.7a}$$

$$\mathcal{O}_\alpha = \begin{bmatrix} \mathbb{C}^T & (\mathbb{C}\mathbb{A})^T & \cdots & (\mathbb{C}\mathbb{A}^\alpha)^T \end{bmatrix}^T \tag{3.7b}$$

$$\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{p\times 1} & O_{p\times 1} & \cdots & O_{p\times 1} \\ \mathbb{C}\mathbb{B}_u & O_{p\times 1} & \cdots & O_{p\times 1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \cdots & O_{p\times 1} \end{bmatrix} \tag{3.7c}$$

$$\mathcal{J}_{n,\alpha} = \begin{bmatrix} O_{p\times m} & O_{p\times m} & \cdots & O_{p\times m} \\ \mathbb{C}\mathbb{B}_n & O_{p\times m} & \cdots & O_{p\times m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_n & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_n & \cdots & O_{p\times m} \end{bmatrix} \tag{3.7d}$$

$$\mathcal{U}_n^s\left[k:k+\alpha\right] = \begin{bmatrix} \mathbb{U}_n^s\left[k\right]^T & \mathbb{U}_n^s\left[k+1\right]^T & \cdots & \mathbb{U}_n^s\left[k+\alpha\right]^T \end{bmatrix}^T \tag{3.7e}$$

$$i_f^s\left[k:k+\alpha\right] = \begin{bmatrix} i_f^s\left[k\right] & i_f^s\left[k+1\right] & \cdots & i_f^s\left[k+\alpha\right] \end{bmatrix}^T \tag{3.7f}$$

In these equations, O is the zero matrix.

For a reliable UIO, the estimation error should approach zero as $k \to \infty$. Accordingly, a UIO that estimates the state vector $\mathbb{X}^s$ at time step $k+1$ can be formulated as

$$\hat{\mathbb{X}}^s\left[k+1\right] = \mathbb{A}\hat{\mathbb{X}}^s\left[k\right] + \mathbb{B}_n\mathbb{U}_n^s\left[k\right] + \mathcal{L}\left(\mathcal{Y}^s[k:k+\alpha] - \mathcal{O}_\alpha\hat{\mathbb{X}}^s\left[k\right] - \mathcal{J}_{n,\alpha}\mathcal{U}_n^s\left[k:k+\alpha\right]\right) \tag{3.8}$$

where $\mathbb{X}^s\left[k\right]$ is the estimate for $\mathbb{X}^s\left[k\right]$ and $\mathcal{L}$ is the UIO's gain, designed such that the UIO is accurate and stable. Once $\mathcal{L}$ is determined, the UIO is fully developed.

3.2.1 Accuracy of UIO

The UIO defined by (3.8) is accurate when $\hat{\mathbb{X}}^s[k] \rightarrow \mathbb{X}^s[k]$ as $k \rightarrow \infty$. To satisfy this condition without requiring the unknown input vector $\mathbb{U}_n[k]$, the UIO's error, i.e., $e^s[k+1] = \hat{\mathbb{X}}^s[k+1] - \mathbb{X}^s[k+1]$, is obtained using (3.5) and (3.8):

$$e^s[k+1] = \underbrace{(\mathbb{A} - \mathcal{L}\mathcal{O}_\alpha)}_{\mathbb{A}'}\hat{\mathbb{X}}^s[k] + \mathcal{L}\mathcal{Y}^s[k:k+\alpha] - \mathcal{L}\mathcal{J}_{n,\alpha}\mathcal{U}_n^s[k:k+\alpha] - \mathbb{A}\mathbb{X}^s[k] - \mathbb{B}_u i_f^s[k] \tag{3.9}$$

By substituting $\mathcal{Y}^s[k:k+\alpha]$ from (3.6), (3.9) can be simplified to

$$e^s[k+1] = \underbrace{(\mathbb{A} - \mathcal{L}\mathcal{O}_\alpha)}_{\mathbb{A}'}e^s[k] + \mathcal{L}\mathcal{J}_{u,\alpha}i_f^s[k:k+\alpha] - \mathbb{B}_u i_f^s[k] \tag{3.10}$$

It is clear from (3.10) that the accuracy condition is met and $e^s[k+1]$ approaches zero if the last two terms on the right side of (3.10) cancel out each other, i.e.,

$$\mathcal{L}\mathcal{J}_{u,\alpha} = \begin{bmatrix} \mathbb{B}_u & O_{n\times 1} & \cdots & O_{n\times 1} \end{bmatrix} \tag{3.11}$$

Theorem 1 shown that there is an $\mathcal{L}$ that satisfies (3.11) if (3.12) is satisfied [81].

$$rank\left(\mathcal{J}_{u,\alpha}\right) - rank\left(\mathcal{J}_{u,\alpha-1}\right) = 1 \tag{3.12}$$

In (3.12), $\mathcal{J}_{u,\alpha-1}$ is obtained using $\mathcal{J}_{u,\alpha}$ in (3.7c) and is as follows:

$$\mathcal{J}_{u,\alpha-1} = \begin{bmatrix} O_{p\times 1} & O_{p\times 1} & \cdots & O_{p\times 1} \\ \mathbb{C}\mathbb{B}_u & O_{p\times 1} & \cdots & O_{p\times 1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_u & \cdots & O_{p\times 1} \end{bmatrix} \tag{3.13}$$

Theorem 1. *There is a matrix $\mathcal{L}$ that satisfies (3.11) if and only if (3.12) is satisfied.*

□

Proof. As $\mathcal{L}\mathcal{J}_{u,\alpha}$ must result in $\Gamma = \begin{bmatrix} \mathbb{B}_u & O_{n\times 1} & \cdots & O_{n\times 1} \end{bmatrix}$, Γ can be constructed with

a linear combination of rows of $\mathcal{J}_{u,\alpha}$. Therefore, there exists an $\mathcal{J}_{u,\alpha}$ that satisfies (3.11) if and only if Γ is in the space spanned by the rows of $\mathcal{J}_{u,\alpha}$. Based on the matrix rank definition, this condition is equivalent to:

$$rank\left(\begin{bmatrix}\Gamma\\ \mathcal{J}_{u,\alpha}\end{bmatrix}\right) = rank\left(\mathcal{J}_{u,\alpha}\right) \tag{3.14}$$

Using (3.7c), $\mathcal{J}_{u,\alpha}$ in (3.14) can equivalently be expressed by

$$\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{p\times 1} & O_{p\times\alpha} \\ \Theta_{\alpha-1}\mathbb{B}_u & \mathcal{J}_{u,\alpha-1}\end{bmatrix} \tag{3.15}$$

where $\mathcal{J}_{u,\alpha-1}$ is given in (3.13), and $\Theta_{\alpha-1}$ is as follows

$$\Theta_{\alpha-1} = \begin{bmatrix} \mathbb{C}^T & (\mathbb{C}\mathbb{A})^T & \cdots & (\mathbb{C}\mathbb{A}^{\alpha-1})^T \end{bmatrix}^T \tag{3.16}$$

By substituting (3.15) in (3.14), the left side of this equation is equal to

$$rank\left(\begin{bmatrix}\Gamma\\ \mathcal{J}_{u,\alpha}\end{bmatrix}\right) = rank\left(\begin{bmatrix} \mathbb{B}_u & O_{n\times\alpha} \\ O_{p\times 1} & O_{p\times\alpha} \\ \Theta_{\alpha-1}\mathbb{B}_u & \mathcal{J}_{u,\alpha-1}\end{bmatrix}\right) \tag{3.17}$$

Multiplying the first row of the right side of (3.17) by $\Theta_{\alpha-1}$ and subtracting the product from the third row results in

$$rank\left(\begin{bmatrix}\Gamma\\ \mathcal{J}_{u,\alpha}\end{bmatrix}\right) = rank\left(\begin{bmatrix} \mathbb{B}_u & O_{n\times\alpha} \\ O_{p\times 1} & O_{p\times\alpha} \\ O_{\alpha p\times 1} & \mathcal{J}_{u,\alpha-1}\end{bmatrix}\right) \tag{3.18}$$

As $rank\left(\mathbb{B}_u\right) = 1$,

$$rank\left(\begin{bmatrix}\Gamma\\ \mathcal{J}_{u,\alpha}\end{bmatrix}\right) = 1 + rank\left(\mathcal{J}_{u,\alpha-1}\right) \tag{3.19}$$

Thus, by substituting (3.14) in (3.19), (3.12) is obtained.

■

Equation (2.2) is the necessary condition for development of a UIO for (3.5). In other words, if this condition is not met, it will not be possible to estimate the states of a system without requiring its unknown inputs. By substituting matrices $\mathbb{A}$, $\mathbb{B}_u$, and $\mathbb{C}$ in (3.7c) and (3.13) and finding the rank of $\mathcal{J}_{u,\alpha}$ and $\mathcal{J}_{u,\alpha-1}$, it can be shown that $\alpha = 2$ satisfies the condition of (3.12). Thus, by selecting $\alpha = 2$, there is an $\mathcal{L}$ that satisfies (3.12). As Theorem 2 proves, such an $\mathcal{L}$ can be formed as follows:

$$\mathcal{L} = [\mathcal{L}_1 \quad \mathcal{L}_2] \times \mathcal{Q} \tag{3.20}$$

where $\mathcal{L}_2 = \mathbb{B}_u$, $\mathcal{L}_1$ is a free $n \times (\alpha - 1)$ matrix, and $\mathcal{Q}$ is an $\alpha \times (\alpha + 1)p$ matrix that satisfies

$$\mathcal{Q}\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{(\alpha-1)\times 1} & O_{(\alpha-1)\times\alpha} \\ 1 & O_{1\times\alpha} \end{bmatrix} \tag{3.21}$$

Theorem 2. *A matrix $\mathcal{L}$ that satisfies (3.11) can be obtained using (3.20).*

□

Proof. A matrix $\mathcal{L}$ that satisfies (3.11) must (i) be located in the left null-space of the last α columns of $\mathcal{J}_{u,\alpha}$, and (ii) result in $\mathbb{B}_u$ if multiplied by the first column of $\mathcal{J}_{u,\alpha}$. To satisfy these conditions, $\mathcal{L}$ is considered as a multiplication of two matrices λ and $\mathcal{Q}$ as $\mathcal{L} = \lambda \times \mathcal{Q}$. The goal is to design a $\mathcal{Q}$ that satisfies (i), and a λ that satisfies (ii).

To design $\mathcal{Q}$, the last α columns of $\mathcal{J}_{u,\alpha}$ must be determined first. Using (3.15), the last α columns of $\mathcal{J}_{u,\alpha}$ are equal to $\begin{bmatrix} O_{\alpha\times p} & \mathcal{J}_{u,\alpha-1}{}^T \end{bmatrix}^T$. By choosing $\epsilon \in \mathbb{R}^{(\alpha p)\times(\alpha p)}$ as a matrix whose rows form a basis for the left null-space of $\mathcal{J}_{u,\alpha-1}$, $\begin{bmatrix} I_{p\times p} & O_{p\times\alpha p} \\ O_{\alpha p\times p} & \epsilon \end{bmatrix}$ becomes a matrix whose rows form a basis for the left null-space of $\begin{bmatrix} O_{\alpha\times p} & \mathcal{J}_{u,\alpha-1}{}^T \end{bmatrix}^T$, as shown in (3.22):

$$\begin{bmatrix} I_{p\times p} & O_{p\times\alpha p} \\ O_{\alpha p\times p} & \epsilon \end{bmatrix} \times \begin{bmatrix} O_{p\times 1} & O_{p\times\alpha} \\ \Theta_{\alpha-1}\mathbb{B}_u & \mathcal{J}_{u,\alpha-1} \end{bmatrix} = \begin{bmatrix} O_{p\times 1} & O_{p\times\alpha} \\ \epsilon\Theta_{\alpha-1}\mathbb{B}_u & O_{\alpha p\times\alpha} \end{bmatrix} \tag{3.22}$$

Multiplying $\begin{bmatrix} \Xi_1 & O_{(\alpha-1)\times\alpha p} \\ \Xi_2 & (\epsilon\Theta_{\alpha-1}\mathbb{B}_u)^+ \end{bmatrix}$ by both sides of (3.22), the following equation is ob-

tained:

$$\underbrace{\begin{bmatrix} \Xi_1 & O_{(\alpha-1)\times\alpha p} \\ \Xi_2 & (\epsilon\Theta_{\alpha-1}\mathbb{B}_u)^+ \end{bmatrix}\begin{bmatrix} I_{p\times p} & O_{p\times\alpha p} \\ O_{\alpha p\times p} & \epsilon \end{bmatrix}}_{\mathcal{Q}}\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{(\alpha-1)\times 1} & O_{(\alpha-1)\times\alpha} \\ 1 & O_{1\times\alpha} \end{bmatrix} \tag{3.23}$$

where "+" denotes the Pseudo inverse [83], and $\Xi_1 \in \mathbb{R}^{(\alpha-1)\times(p)}$ and $\Xi_2 \in \mathbb{R}^{1\times p}$ are free matrices. Therefore, choosing $\mathcal{Q}$ as in (3.23) and multiplying it by $\mathcal{J}_{u,\alpha}$ results in the right side of (3.23), and thus (3.21) is proved.

To satisfy condition (ii), λ is designed such that $\lambda\mathcal{Q}\mathcal{J}_{u,\alpha} = \begin{bmatrix} \mathbb{B}_u & O_{n\times 1} & \cdots & O_{n\times 1} \end{bmatrix}$. Breaking λ into two sub-matrices, $\mathcal{L}_1$ and $\mathcal{L}_2$, with $\alpha-1$ and 1 columns, respectively, yields

$$\lambda\mathcal{Q}\mathcal{J}_{u,\alpha} = \begin{bmatrix} \mathcal{L}_1 & \mathcal{L}_2 \end{bmatrix}\begin{bmatrix} O_{(\alpha-1)\times 1} & O_{(\alpha-1)\times\alpha} \\ 1 & O_{1\times\alpha} \end{bmatrix} \tag{3.24}$$

By equating (3.24) with $\begin{bmatrix} \mathbb{B}_u & O_{n\times 1} & \cdots & O_{n\times 1} \end{bmatrix}$, it is clear that $\mathcal{L}_2$ must equal $\mathbb{B}_u$. Additionally, as the first $\alpha-1$ rows of $\begin{bmatrix} O_{(\alpha-1)\times 1} & O_{(\alpha-1)\times\alpha} \\ 1 & O_{1\times\alpha} \end{bmatrix}$ are zero, $\mathcal{L}_1$ is an $n\times(\alpha-1)$ free matrix with no impact on the conditions of (3.11). Therefore, an $\mathcal{L}$ in the form of (3.20) can satisfy (3.11). ■

As shown by Theorem 2, by choosing $\mathcal{L}$ according to (3.20) and designing $\mathcal{Q}$ according to (3.21), equation (3.11) is satisfied for any $\mathcal{L}_1$, and the estimation error in (3.10) approaches zero as $k\to\infty$. As a result, $\mathcal{L}_1$ is a free $n\times(\alpha-1)$ matrix from the perspective of the UIO's error, and can be designed to make the UIO stable.

3.2.2 Stability of UIO

A UIO is stable when all the eigenvalues of $\mathbb{A}'$ in (3.10) are located in the unit circle in the complex plane [79]. In addition, the locations of the eigenvalues of $\mathbb{A}'$ affect the rate at which $e^s[k]$ approaches zero—or equivalently, the estimated states approach the actual ones. For instance, all entries of $e^s[k]$ approach zero at rates faster than σ^k, where σ is the

maximum magnitude of all eigenvalues of $\mathbb{A}'$. Therefore, even if a large error exists between $\mathbb{X}^s$ and $\hat{\mathbb{X}}^s$ when the UIO starts to operate, by selecting sufficiently small eigenvalues for $\mathbb{A}'$, the estimated states approach the actual states rapidly, and the estimation error remains zero thereafter [84].

As shown in Section 3.2.1, $\mathcal{L}_1$ is a free matrix from the UIO's error perspective. Therefore, it can be used for satisfying the stability condition. Substituting $\mathcal{L}$ from (3.20) into $\mathbb{A}'$ and breaking $\mathcal{QO}_\alpha$ into two sub-matrices $\mathcal{S}_1$ and $\mathcal{S}_2$, with $\alpha-1$ and 1 rows, respectively, result in

$$\mathbb{A}' = (\mathbb{A} - \mathbb{B}_u\mathcal{S}_2) - \mathcal{L}_1\mathcal{S}_1 \tag{3.25}$$

where $\mathcal{S}_1$ and $\mathcal{S}_2$ include the first $\alpha-1$ rows and the last row of $\mathcal{QO}_\alpha$, respectively. As shown in [85], there is an $\mathcal{L}_1$ that stabilizes the eigenvalues of (2.22) if

$$rank\begin{pmatrix} \mathbb{A} - zI_{n\times n} & \mathbb{B}_u \\ \mathbb{C} & O_{p\times 1} \end{pmatrix} = n+1, \quad \forall z \in \mathcal{C},\ |z| \geqslant 1 \tag{3.26}$$

in which $\mathcal{C}$ is the set of all complex numbers. Thus, if (3.26) is satisfied, $\mathcal{L}_1$ can be designed to stabilize the UIO's poles. The following theorem proves that (3.26) is satisfied for the state-space model of equation (3.5).

Theorem 3. *By selecting $\alpha = 2$, the condition given by (3.26) is satisfied for the state-space equation of a faulty transmission line, given in (3.5).* □

Proof. Condition (3.26) states that for any complex z whose magnitude is greater than or equal to 1, the rank of $\begin{bmatrix} \mathbb{A} - zI_{n\times n} & \mathbb{B}_u \\ \mathbb{C} & O_{p\times 1} \end{bmatrix}$ equals $n+1$. To find the rank of (3.26), this matrix can be written as the multiplication of three matrices, and its rank can be computed by finding the rank of the right-hand-side of the following equation:

$$\begin{bmatrix} \mathbb{A} - zI_{n\times n} & \mathbb{B}_u \\ \mathbb{C} & O_{p\times 1} \end{bmatrix} = \begin{bmatrix} I_{n\times n} & O_{n\times p} \\ \mathbb{C}(\mathbb{A} - zI_{n\times n})^{-1} & I_{p\times p} \end{bmatrix} \times$$

$$\begin{bmatrix} \mathbb{A} - zI_{n\times n} & O_{n\times 1} \\ O_{p\times n} & -\mathbb{C}(\mathbb{A} - zI_{n\times n})^{-1}\mathbb{B}_u \end{bmatrix} \times \begin{bmatrix} I_{n\times n} & (\mathbb{A} - zI_{n\times n})^{-1}\mathbb{B}_u \\ O_{1\times n} & 1 \end{bmatrix} \tag{3.27}$$

The first and the third matrices on the right-hand-side of the above equation are full-ranked, thus

$$rank\left(\begin{bmatrix} \mathbb{A}-zI_{n\times n} & \mathbb{B}_u \\ \mathbb{C} & O_{p\times 1} \end{bmatrix}\right) = rank\left(\begin{bmatrix} \mathbb{A}-zI_{n\times n} & O_{n\times 1} \\ O_{p\times n} & -\mathbb{C}(\mathbb{A}-zI_{n\times n})^{-1}\mathbb{B}_u \end{bmatrix}\right) \quad (3.28)$$

As a result,

$$\left(\begin{bmatrix} \mathbb{A}-zI_{n\times n} & \mathbb{B}_u \\ \mathbb{C} & O_{p\times 1} \end{bmatrix}\right) = rank\left(\mathbb{A}-zI_{n\times n}\right) + rank\left(\mathbb{C}(\mathbb{A}-zI_{n\times n})^{-1}\mathbb{B}_u\right) \quad (3.29)$$

To evaluate (3.29), the two ranks on the right-hand side of this equation must be found. To find the rank of $(\mathbb{A}-zI_{n\times n})$, Lemma 1 must be used.

Lemma 1. *For any $z \notin \sigma(\mathbb{A})$, where $\sigma(\mathbb{A})$ is the set of all eigenvalues of $\mathbb{A}$, the rank of $\mathbb{A}-zI_{n\times n}$ is equal to n [86].* □

For a stable state-space system, the eigenvalues of $\mathbb{A}$ are located inside the unit circle, and thus $|\lambda_j| < 1$ for $j \in \{1, 2, \cdots, n\}$. As a result, according to Lemma 1, the rank of $\mathbb{A}-zI_{n\times n}$ is equal to n for $|z| \geq 1$.

On the other hand, to find the rank of $\left(\mathbb{C}(\mathbb{A}-zI_{n\times n})^{-1}\mathbb{B}_u\right)$, the following lemma must be used.

Lemma 2. *Consider $\langle S\rangle$ as a state-space model represented by $\mathbb{A} \in R^{n\times n}$, $\mathbb{B}_u \in R^{n\times 1}$, and $\mathbb{C} \in R^{p\times n}$. This system has a transfer function $G(s) = \mathbb{C}\left(zI_{n\times n}-\mathbb{A}\right)^{-1}\mathbb{B}_u$ with rank 1 over the field of rational functions in z if and only if $\langle S\rangle$ is invertible, i.e., equation (3.12) holds [87].* □

As discussed in Section 3.2.1, condition (3.12) holds for a faulty transmission line by selecting $\alpha = 2$. Therefore, according to Lemma 2, the rank of $\mathbb{C}\left(zI_{n\times n}-\mathbb{A}\right)^{-1}\mathbb{B}_u$ is equal to 1 for $\alpha = 2$. As a result, (3.29) equals $n+1$, and (3.26) is satisfied. ■

As Theorem 3 proved, (3.26) is met for the system; thus there exists an $\mathcal{L}_1$ that stabilizes the system poles. Such an $\mathcal{L}_1$ can be designed using a pole-placement method, such as the algorithm proposed in [88]. This algorithm considers n desired stable eigenvalues and

designs $\mathcal{L}_1$ such that the eigenvalues of $\mathbb{A}'$ are equal to those eigenvalues. In this design, the algorithm assigns n linearly independent eigenvectors to the desired eigenvalues such that the eigenvector matrix is as well-conditioned as possible [89]. Then, $\mathcal{L}_1$ is obtained using these eigenvalues and eigenvectors. Once $\mathcal{L}_1$ is designed the UIO's gain expressed in (3.20) is fully designed and the system states can be estimated using (3.8).

In conclusion, a system is observable and its states can be estimated by a UIO, if conditions (3.12) and (3.26) are met. These conditions were both satisfied by the state-space model of a faulty lines shown in equation (3.5) and Fig. 3.1. As a results, UIOs can be used to estimate the states of a faulty line, and their development procedure is as follows [81]:

1. the UIO's delay is chosen as $\alpha = 2$.
2. The UIO's gain, i.e, $\mathcal{L}$, is developed as follows:
   (a) $\mathcal{Q}$ is obtained such that it satisfies (3.21).
   (b) $\mathcal{L}_2$ is equated with $\mathbb{B}_u$.
   (c) L_1 is designed using a pole-placement method such that it stabilizes the eigenvalues of (3.25).
   (d) $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{Q}$ are substituted in (3.20) to form $\mathcal{L}$.

After designing a UIO's gain, the states of the system in (3.5) at each time step can be estimated using (3.8) and system outputs. The estimated states of the system are used in the Section 3.3.2 to detect FDIAs and TSAs against LCDRs.

3.3 Attack Diagnosis Using UIO

Using the obtained state-space equation for faulty lines and the developed UIO, this section presents a method for detecting FDIAs and TSAs targeting LCDRs. To this aim, first the mismatch between the state-space models of a line during faults and attacks is shown in Section 3.3.1. Afterwards, the obtained mismatch is used in Section 3.3.2 to detect attacks and differentiate them from faults.

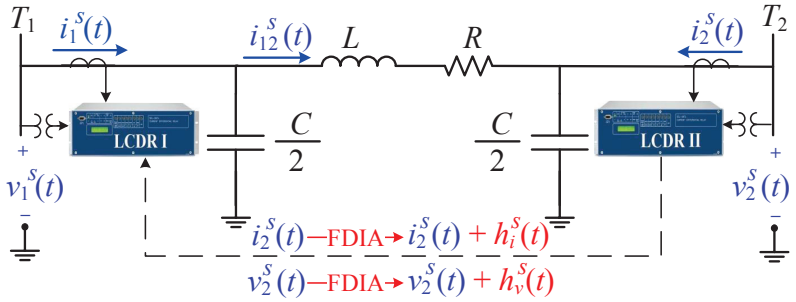


Figure 3.2: A two-terminal transmission line during FDIAs.

3.3.1 State-space Model of AC Lines During FDIAs and TSAs

This section proves that there exists a mismatch between a line's state-space model during faults, i.e., (3.5), and its model in the presence of attacks. During an FDIA or a TSA, the values or time stamps of remote measurements received by an LCDRs are manipulated. These manipulations are modeled by two inputs, i.e., h_v^s and h_i^s, which target remote voltage and current measurements, i.e., $v_2^s(t)$ and $i_2^s(t)$, respectively, and are shown in Fig. 3.2. Writing differential equations similar to (3.2) for the under-attack line in this figure and separating attack inputs $h_i^s(t)$ and $h_v^s(t)$ yield

$$\underbrace{\begin{bmatrix} \dot{v}_1^s(t) \\ \dot{i}_{12}^s(t) \\ \dot{v}_2^s(t) \end{bmatrix}}_{\dot{\overline{\mathbb{X}}}^s(t)} = \underbrace{\begin{bmatrix} 0 & \frac{-2}{C} & 0 \\ \frac{1}{L} & \frac{-R}{L} & \frac{-1}{L} \\ 0 & \frac{2}{C} & 0 \end{bmatrix}}_{\overline{\mathbb{A}}_c} \underbrace{\begin{bmatrix} v_1^s(t) \\ i_{12}^s(t) \\ v_2^s(t) \end{bmatrix}}_{\overline{\mathbb{X}}^s(t)} + \underbrace{\begin{bmatrix} \frac{2}{C} & 0 \\ 0 & 0 \\ 0 & \frac{2}{C} \end{bmatrix}}_{\overline{\mathbb{B}}_{c,n}} \underbrace{\begin{bmatrix} i_1^s(t) \\ i_2^s(t) \end{bmatrix}}_{\mathbb{U}_n^s(t)}$$

$$+ \underbrace{\begin{bmatrix} 0 & 0 & \frac{2}{C} \\ 0 & 0 & 0 \end{bmatrix}^T}_{\overline{\mathbb{B}}_{c,ca}} \underbrace{\begin{bmatrix} h_i^s(t) \\ h_v^s(t) \end{bmatrix}}_{\overline{\mathbb{U}}_{ca}^s(t)} \tag{3.30a}$$

$$\mathbb{Y}^s(t) = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_{\overline{\mathbb{C}}} \overline{\mathbb{X}}^s(t) + \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{\overline{\mathbb{D}}_{ca}} \overline{\mathbb{U}}^s_{ca}(t) \tag{3.30b}$$

To differentiate between the state-space model of the line under faults and attacks, the parameters of the state-space model under attacks are presented by an over-line in (3.30). As seen in (3.30b), manipulating remote voltage measurements modifies $v_2^s(t)$ to $h_v^s(t) + v_2^s(t)$. As a result, manipulating this parameter only affects $v_2^s(t)$ in $\mathbb{Y}^s(t)$, without influencing the states of the system. However, targeting the remote current measurements modifies $i_2^s(t)$ to $h_i^s(t) + i_2^s(t)$ in (3.30a), so the states are all affected.

For each sequence, discretizing (3.30) using (3.4)—by replacing $\overline{\mathbb{B}}_{c,ca}$ and $\overline{\mathbb{B}}_{c,n}$ with $\mathbb{B}_{c,n}$, and $\overline{\mathbb{A}}_c$ with $\mathbb{A}_c$—yields the discretized state-space model of the line during FDIAs or TSAs:

$$\overline{\mathbb{X}}^s[k+1] = \overline{\mathbb{A}}\,\overline{\mathbb{X}}^s[k] + \overline{\mathbb{B}}_n \mathbb{U}_n^s[k] + \overline{\mathbb{B}}_{ca}\overline{\mathbb{U}}^s_{ca}[k] \tag{3.31a}$$

$$\mathbb{Y}^s[k] = \overline{\mathbb{C}}\,\overline{\mathbb{X}}^s[k] + \overline{\mathbb{D}}_{ca}\overline{\mathbb{U}}^s_{ca}[k] \tag{3.31b}$$

where $\overline{\mathbb{A}}$, $\overline{\mathbb{B}}_n$, and $\overline{\mathbb{B}}_{ca}$ are the discretized versions of $\overline{\mathbb{A}}_c$, $\overline{\mathbb{B}}_{c,n}$ and $\overline{\mathbb{B}}_{c,ca}$ during attacks, and $\overline{\mathbb{U}}_{ca}[k]$ is the attack input at time step k. Apart from other differences, (3.22) contains two extra components than (3.5), i.e., $\overline{\mathbb{B}}_{ca}\overline{\mathbb{U}}^s_{ca}[k]$ and $\overline{\mathbb{D}}_{ca}\overline{\mathbb{U}}^s_{ca}[k]$, which are added due to FDIAs or TSAs. Therefore, the state-space equations of a line under faults and attacks differ. This differences enables discriminating between faults and attacks, as explained in the next subsection.

3.3.2 Attack Detection Scheme

As explained in Section 3.3.1, the state-space models of a line during attacks and faults differ. This difference is used in the proposed method to detect FDIAs or TSAs. To this aim, a submodule is created for each sequence in the proposed method, i.e., PS and NS submodules, each including a UIO designed based on the state-space model of the faulty line for that sequence. In the proposed method, when the LCDRs of a line pick up, instead of immediately tripping the line, they first determine the location of the fault (the obtained fault location is incorrect during FDIAs or TSAs, since there is no actual fault and only the

measurements are compromised). Then, the PS and NS submodules estimate the states of the system using their associated UIOs. Since during faults the line's actual model and the model used to design the UIO are the same, the UIOs' error for both sequences, i.e., $e^s[k]$, approach zero, as explained in Section 3.2. However, during attacks, these two models are no longer the same, generating a large estimation error, as explained in the following.

To obtain each submodule's estimation error during FDIAs or TSAs, i.e., $e^s\left[k+1\right] = \hat{\mathbb{X}}^s[k+1] - \mathbb{X}^s[k+1]$, $\hat{\mathbb{X}}^s[k+1]$ should be found using (3.8) during FDIAs or TSAs. In this equation, everything remains the same during FDIAs or TSAs, except for the system outputs, i.e., $\mathcal{Y}^s\left[k:k+\alpha\right]$, which should be obtained using under-attack state-space model of the system, given in (3.31). To modify $\mathcal{Y}^s\left[k:k+\alpha\right]$ for the attack condition, the system outputs given by (3.31b)—which include manipulated measurements—should be developed in a matrix form, from time step k to $k+\alpha$, as follows:

$$\overline{\mathcal{Y}}^s_{ca}\left[k:k+\alpha\right] = \overline{\mathcal{O}}_\alpha \overline{\mathbb{X}}^s\left[k\right] + \overline{\mathcal{J}}_{n,\alpha}\mathcal{U}^s_n\left[k:k+\alpha\right] + \overline{\mathcal{J}}_{ca,\alpha}\overline{\mathcal{U}}^s_{ca}\left[k:k+\alpha\right] \tag{3.32}$$

where $\overline{\mathcal{Y}}^s_{ca}\left[k:k+\alpha\right]$ is the output vector during FDIAs from time-step k to $k+\alpha$, and

$$\overline{\mathcal{O}}_\alpha = \begin{bmatrix} \overline{\mathbb{C}}^T & \left(\overline{\mathbb{C}}\ \overline{\mathbb{A}}\right)^T & \cdots & \left(\overline{\mathbb{C}}\ \overline{\mathbb{A}}^\alpha\right)^T \end{bmatrix}^T \tag{3.33a}$$

$$\overline{\mathcal{J}}_{n,\alpha} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \overline{\mathbb{C}}\ \overline{\mathbb{B}}_n & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \overline{\mathbb{C}}\ \overline{\mathbb{A}}^{\alpha-1}\overline{\mathbb{B}}_n & \overline{\mathbb{C}}\ \overline{\mathbb{A}}^{\alpha-2}\overline{\mathbb{B}}_n & \cdots & 0 \end{bmatrix} \tag{3.33b}$$

$$\overline{\mathcal{U}}^s_{ca}\left[k:k+\alpha\right] = \begin{bmatrix} \mathbb{U}^s_{ca}\left[k\right]^T & \mathbb{U}^s_{ca}\left[k+1\right]^T & \cdots & \mathbb{U}^s_{ca}\left[k+\alpha\right]^T \end{bmatrix}^T \tag{3.33c}$$

$$\overline{\mathcal{J}}_{ca,\alpha} = \begin{bmatrix} \overline{\mathbb{D}}_{ca} & 0 & 0 & \cdots & 0 \\ \overline{\mathbb{C}}\ \overline{\mathbb{B}}_u & \overline{\mathbb{D}}_{ca} & 0 & \cdots & 0 \\ \overline{\mathbb{C}}\ \overline{\mathbb{A}}\ \overline{\mathbb{B}}_u & \overline{\mathbb{C}}\ \overline{\mathbb{B}}_u & \overline{\mathbb{D}}_{ca} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \overline{\mathbb{C}}\ \overline{\mathbb{A}}^{(\alpha-1)}\overline{\mathbb{B}}_u & \overline{\mathbb{C}}\ \overline{\mathbb{A}}^{(\alpha-2)}\overline{\mathbb{B}}_u & \overline{\mathbb{C}}\ \overline{\mathbb{A}}^{(\alpha-3)}\overline{\mathbb{B}}_u & \cdots & \overline{\mathbb{D}}_{ca} \end{bmatrix} \tag{3.33d}$$

Thus, to find each submodule's estimation error during FDIAs or TSAs, $\mathcal{Y}^s[k:k+\alpha]$ in

(3.8) is substituted by $\overline{\mathcal{Y}}^s_{ca}[k:k+\alpha]$. Using (3.32) and (3.5a), the error for each submodule during FDIAs or TSAs becomes

$$e^s\left[k+1\right] = \overline{\mathbb{A}}e^s[k] + \mathcal{L}\overline{\mathcal{J}}_{ca,\alpha}\overline{\mathcal{U}}^s_{ca}\left[k:k+\alpha\right] + \mathcal{L}\overline{\mathcal{O}}_\alpha\overline{\mathbb{X}}^s[k]$$

$$- \mathcal{L}\mathcal{O}_\alpha\mathbb{X}^s[k] + \mathcal{L}\left[\overline{\mathcal{J}}_{n,\alpha} - \mathcal{J}_{n,\alpha}\right]\mathcal{U}^s_n\left[k:k+\alpha\right] \tag{3.34}$$

As seen in (3.34), the addition of new terms to the UIO's error during FDIAs and TSAs deviates it from zero, resulting in erroneous estimated states for both PS and NS submodules. The increased estimation error is utilized for detecting attacks by defining the following residual function for each submodule:

$$r^s\left[k\right] = \frac{v^s_1\left[k\right] - \hat{v}^s_1\left[k\right]}{\|v^s_1[k]\|} \tag{3.35}$$

where $\hat{v}^s_1\left[k\right]$ denotes the estimated local voltage. The reason for choosing such a residual function is that $v^s_1[k]$ is the only system state that is measured locally. Therefore, its estimated value can be compared with the measured one, which is reliable due to being local. As a result, in the absence of attacks, $e^s\left[k\right]$ approaches zero, resulting in $r^s[k] \to 0$. However, $r^s\left[k\right]$ grows during FDIAs due to the increased estimation error. Attacks can thus be detected by monitoring the residual function of each submodule and comparing it with a detection threshold. An FDIA or a TSA is thus in progress if

$$|r^s\left[k\right]| > tr^s \tag{3.36}$$

where $|.|$ denotes the absolute value, and tr^s is the detection threshold for sequence s. Detection thresholds should be found such that false-positive alarms during internal faults and false-negative alarms during attacks are minimized. The procedure used for obtaining the thresholds is explained in the next section.

To avoid false attack-detection during faults, the NS submodule must be deactivated during balanced conditions. To this aim, similar to what 67NEG element does, small NS currents can be detected by obtaining the ratio of current magnitudes for both sequences and comparing the result with a predetermined threshold. Hence, the NS submodule is deactivated if the following condition is satisfied for both terminals, using the remote and

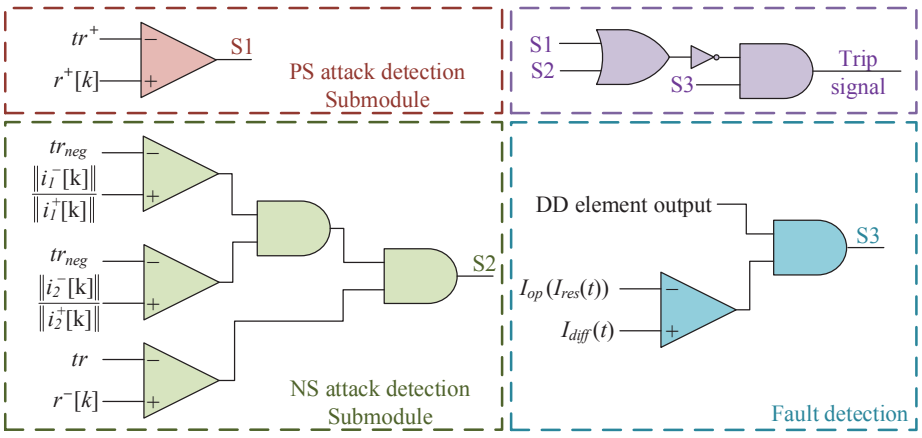


Figure 3.3: Tripping logic of LCDRs after implementing the proposed method.

local measurements:

$$\frac{\|i_n^-[k]\|}{\|i_n^+[k]\|} \leq tr_{neg} \quad n \in \{1,2\} \tag{3.37}$$

where tr_{neg} is the deactivation threshold for the NS submodule, and is set to 2% [90]. Fig. 3.3 shows LCDRs' tripping logic after implementing the proposed method.

3.4 Performance Evaluation

This section first determines the attack detection thresholds, i.e., tr^+ and tr^-, and then investigates the performance of the proposed attack-detection method. Simulations are carried out using PSCAD/EMTDC program on the 39-bus new England system of Fig. 2.2. In this test system, Line 6-11, with 100 km length, is protected by LCDRs—which are set based on the default settings of [1]. The proposed method is incorporated as a built-in function in the LCDR installed at Bus 11. Hence, for evaluating its performance, the remote measurements coming from Bus 6 are targeted.

3.5 Determining tr^+ and tr^-

To accurately detect attacks targeting Bus 11's remote measurements, and to avoid false-positive and false-negative alarms, tr^+ and tr^- must be determined for both submodules of the LCDR installed on Bus 11. Given that the proposed method is implemented in LCDRs, it starts operating only when an LCDR picks up. On the other hand, thanks to the considered restraint in the differential characteristic of LCDRs and their implemented state-of-the-art built-in functions, commercial LCDRs do not normally pick up during fault/non-fault external events, such as connection/disconnection of generators/DGs. In other words, the proposed method operates only during faults on Line 6-11, or during attacks targeting remote measurements of the LCDR at Bus 11. On this basis, tr^+ and tr^- are obtained during internal faults, in the presence of various possible sources of error and nonlinearities, including

- Measurement noise (Fig. 3.4): This noise is modeled as independent, white and Gaussian, with a signal-to-noise ratio (SNR) of 35 dB.
- Process noise: This noise is modeled as independent, white and Gaussian, with an SNR of 35 dB.
- CT saturation: three saturation levels are considered for the CTs installed at Buses 6 and 11: 1) Very Fast Saturation (VFS), which is defined to occur in less than 3 ms, 2) Fast Saturation (FS), which occurs before the fault current reaches its first extremum, and 3) Mild Saturation (MS), which occurs after the first extremum of the fault current [91]. Fig. 3.5 shows the primary and secondary currents of the CTs installed at Buses 6 and 11 during these three saturation levels.
- Coupling Capacitor Voltage Transformer (CCVT) transients: to consider the effect of CCVTs' transients, the equivalent model shown in Fig. 3.6 is utilized [92]. The CCVT model consists of two series capacitances $C_1 = 135$ mF and $C_2 = 292$ μF; a compensating inductor $L_{comp} = 42$ H, which controls the voltage lag in the capacitive divider; a step-down transformer with $L_t = 0.94$ mH, $R_t = 0.23$ Ω, and $N = 40$; a ferro-resonance filter to damp out ferro-resonance oscillations with parameters $L_{f1} =$

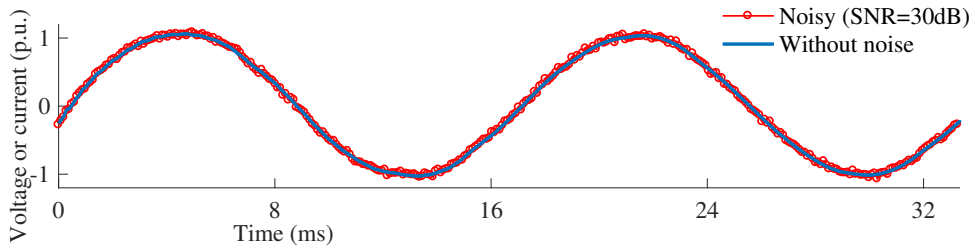


Figure 3.4: Added noise to voltage and current waveforms.

0.394 H, $R_{f1} = 3.9\ \Omega$, $L_{f2} = 0.01$ H, $R_{f2} = 5.5\ \Omega$, $C_{f2} = 8$ F, and $R_{f3} = 40\ \Omega$; and $R_{burden} = 52\ \text{k}\Omega$, which represents an LCDR's burden, and is set based on [66].

To determine tr^+ and tr^-, 500 case of internal faults—with various types, resistances and locations—were simulated in the presence of above-mentioned sources of error. For each case, the maximum $r^+[k]$ and $r^-[k]$ were recorded. The largest recorded r^+ and r^- plus a 10% security margin were assigned to tr^+ and tr^-. Afterwards, to verify the obtained thresholds, the above-mentioned procedure was repeated two more rounds, each for 500 cases of internal faults with random types, resistances and locations. If the obtained thresholds in the test rounds are more than the initial ones, tr^+ and tr^- are replaced by the largest recorded thresholds for each sequence. This procedure was continued until the test rounds verified the obtained thresholds.

In the above-mentioned procedure, the maximum obtained $r^+[k]$ was related to a three-phase ABC fault occurred at $x = 0.2$ with the resistance 0f 0.5 Ω. During this fault, saturation level for both local and remote CTs were VFS, Signal-to-Noise Ratio (SNR) was 30 dB, and parameters uncertainty was as described above. The estimated and measured local voltages during this fault are shown in Fig. 3.7a. Additionally, $r^+[k]$ is shown in Fig. 3.7b. As seen in Fig. 3.7, the maximum $r^+[k]$ is 9%. Thus, tr^+ was selected equal to 10%.

The maximum $r^-[k]$ was achieved during a two-phase AC fault, occurred at $x = 0.4$ with the resistance of 0.5 Ω. Similarly, saturation level for both local and remote CTs were VFS, SNR was 30 dB, and parameters uncertainty was as described above. The estimated and measured local voltages associated with NS during this fault are shown in Fig. 3.8a. Additionally, $r^-[k]$ is shown in Fig. 3.8b: the maximum $r^-[k]$ is 11.3%. Thus, tr^- was

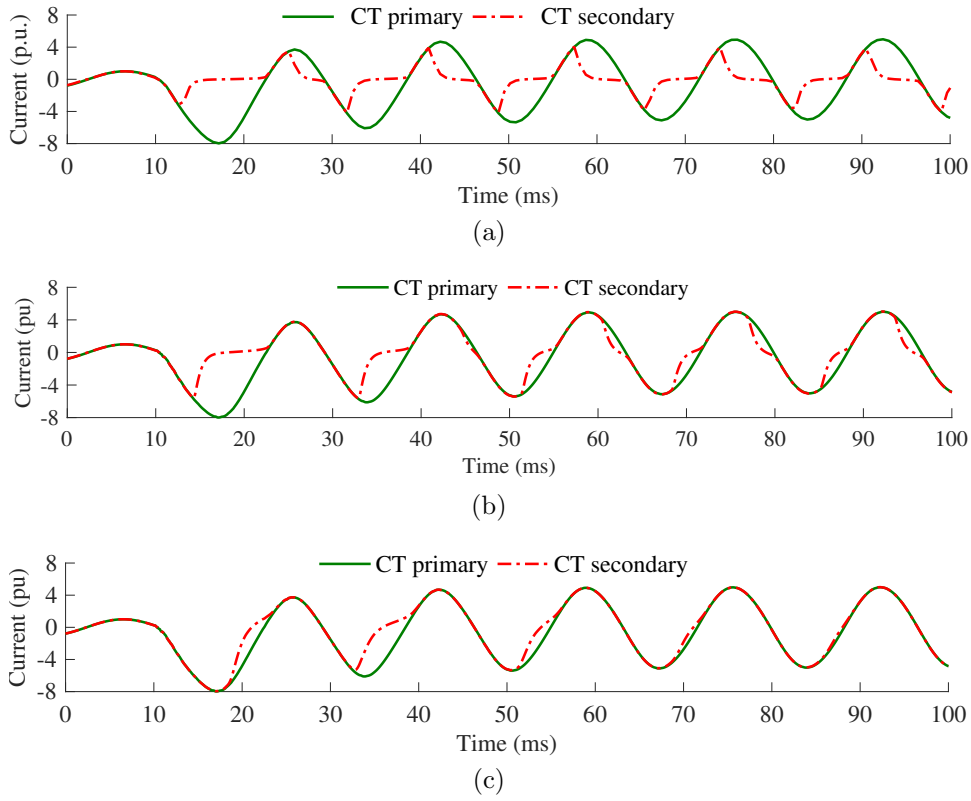


Figure 3.5: Primary and secondary currents of CTs installed at Buses 6 and 11 for different levels of saturation, (a) VFS, (b) FS, (C) MS.

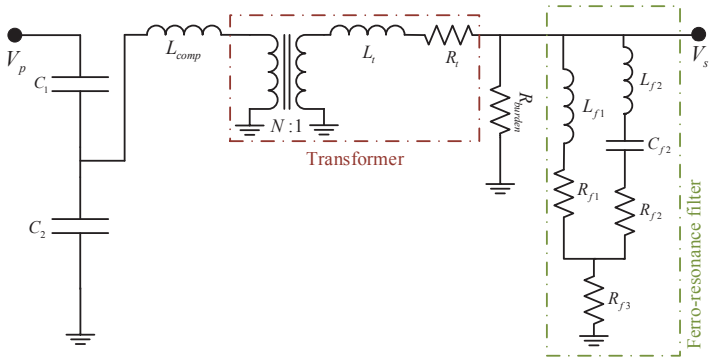


Figure 3.6: Equivalent model for utilized CCVTs.

selected equal to 12.4%.

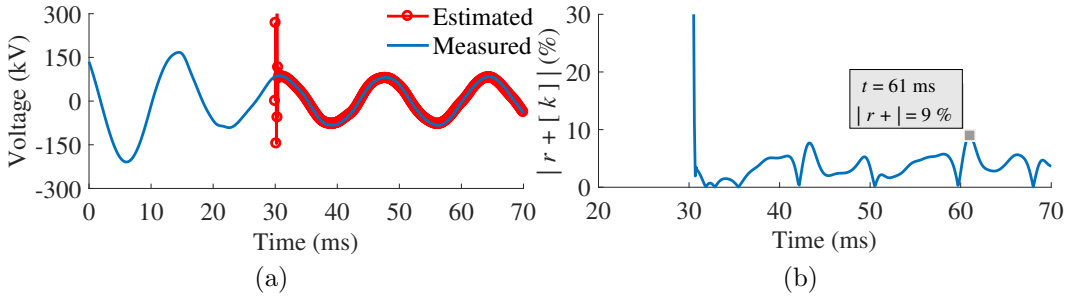


Figure 3.7: PS results for the case in which maximum $r^{+}[k]$ occurred, (a) Estimated and measured voltages for Bus 11, (b) RF.

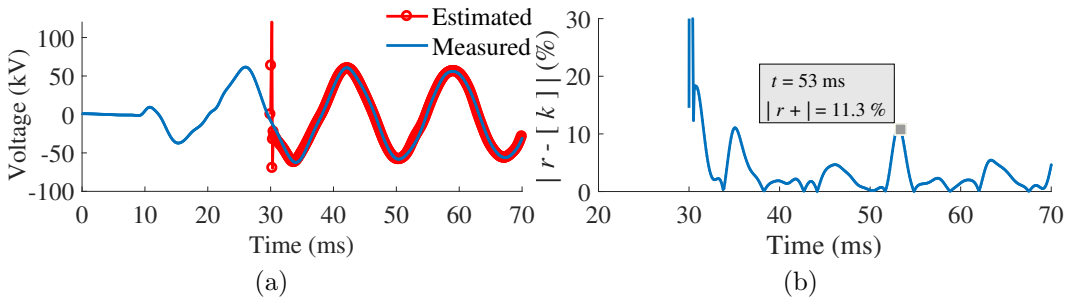


Figure 3.8: NS results for the case in which maximum $r^{-}[k]$ occurred, (a) Estimated and measured voltages for Bus 11, (b) RF.

3.6 Evaluation Scenarios

To evaluate the performance of the proposed method, this section presents seven scenarios: Scenarios 1 to 4 include 4 different internal faults, all happening at $t = 10$ ms on Line 6-11; Scenarios 5-7, on the other hand, include FDIAs against Bus 11's LCDR. All the FDIAs are initiated at $t = 10$ ms, after the DD element of the LCDR is already activated. Given that each LCDR detects attacks and differentiates them from faults independently, without being affected by other LCDRs' operation, only one LCDR is targeted in each scenario. Additionally, to be able to compare the performance of the proposed method during various fault/attack conditions, all presented scenarios focus on the same LCDR. Therefore, all the results are presented from the perspective of the LCDR installed at Bus 11.

- Scenario 1: This scenario evaluates the performance of the proposed method during

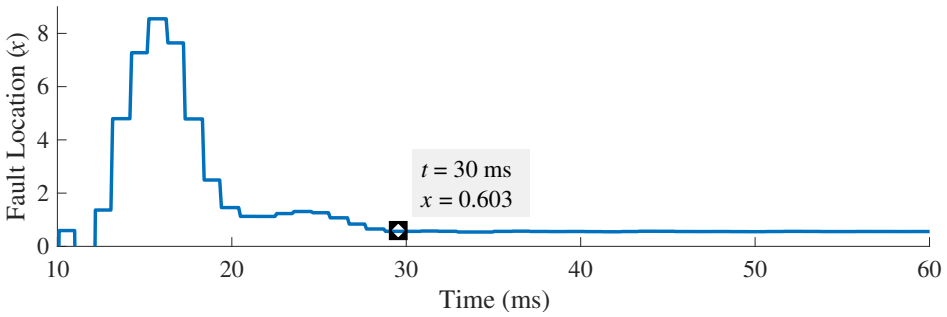


Figure 3.9: The location of the fault obtained by the utilized fault location technique.

a high-impedance AG fault occurring 60 km away from Bus 11 on Line 6-11. The fault resistance is 100 Ω. Once the fault happens, at $t = 10$ ms, the operating point of LCDRs protecting this line enters the trip zone, so they pick up. At this time, the utilized fault location technique calculates the fault location using remote and local measurements (Fig. 3.9). About 20 ms after the fault occurs, its location—defined as the distance between Bus 11 and the fault—is obtained with less than 1% error. Since this scenario presents an unsymmetrical fault, $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$ and $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\|$ become 1.94% and 2.54%, respectively, indicating that both the PS and NS submodules should operate. After obtaining x, UIOs of submodules estimate $v_{11}^{+}[k]$ and $v_{11}^{-}[k]$, and compare them with the measured ones to find the RFs. Fig. 3.10 illustrates the estimated and measured PS and NS voltages for Bus 11. For both sequences, $r^{s}[k]$ is relatively large at the beginning; however, in around 2 ms, $r^{+}[k]$ and $r^{-}[k]$ become less than 0.30% and 3.31%, respectively (Figs. 3.11). Since $r^{+}[k]$ and $r^{-}[k]$ remain less than tr^{+} and tr^{-} for $t \geq 32$ ms, respectively, the proposed method confirms that the pickup of the LCDR was due to a real internal fault, so the trip command is issued 25 ms after the inception of the fault.

• Scenario 2: To investigate the effect of fault resistance on UIOs' RF during high impedance faults, this scenario also simulates a high-impedance AG fault occurring 60 km away from Bus 11 on Line 6-11. Yet, in this scenario fault resistance is 200 Ω. In contrast to Scenario 1, in this scenario $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\| = 1.21\%$ and $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\| = 1.50\%$, both smaller than the defined deactivation threshold for NS. Thus, only the PS submodule operates in this scenario. Fig. 3.12a illustrates the estimated and measured PS voltages for Bus 11. Additionally, Fig. 3.12b shows the RF of PS submodule. Similar to Scenario

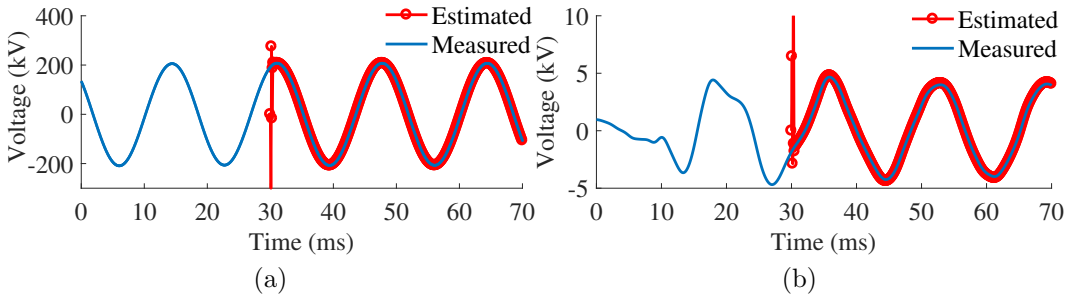


Figure 3.10: Estimated and measured voltages for Bus 11 in Scenario 1, (a) PS, (b) NS.

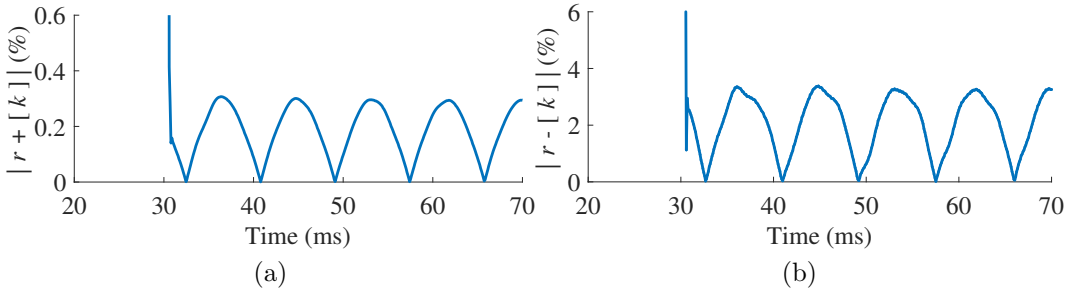


Figure 3.11: RFs of Scenario 1, (a) PS, (b) NS.

1, $r^{+}[k]$ in this scenario is less than tr^{+} for $t \geq 32$ ms, thus the proposed method confirms that the pickup of the LCDR was due to a real internal fault, and the line is tripped.

• Scenario 3: A low-impedance ABG fault with the resistance of 1 Ω happens 90 km away from Bus 11 on Line 6-11. Similar to the previous scenarios, the fault occurs at $t = 10$ ms, and its location is obtained at $t = 30$ ms. The values obtained for $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$ and $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\|$ in this scenario are 12.66% and 22.66%, respectively, indicating that both the PS and NS submodules should be active. The estimated and measured $v_{11}^{+}[k]$ and $v_{11}^{-}[k]$ are shown in Fig. 3.13, and the RFs of this scenario are illustrated in Fig. 3.14 for both sequences. As these figures represent, 2 ms after initiation of the state estimation, $r^{+}[k]$ and $r^{-}[k]$ become and remain less than 0.70% and 4.24%, respectively, both of these values being less than the defined detection thresholds. As a result, the proposed method truly confirms the occurrence of an internal fault, and the trip command is issued by the LCDR at $t = 35$ ms.

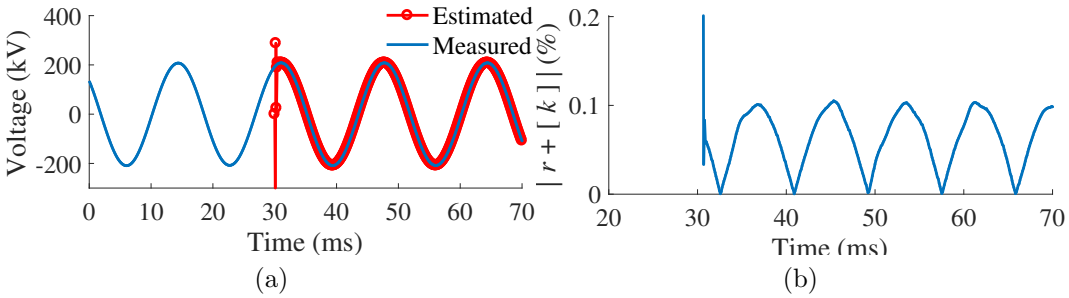


Figure 3.12: PS results obtained for Scenario 2, (a) Estimated and measured voltages for Bus 11, (b) RF.

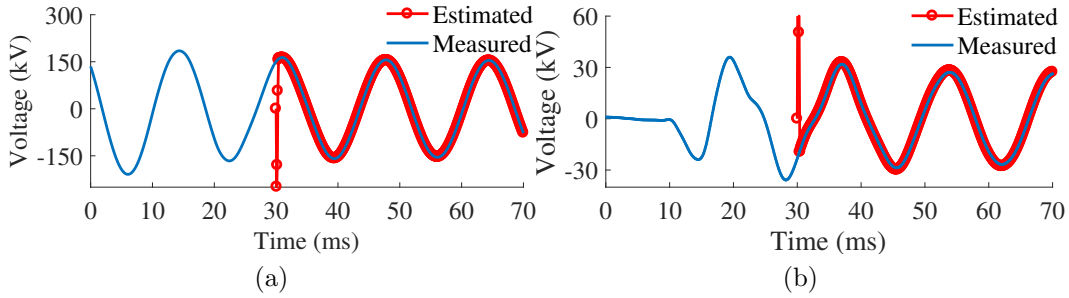


Figure 3.13: Estimated and measured voltages for Bus 11 in Scenario 3, (a) PS, (b) NS.

• Scenario 4: This scenario investigates the performance of the proposed method during a symmetrical ABC fault with the resistance of 1 Ω. This fault occurs 20 km away from Bus 11 on Line 6-11 at $t = 10$ ms. Since the fault is symmetrical, $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$ and $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\|$ are both close to zero, indicating that the NS submodule does not take part in attack-detection during this scenario. Hence, only PS submodule estimates the local voltage (Fig. 3.15a). The RF of the PS submodule is also shown in Fig. 3.15b: after $t = 32$ ms, the obtained RF becomes and remains less than 0.8%, which is smaller than tr^{+}. As a result, the proposed method indicates that the event in this scenario is an internal fault; the line is thus tripped.

• Scenario 5: This scenario investigates the performance of the proposed method during the FDIA targeted Line 6-11 in Case Study 2 of Section 2.6.2 in Chapter 2. In this attack, the healthy remote current measurements, i.e., $i_6[k]$, are multiplied by $\gamma = 1.96$, before they are received by the LCDR installed at Bus 11. Therefore, the LCDRs are fooled into

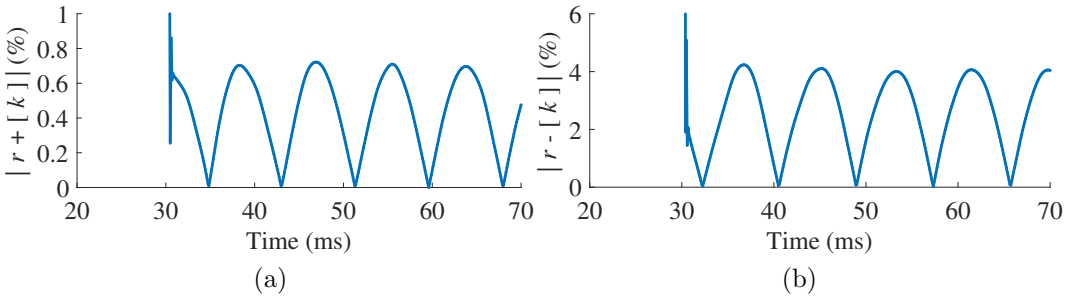


Figure 3.14: RFs of Scenario 3, (a) PS, (b) NS.

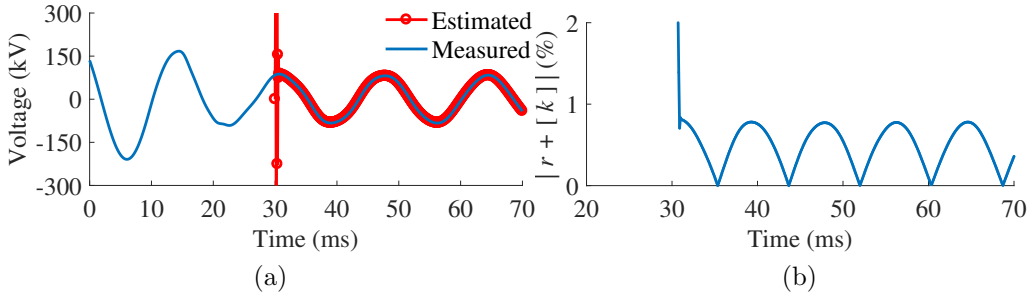


Figure 3.15: PS results obtained for Scenario 4, (a) Estimated and measured voltages for Bus 11, (b) RF.

an unwarranted pickup, as indicated in Case Study 2 of Section 2.6.2 in Chapter 2. At this time, the proposed method assumes that a fault has happened, so it runs the fault location technique to obtain its location. However, because only the remote measurements are manipulated and no real fault is in progress, the fault location technique yields an incorrect meaningless x. On the other hand, since in this scenario the remote current measurements during the normal condition are symmetrically multiplied by γ, $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$ and $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\|$ both remain around zero; thus, only the PS submodule functions. Fig. 3.16a shows the estimated and measured voltages at Bus 11: the wrong x and manipulated remote current measurements result in an erroneous local-voltage estimation; hence the RF of the PS increases (Fig. 3.16b). The RF in this scenario increases up to 24.45%, which is greater than tr^{+}. Consequently, the proposed method detects the attack, and the trip signal is blocked.

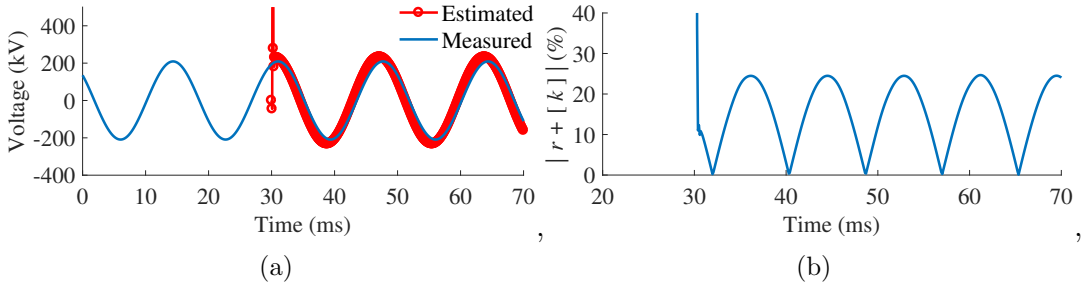


Figure 3.16: PS results obtained for Scenario 5, (a) Estimated and measured voltages for Bus 11, (b) RF.

• Scenario 6: This scenario targets the LCDR installed at Bus 11 by a replay attack—defined here as an FDIA in which a valid previously-recorded data transmission is maliciously repeated. In this scenario, the authentic remote measurements are replaced by ones pertaining to an internal BC fault, with a resistance of 10 Ω and at 70 km from Bus 11 on Line 6-11. The attacker starts manipulating the measurements at $t = 10$ ms, so the LCDR's operating point enters the trip zone and it picks up. The ratio of the NS and PS currents for Bus 11, i.e., $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$, remains around zero, because local measurements are related to a normal condition, which is balanced. Nonetheless, the remote measurements are pertinent to an unsymmetrical fault, resulting in $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\| = 2.28\%$. Thus, in this scenario, both submodules are active, and their results are shown in Fig. 3.17. The RFs of the PS and NS are illustrated in Fig. 3.18. As seen in these two figures, manipulating the remote measurements results in the increase of $r^{+}[k]$ and $r^{-}[k]$ up to 38.7% and 2000%, respectively, both values being greater than the determined thresholds. Therefore, the proposed method blocks the trip signal, and the line continues its normal operation.

• Scenario 7: In this scenario, another replay attack targets remote measurements of the LCDR installed at Bus 11. The replay attack in this scenario is pertinent to the high-impedance fault discussed in Scenario 1. When the attack is initiated at $t = 10$ ms, the authentic remote measurements are replaced by faulty measurements of Scenario 1. Thus, $\left\|i_{11}^{-}[k]\right\| / \left\|i_{11}^{+}[k]\right\|$ remains around zero, while $\left\|i_{6}^{-}[k]\right\| / \left\|i_{6}^{+}[k]\right\|$ changes from zero to 2.54% due to the attack, indicating that both submodules are active in this scenario. Fig. 3.19 illustrates the estimated and measured local voltages at Bus 11 obtained by the PS and NS submodules of the LCDR installed at this bus: there are significant errors, specifically

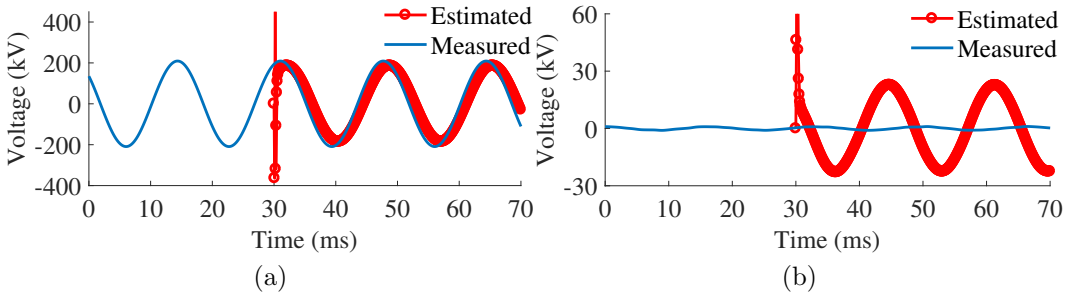


Figure 3.17: Estimated and measured voltages for Bus 11 in Scenario 6, (a) PS, (b) NS.

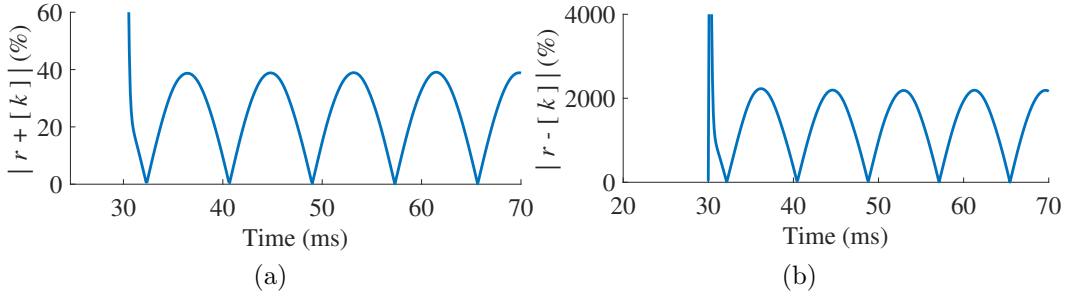


Figure 3.18: RFs of Scenario 6, (a) PS, (b) NS.

for the NS, between the measured and estimated voltages. These errors are shown in Fig. 3.20: the $r^{+}[k]$ for the PS grows up to 12.5%, while $r^{-}[k]$ increases up to 2090%. As a result, both $r^{+}[k]$ and $r^{-}[k]$ are greater than the defined thresholds, indicating an FDIA.

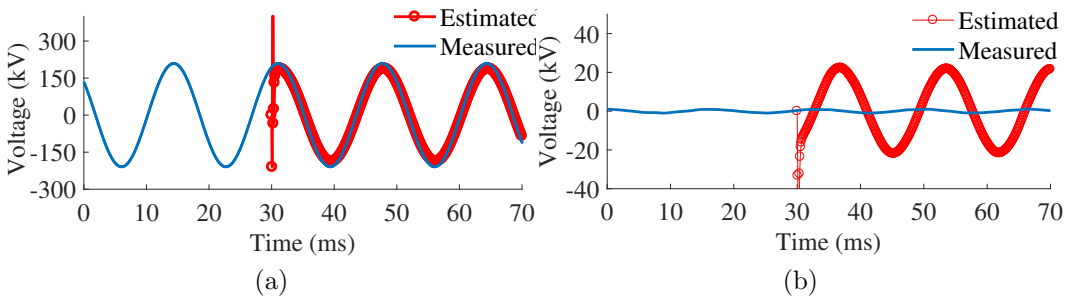


Figure 3.19: Estimated and measured voltages for Bus 11 in Scenario 7, (a) PS, (b) NS.

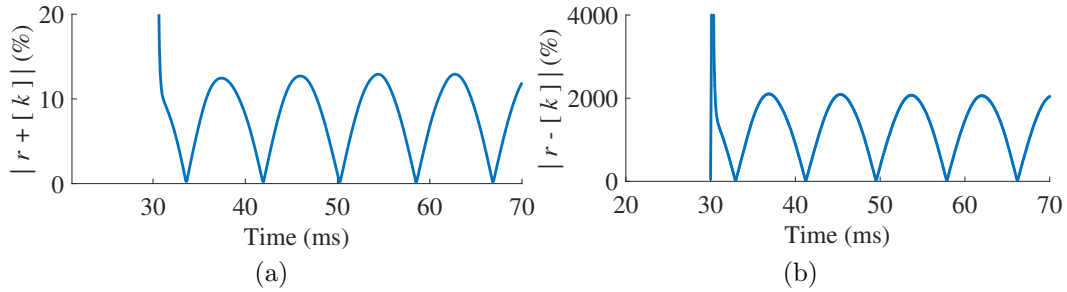


Figure 3.20: RFs of Scenario 7, (a) PS, (b) NS.

3.7 Conclusion

This chapter proposed an attack-detection method for AC LCDRs that are working based on SVs of remote measurements. To differentiate between faults and attacks, the proposed method is initiated immediately after the operating point of LCDRs enters the trip zone. This method uses the local and remote measurements, the state-space model of the faulty line, and UIOs to estimate the local voltage for both PS and NS. The RF of each sequence was then defined as the difference between the measured and estimated local voltages. The defined RFs for both sequences are small during internal faults, since in such situations the state-space model based on which the UIO operates and the actual system model are the same. Nevertheless, these two models differ during FDIAs, the RFs thus grow. As a result, a rise in the RF of any submodule over a predefined threshold along with the pickup signal of the LCDR indicate the occurrence of an attack. The proposed method was then tested on the 39-bus new England system for different fault and attack scenarios. The results of

scenarios corroborated the effectiveness of the proposed method in detecting attacks and differentiating them from faults.

Chapter 4

Attack Detection Method for SV-based and Phasor-based AC LCDRs

Chapter 3 presented an attack detection method for SV-based AC LCDRs. This chapter, however, proposes a technique for detecting FDIAs and TSAs against both SV-based and phasor-based AC LCDRs. This method works for two-terminal lines, and utilizes phasor values of local and remote current and local voltage measurements, i.e., the measurements available for an AC LCDR. Therefore, if it is implemented in SV-based type, the phasor values should be extracted from SVs. In this method, when an AC LCDR picks up, instead of immediately tripping the line, it calculates and measures the superimposed voltage at its local terminal, using the proposed PS and NS submodules. To calculate these voltages, the LCDR models the protected line in detail and replaces the rest of the system with a Thevenin equivalent that produces accurate responses at the line terminals. Afterwards, remote current measurements are utilized by the PS and NS submodules to compute each sequence's superimposed voltage. A difference between the calculated and the measured superimposed voltages in any sequence reveals that the remote current measurements are not authentic. This is because local measurements cannot be manipulated by cyber-attacks, thus any difference between the calculated and measured superimposed voltages in either sequences is due to the inauthenticity of remote current measurements. Hence, the LCDR's

trip command is blocked. The effectiveness of the proposed method is corroborated using simulation results for the 39-bus new England test system. The performance of the proposed method is also tested using an OPAL Real-Time Simulator (RTS).

On this basis, Section 4.1 illustrates the system model and explains the procedure used to obtain its parameters. Section 4.2 elaborates on calculating superimposed voltages at the local terminal of LCDRs, as well as the proposed attack diagnosis method. Afterwards, the performance of the proposed method is evaluated and its effectiveness is corroborated in Section 4.3. Finally, Section 4.4 concludes this chapter.

4.1 System Model

To detect attacks targeting a specific line in the grid, the line and the rest of the system should be modeled. To this end, the grid is divided into two main subsystems, i.e., the study and external. The study subsystem contains the line protected by AC LCDRs and so is modeled in detail, using the PI model, as shown in Fig. 4.1. In this figure, Z_c is the characteristic impedance, γ is the propagation constant, and l is the length of the transmission line in meters. On the other hand, the external subsystem contains the rest of the grid, and should be modeled to produce an accurate response at line terminals. According to the Thevenin theory, the external system seen at both 2 boundary terminals can be represented as a multi-terminal Thevenin circuit, including 2 equivalent voltage sources and 4 impedances—where 2 of them are mutual impedances between different terminals [93, 94]. Fig. 4.1 represents the External System Thevenin Equivalent (ESTE) used in this dissertation. In this model, the following equation holds:

$$\underbrace{\begin{bmatrix} E_{th1} \\ E_{th2} \end{bmatrix}}_{E_{th}} - \underbrace{\begin{bmatrix} Z_{1,1} & Z_{1,2} \\ Z_{2,1} & Z_{2,2} \end{bmatrix}}_{Z_{th}} \underbrace{\begin{bmatrix} I_1 \\ I_2 \end{bmatrix}}_{I_t} = \underbrace{\begin{bmatrix} V_1 \\ V_2 \end{bmatrix}}_{V_t} \tag{4.1}$$

in which, I_t and V_t are the voltage and current vectors for line terminals, and all other parameters are shown in Fig. 4.1. To fully model the system, the impedance and voltage source values in ESTE should be obtained. For passive networks consisting of linear, bilat-

eral, lumped or distributed elements, Open-Circuit Transfer Impedances (OTIs) between two terminals, e.g., $Z_{1,2}$ and $Z_{2,1}$, are equal. Thus, to model the external network in Fig. 4.1, three Thevenin impedances and two Thevenin voltage sources should be found.

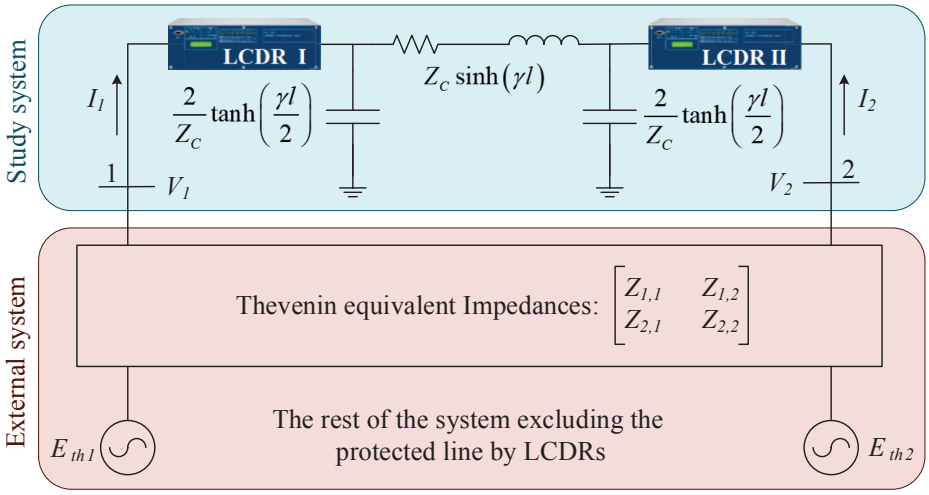
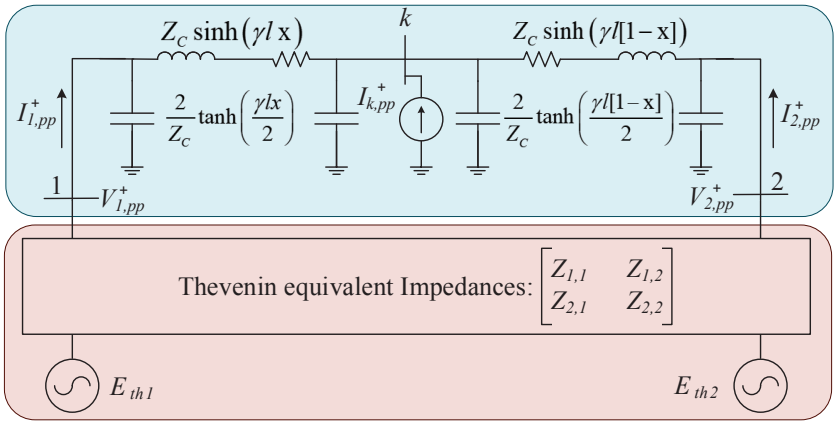


Figure 4.1: The equivalent model of the test system.

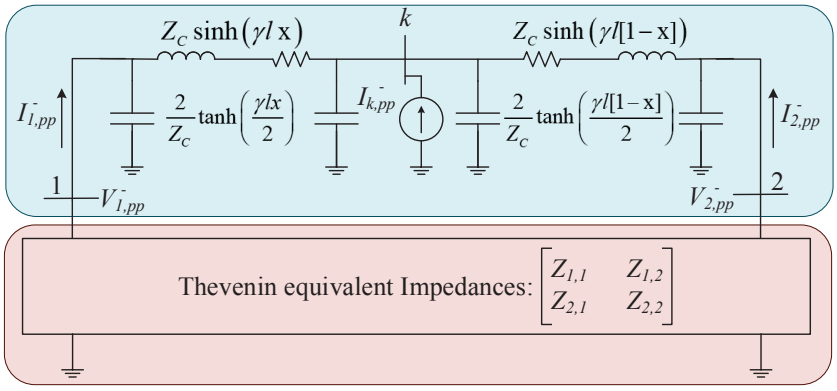
If an AC LCDR picks up (due to a fault or an attack), it can calculate ESTE parameters using the available voltage and current measurements before and after its pickup, as will be shown in the rest of this section.

• Before-pickup voltage equations: Since the Thevenin equivalent of large power systems do not change considerably during short periods of time (e.g., a few milliseconds), current and voltage samples taken before LCDRs pickup time can be used to estimate ESTE parameters [95, 96]. Meanwhile, no significant change in the configuration of the system must happen between these samples. Such changes can be detected by commercial LCDRs using the traveling waves generated after their occurrence [66]. Using the obtained samples, each LCDR finds the equations for before-pickup PS voltage at all terminals. For instance, for the α-th sample measured by LCDR I in Fig. 4.1, the following equations are obtained:

$$\begin{bmatrix} E_{th1} \\ E_{th2} \end{bmatrix} - \begin{bmatrix} Z_{1,1} & Z_{1,2} \\ Z_{2,1} & Z_{2,2} \end{bmatrix} \begin{bmatrix} I^{+}_{1,bp}[\alpha] \\ I^{+}_{2,bp}[\alpha] \end{bmatrix} = \begin{bmatrix} V^{+}_{1,bp}[\alpha] \\ V^{+}_{2,bp}[\alpha] \end{bmatrix} \tag{4.2}$$



(a)



(b)

Figure 4.2: Model of the test system during internal faults (a) PS, (b) NS.

in which, subscripts *bp* and superscript "+" denote the quantities measured before pickup and PS values, respectively. In these equation, parameters $I^+_{1,bp}[\alpha]$, $I^+_{2,bp}[\alpha]$, and $V^+_{1,bp}[\alpha]$ are available. However, $V^+_{2,bp}[\alpha]$ must be found using $I^+_{1,bp}[\alpha]$, $V^+_{1,bp}[\alpha]$ and the following equation:

$$V^+_{2,bp}[\alpha] = V^+_{1,bp}[\alpha] - \left(I^+_{1,bp}[\alpha] - \frac{2V^+_{1,bp}[\alpha]\tanh\left(\frac{\gamma l}{2}\right)}{Z_C} \right) Z_C Sinh\left(\gamma l\right) \tag{4.3}$$

A higher number of samples yield more accurate results.

• Post-pickup voltage equations: Since in attack-free conditions LCDRs must pickup only when internal faults occur, post-pickup conditions are modeled in the presence of an internal fault. Fig. 4.2 presents the PS and NS models of the system during a fault. In these models, the PS and NS impedances are similar [97], and the fault is represented by a current source located xl meters away from terminal 1 [76]. Short-circuit studies commonly assume that variations in large systems in the short term (a few cycles) are not expected to cause a significant change in the parameters of the ESTE. As a result, the ESTE before and during an internal fault are considered to be the same [98], and during-fault equations can also be used for finding the ESTE parameters. Hence, another equation can be written for the PS voltage at LCDR locations. For example, for LCDR I in Fig. 4.2a, the following equation holds:

$$V^{+}_{1,pp} = E_{th1} - Z_{11} I^{+}_{1,pp} - Z_{12} I^{+}_{2,pp} \tag{4.4}$$

in which, subscript pp denotes post-pickup values, and $V^{+}_{1,pp}$, $I^{+}_{1,pp}$, and $I^{+}_{2,pp}$ are available through measurement. In cases of non-zero NS fault current, another equation can be written for the post-pickup NS local voltage measured by LCDRs. This equation for LCDR I is

$$V^{-}_{1,pp} = -Z_{11} I^{-}_{1,pp} - Z_{12} I^{-}_{2,pp} \tag{4.5}$$

where, superscript "−" denotes NS values.

Once before-pickup and post-pickup equations (4.2), (4.4), and (4.5) are found, they can be written in the following matrix form:

$$\begin{bmatrix}
1 & 0 & -I^{+}_{1,bp}[1] & -I^{+}_{2,bp}[1] & 0 \\
1 & 0 & -I^{+}_{1,bp}[2] & -I^{+}_{2,bp}[2] & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
1 & 0 & -I^{+}_{1,bp}[m] & -I^{+}_{2,bp}[m] & 0 \\
\hline
0 & 1 & 0 & -I^{+}_{1,bp}[1] & -I^{+}_{2,bp}[1] \\
0 & 1 & 0 & -I^{+}_{1,bp}[2] & -I^{+}_{2,bp}[2] \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 1 & 0 & -I^{+}_{1,bp}[m] & -I^{+}_{2,bp}[m] \\
\hline
1 & 0 & -I^{+}_{1,pp} & -I^{+}_{2,pp} & 0 \\
0 & 0 & -I^{-}_{1,pp} & -I^{-}_{2,pp} & 0
\end{bmatrix}
\underbrace{\begin{bmatrix} E_{th1} \\ E_{th2} \\ Z_{11} \\ Z_{12} \\ Z_{22} \end{bmatrix}}_{X}
=
\begin{bmatrix}
V^{+}_{1,bp}[1] \\ V^{+}_{1,bp}[2] \\ \vdots \\ V^{+}_{1,bp}[m] \\
\hline
V^{+}_{2,bp}[1] \\ V^{+}_{2,bp}[2] \\ \vdots \\ V^{+}_{2,bp}[m] \\
\hline
V^{+}_{1,pp} \\ V^{-}_{1,pp}
\end{bmatrix} \tag{4.6}$$

in which, X is the unknown vector that should be obtained. The set of equations in (4.6) can be solved using the Least Square Method (LSM) [99]. Once vector X in (4.6) is obtained, the external subsystem model is fully identified, and can be used for differentiating between faults and attacks.

4.2 Proposed Attack Detection Method

This section first explains how to obtain the OTI between an LCDR's terminals and a fault location. After estimating the fault current, Section 4.2.2 elaborates on computing the superimposed voltage at the LCDR's terminal using the obtained OTI and the fault current. Finally, Section 4.2.3 explains the proposed method utilizes the calculated superimposed voltages to detect FDIAs and TSAs.

4.2.1 OTI between LCDR's terminals and fault location

To find the local superimposed voltage, an LCDR must find the OTI between its terminal and the fault location (i.e., virtual bus k in Fig. 4.2) after the LCDR picks up. To find a fault location, the technique suggested in [77] for LCDRs is used. This fault location technique utilizes only the measurements available for LCDRs, and does not require any extra input. The OTI between buses i and k is the element at row i and column k of the system impedance matrix [100]. This impedance can be calculated using the fault location and the before-pickup impedance matrix. To find this impedance matrix, the equation that relates currents and voltages of the line's terminals should be determined first. Given that the current flowing into line terminals from the external subsystem is I_t and the terminal's voltage is V_t—as explained in (4.1)—I_t can be described by

$$I_t = Y_L V_t \tag{4.7}$$

where, Y_L is the admittance matrix of the line, when separated from the rest of grid. On the other hand, multiplying Z_{th}^{-1} in both sides of (4.1) results in

$$I_t = Z_{th}^{-1} E - Z_{th}^{-1} V_t \tag{4.8}$$

Equating (4.7) and (4.8) yields

$$Y_L V_t = Z_{th}^{-1} E - Z_{th}^{-1} V_t \tag{4.9}$$

Rearranging and simplifying (4.9) results in

$$I_{inj} = \underbrace{\left(Z_{th}^{-1} + Y_L\right)}_{Y_{bus,bp}} V_t \tag{4.10}$$

in which, I_{inj}= $Z_{th}^{-1} E$, and is the injected current to terminal buses. Using the obtained impedance matrix for the equivalent system, the system impedance matrix is obtained using

$$Z_{bus,bp} = \left(Z_{th}^{-1} + Y_L\right)^{-1} \tag{4.11}$$

In the next step, post-pickup impedance and admittance matrices—i.e., $Z_{bus,pp}$ and $Y_{bus,pp}$, respectively—should be found using $Z_{bus,bp}$ and $Y_{bus,bp}$. Since impedance (admittance) matrix is the same for both the PS and NS [97], the following equation holds for both sequences

$$Z_{bus,pp} \times Y_{bus,pp} = I_{3\times 3} \tag{4.12}$$

where,

$$Z_{bus,pp} = \begin{bmatrix} Z_{1,1,pp} & Z_{1,2,pp} & Z_{1,k,pp} \\ Z_{2,1,pp} & Z_{2,2,pp} & Z_{2,k,pp} \\ Z_{k,1,pp} & Z_{k,2,pp} & Z_{k,k,pp} \end{bmatrix} \tag{4.13}$$

$$Y_{bus,pp} = \begin{bmatrix} Y_{1,1,pp} & Y_{1,2,pp} & Y_{1,k,pp} \\ Y_{2,1,pp} & Y_{2,2,pp} & Y_{2,k,pp} \\ Y_{k,1,pp} & Y_{k,2,pp} & Y_{k,k,pp} \end{bmatrix} \tag{4.14}$$

and k denotes the fault virtual bus. The OTI between terminal n and bus k is found by multiplying row n of $Z_{bus,pp}$ by column k of $Y_{bus,pp}$ in (4.12), resulting in

$$Z_{n,1,pp} Y_{1,k,pp} + Z_{n,2,pp} Y_{2,k,pp} + Z_{n,k,pp} Y_{k,k,pp} = 0 \tag{4.15}$$

Since the addition of bus k does not change $Z_{n,1}$ and $Z_{n,2}$ elements in $Z_{bus,bp}$ [76], the OTI between terminal n and fault virtual bus k can be obtained by

$$Z_{n,k,pp} = \frac{-\left(Z_{n,1,bp}Y_{1,k,bp} + Z_{n,2,bp}Y_{2,k,bp}\right)}{Y_{k,k,pp}} \tag{4.16}$$

For example, to obtain the OTI between terminal 1 and fault bus k in Fig. 4.2, $Y_{1,k,pp}$, $Y_{2,k,pp}$, and $Y_{k,k,pp}$ can be computed using

$$Y_{1,k} = -\frac{1}{Z_C \sinh\left(\gamma l x\right)} \tag{4.17}$$

$$Y_{2,k} = -\frac{1}{Z_C \sinh\left(\gamma l \left[1-x\right]\right)} \tag{4.18}$$

$$\begin{aligned} Y_{k,k} = \frac{1}{Z_C \sinh\left(\gamma l x\right)} + \frac{1}{Z_C}\tanh\left(\frac{\gamma l x}{2}\right) + \frac{1}{Z_C \sinh\left(\gamma l \left[1-x\right]\right)} \\ + \frac{1}{Z_C}\tanh\left(\frac{\gamma l \left[1-x\right]}{2}\right) \end{aligned} \tag{4.19}$$

Therefore, using (4.17) to (4.19), $Z_{1,k,pp}$ is obtained by [76]

$$Z_{1,k,pp} = \frac{\frac{Z_{1,1,bp}}{\sinh(\gamma l x)} + \frac{Z_{1,2,bp}}{\sinh(\gamma l[1-x])}}{\frac{1}{\sinh(\gamma l x)} + \frac{1}{\sinh(\gamma l[1-x])} + \tanh\left(\frac{\gamma l x}{2}\right) + \tanh\left(\frac{\gamma l[1-x]}{2}\right)} \tag{4.20}$$

Similarly, $Z_{2,k,pp}$ can be obtained by

$$Z_{2,k,pp} = \frac{\frac{Z_{2,2,bp}}{\sinh(\gamma l x)} + \frac{Z_{1,2,bp}}{\sinh(\gamma l[1-x])}}{\frac{1}{\sinh(\gamma l x)} + \frac{1}{\sinh(\gamma l[1-x])} + \tanh\left(\frac{\gamma l x}{2}\right) + \tanh\left(\frac{\gamma l[1-x]}{2}\right)} \tag{4.21}$$

4.2.2 Calculating Local Superimposed Voltage

When an internal fault happens, the voltage at all terminals of the line are affected. The PS and NS superimposed voltage at terminal n can be calculated using

$$\Delta V^{s}_{n,c} = -Z_{n,k,pp} \times I^{s}_{k,pp} \quad n \in \{1,2\} \ , \ s \in \{+,-\} \tag{4.22}$$

where, $I^s_{k,pp}$ is the s-sequence fault current phasor, shown in Fig. 4.2 [101]. This current can be found using LCDR current measurements, fault location, and the relations describing the fault circuit, as shown in the following equation:

$$I^s_{k,pp} = I^s_{1,pp} + I^s_{2,pp} - \frac{V^s_{2,pp}}{Z_C}\tanh\left(\frac{\gamma l\,[1-x]}{2}\right) - \frac{V^s_{1,pp}}{Z_C}\tanh(\frac{\gamma l x}{2})$$
$$-\frac{V^s_{k,pp}}{Z_C}\left(\tanh\left(\frac{\gamma l x}{2}\right) + \tanh\left(\frac{\gamma l\,[1-x]}{2}\right)\right) \tag{4.23}$$

where

$$V^s_{k,pp} = V^s_{1,pp} - \left(I^s_{1,pp} - \frac{V^s_{1,pp} \times \tanh\left(\frac{\gamma l x}{2}\right)}{Z_C}\right) Z_C \sinh\left(\gamma l x\right) \tag{4.24}$$

$$V^s_{2,pp} = \frac{V^s_{k,pp} + Z_C \sinh\left(\gamma l\,[1-x]\right) \times I^s_{2,pp}}{1 + \tanh\left(\frac{\gamma l[1-x]}{2}\right) \times \sinh\left(\gamma l\,[1-x]\right)} \tag{4.25}$$

The PS and NS submodules of LCDRs I and II thus calculate the PS and the NS superimposed voltages at their terminals using (4.20)-(4.25).

4.2.3 Detecting Attacks

As explained in Section 4.2.1 and 4.2.2, remote current measurements were used in calculating the PS and NS superimposed voltages, i.e., $\Delta V^s_{n,c}$. As a result, in case of an FDIA or a TSA against remote current measurements, $\Delta V^s_{n,c}$ in (4.22) differ from their values obtained by local measurement. These differences are used for detecting FDIAs, i.e., an FDIA happens if

$$\underbrace{\frac{\left|\Delta V^s_{n,c} - \Delta V^s_{n,m}\right|}{\left|\Delta V^s_{n,m}\right|}}_{\delta^s_n} \times 100 \geq tr^s_n \quad n \in \{1,2\} \quad s = \{+ \text{ or } -\} \tag{4.26}$$

in which, $\Delta V^s_{n,m}$ is the superimposed voltage measured by the LCDR locally, δ^s_n is the difference between the measures and calculated superimposed voltages at terminal n in percent, and tr^s_n is the detection threshold, all for sequence s. The setting process for tr^s_n

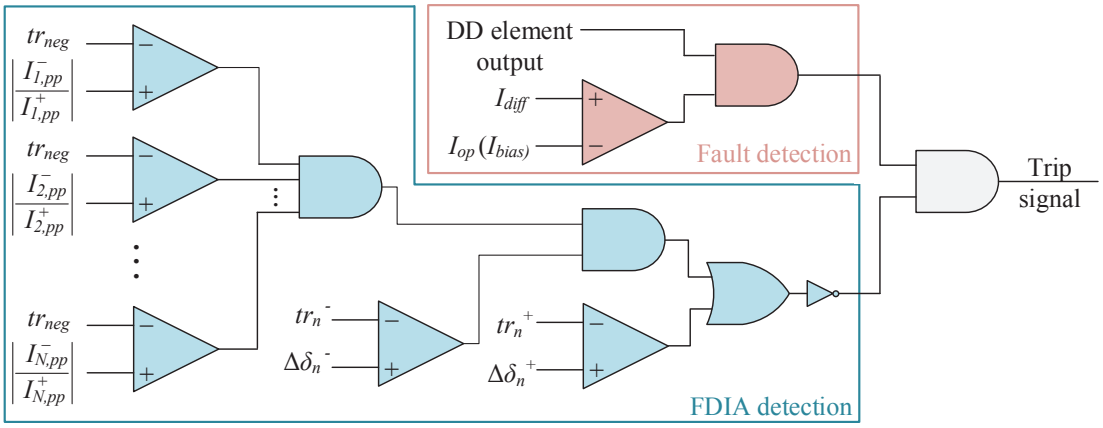


Figure 4.3: Tripping logic of LCDRs after implementing the proposed method.

will be discussed in Section 4.3.1. Since δ_n^s in (4.26) must ideally be zero during attack-free conditions for both PS and NS, exceeding δ_n^s from tr_n^s for either sequence implies an FDIA or a TSA. However, for the reliable function of the proposed method under unbalanced conditions, the NS submodule can be deactivated if the ratio of the NS current over the PS current falls bellow a certain threshold, similar to what 67NEG element carries out in case of small NS currents [90]. As a result, in the proposed method, the NS submodule is deactivated if the following condition is met for all local and remote measurements

$$\left|\frac{I^-_{n,pp}}{I^+_{n,pp}}\right| \leq tr_{neg} \quad n \in \{1,2\} \tag{4.27}$$

where tr_{neg} is the NS deactivation threshold, and is set to 2% [90]. Such a formulation deactivates the NS when a real symmetrical internal fault happens, as will be shown in Section 4.3.1. The tripping logic of LCDRs after implementing the proposed method is illustrated in Fig. 4.3. Additionally, Fig. 4.4 is the flowchart of the procedure carried out by each LCDR after its pickup to detect attacks and differentiate them from faults.

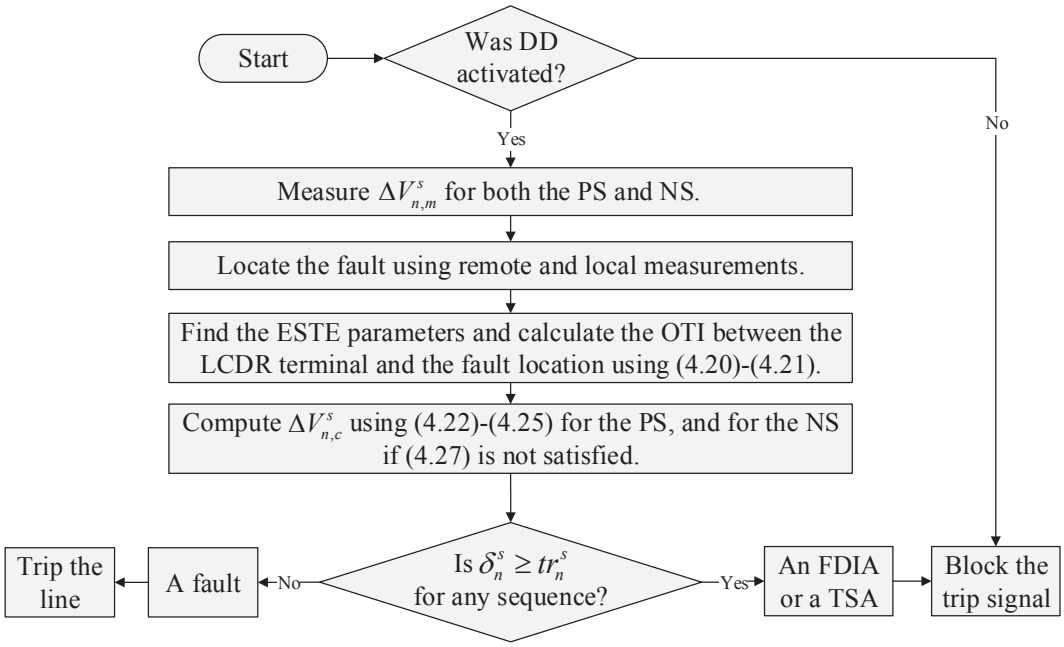


Figure 4.4: Flowchart of the proposed method

4.3 Performance Evaluation

4.3.1 Off-line Simulations

This section investigates the performance of the proposed method for LCDR I in the test system shown in Fig 2.2 using PSCAD/EMTDC program. LCDRs I and II in the test system have been installed at terminals 1 and 2 of Line 6-11 (or on buses 11 and 6, respectively). To differentiate between attacks and faults, the detection thresholds tr_1^+ and tr_1^- must be determined for both PS and NS submodules, so that false diagnosis during fault and attack conditions is avoided. To this aim, tr_1^s was obtained in the presence of different sources of error, e.g., measurement noise, CT saturation, and line-parameter uncertainty during internal faults. The measurements used by LCDR I were combined with white Gaussian noise with a signal-to-noise ratio (SNR) of 30 dB. The CTs were sized

based on the specifications in [102]. Parameter uncertainty was modeled, using a Gaussian percentage error that is normally distributed around zero, with a standard deviation of 2%. About 200 simulations of internal faults with different types, resistances and locations were run. For each, δ_1^s was derived. The maximum recorded δ_1^s plus a security margin of 10% were assigned to tr_1^s. Afterwards, to verify the obtained thresholds, the above-mentioned procedure was repeated two more rounds, each for other 200 cased of internal faults with random types, resistances and locations. If the obtained thresholds in the test rounds are greater than the initial ones, tr_1^+ and tr_1^- are replaced by the largest recorded thresholds for each sequence. This procedure was continued until the test rounds verified the obtained thresholds, and resulted in tr_1^+ and tr_1^- equal to 11% and 9%, respectively.

This section defines seven scenarios to evaluate the performance of the proposed method: Scenarios 1 to 3 include 3 different internal faults; Scenarios 4 and 5 include the basic FDIAs studied in Section 2.3; and Scenarios 6 and 7 involve two replay attacks. All faults or FDIAs start at $t = 50$ ms on/against Line 6-11. Attacks are initiated after the DD element of Bus 11's LCDR picks up. All the results are presented from the perspective of this LCDR. In these scenarios, line terminals connected to Buses 11 and 6 are called Terminals 1 and 2, respectively.

• Scenario 1: This scenario includes a high-impedance internal AG fault 30 km away from Bus 11 on Line 6-11, with a fault resistance of 300 Ω. Immediately after the fault happens, the operating points of LCDRs I and II enter the trip zone, and the proposed method is initiated. The results for the PS are illustrated in Fig. 4.5a: at $t = 75$ ms—i.e., 1.5 cycles after the fault occurs—$\Delta V_{1,c}^+$ and $\Delta V_{1,m}^+$ are 1.56 and 1.44 kV, respectively, resulting in $\delta_1^+ = 8.33\%$. The non-zero value of δ_1^+ is due to the above-discussed sources of error. On the other hand, $\left|I_{n,pp}^-/I_{n,pp}^+\right|$ for terminals 1 and 2 are 76% and 186%, which are both greater than 2%. As a result, the NS submodule of the proposed method should be active. For the NS, $\Delta V_{1,c}^- = 1.53$ kV, $\Delta V_{1,m}^- = 1.45$ kV, and thus $\delta_1^- = 5.5\%$, as shown in Fig. 4.5b. The below-threshold δ_1^+ and δ_1^- confirm that the occurred event is an internal fault.

• Scenario 2: An AB fault with a fault resistance of 1 Ω happens 75 km away from Bus 11 on Line 6-11. As shown in Fig. 4.6a, at $t = 75$ ms, $\Delta V_{1,c}^+$ and $\Delta V_{1,m}^+$ are 30.46 and 27.86 kV, respectively, which result in $\delta_1^+ = 9.33\%$. On the other hand, $I_{n,pp}^-/I_{n,pp}^+$ for terminals

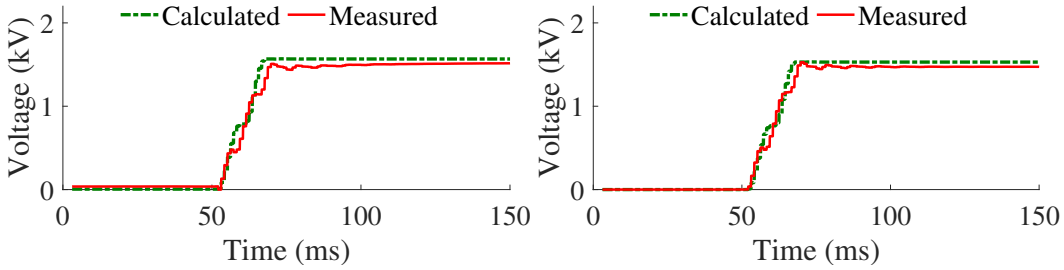


Figure 4.5: Superimposed voltages at bus 11 during Scenario 1, (a) PS, (b) NS.

1 and 2 are 67% and 46%. As a result, the NS submodule is active in this scenario as well. As Fig. 4.6b shows, $\Delta V_{1,c}^{-}$ and $\Delta V_{1,m}^{-}$ are 24.44 kV and 22.71 kV, respectively, at $t = 75$ ms, resulting in $\delta_1^{-} = 7.6\%$. Being smaller than the defined thresholds, the obtained δ_1^{-} and δ_1^{+} confirm that an internal fault has happened.

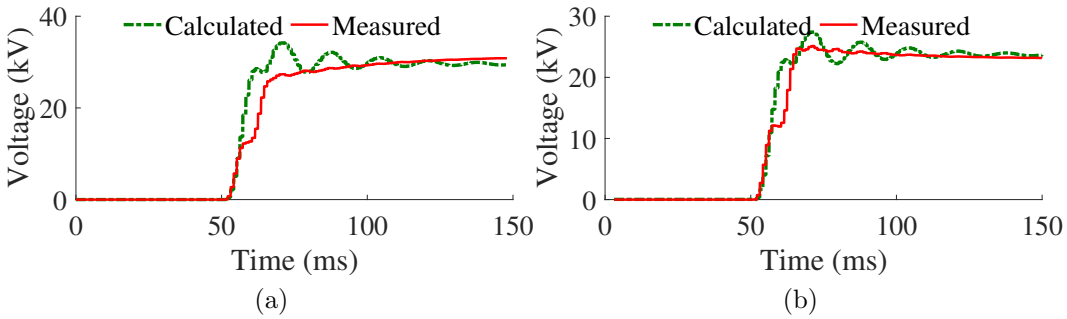


Figure 4.6: Superimposed voltages at bus 11 during Scenario 2, (a) PS, (b) NS.

• Scenario 3: An ABCG fault occurs 10 km away from Bus 11 on Line 6-11 in the test system, with a 1 Ω fault resistance. Fig. 4.7a displays the measured and calculated PS superimposed voltages: at $t = 75$ ms, $\Delta V_{1,c}^{+}$ and $\Delta V_{1,m}^{+}$ are 114.9 and 109.8 kV, respectively. Therefore, δ_1^{+} is 4.64%, which is less than tr_1^{+}, indicating an internal fault. In this scenario, since $\left|I_{n,pp}^{-}/I_{n,pp}^{+}\right| = 0.3\%$ for each terminal, due to the symmetrical nature of the fault, the NS submodule of the proposed method is inactive.

• Scenario 4: In this case, LCDR II's measurements for all phases are targeted by an MMA with $|\Delta I_6| = 0.251$ kA. As explained in Section 2.3, this is the minimum $|\Delta I_6|$ that

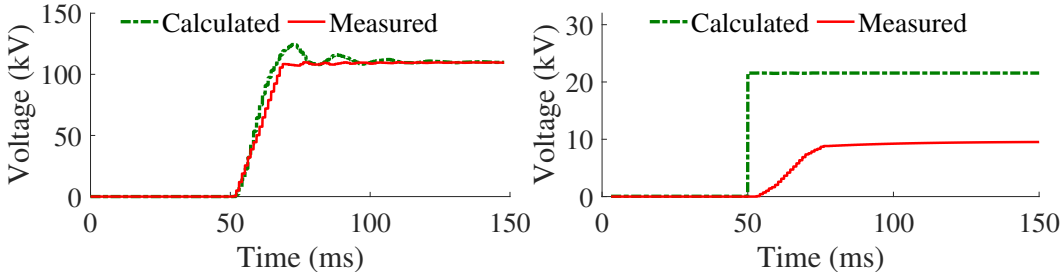


Figure 4.7: PS Superimposed voltages at bus 11 during (a) Scenario 3, (b) Scenario 4.

can move LCDR I's operating point into the trip zone. Fig. 4.7b illustrates the measured and calculated superimposed voltages during this FDIA: at $t = 75$ ms, δ_1^+ is 127% for PS. Therefore, the PS submodule of the proposed method detects the attack, and the trip signal for all differential elements (i.e., phase and sequence 87L) are blocked. In this scenario, the NS submodule is inactive, since the FDIA is symmetrical and $\left|I_{n,pp}^-/I_{n,pp}^+\right|$ for both terminals are 0.01%. It should be mentioned that, once the FDIA of this scenario starts, $\Delta V_{1,c}^+$ immediately changes from zero to 21.56 kV in one step, due to the sudden initiation of false data injection, which changes I_{diff} from zero to 0.251 kA.

• Scenario 5: This case involves a PMA with $\Delta\theta_6 = 35.1°$. As explained in Section 2.3, this $\Delta\theta_6$ is the smallest one that moves the operating point of the LCDR into the trip zone. Thus, LCDR I falsely picks up. Fig. 4.8a illustrates that at $t = 75$ ms, $\Delta V_{1,m}^+ = 0.375$ kV, but $\Delta V_{1,c}^+ = 8.55$ kV. Thus, $\delta_1^+ > tr_1^+$ and the attack is detected. The NS submodule, on the other hand, is inactive during this scenario, since $\left|I_{n,pp}^-/I_{n,pp}^+\right|$ for both terminals are almost zero. Additionally, converting this $\Delta\theta_6$ to a time delay results in $\Delta t = 1.625$ ms. A TSA associated with the obtained Δt is developed by modifying the true measurement times from t to $t + \Delta t$. Superimposed voltages at Bus 11 during such a TSA are shown in Fig. 4.8b: $\Delta V_{1,c}^+$ is much greater than $\Delta V_{1,m}^+$, resulting in $\delta_1^+ > tr_1^+$ and indicating an attack.

• Scenario 6: By intruding into the communication system, an attack changes I_6 received by LCDR I to the currents pertaining to a real internal AC fault—in the middle of Line 6-11 with 5 Ω fault resistance. As a result, LCDR I's operating point moves into the trip zone. As Fig. 4.9a shows, $\Delta V_{1,c}^+$ is 4.22 times larger than $\Delta V_{1,m}^+$, which results in a sig-

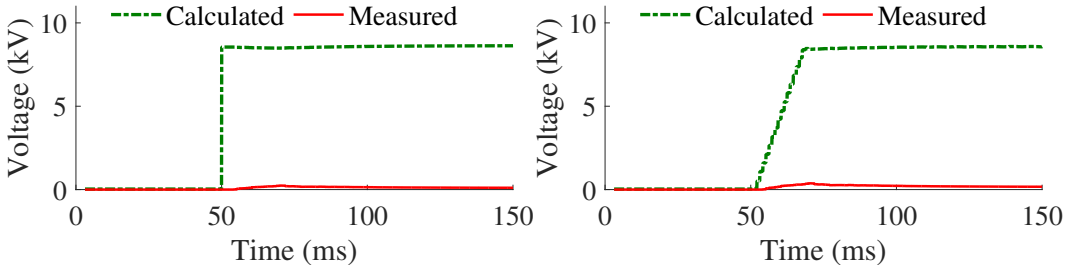


Figure 4.8: PS superimposed voltages at bus 11 during Scenario 5, (a) PMA, (b) TSA.

nificantly greater δ_1^+ than tr_1^+. On the other hand, $\left|I_{1,pp}^-/I_{1,pp}^+\right|$ is 0.01%, while $\left|I_{2,pp}^-/I_{2,pp}^+\right|$ is 105%, due to manipulated remote measurements. As a result, the NS submodule is active in this scenario. In spite of $\Delta V_{1,m}^-$, which is zero, $\Delta V_{1,c}^-$ is about 8.37 kV (Fig. 4.9b). This difference implies $\delta_1^- = \infty$. As a result, both NS and PS submodules detect the FDIA.

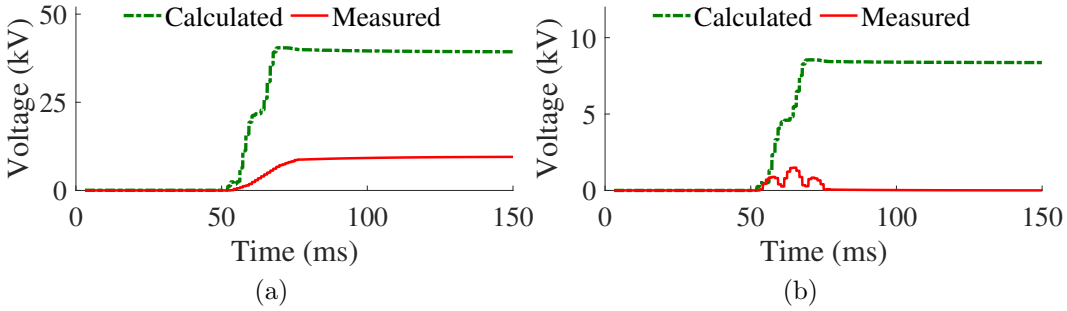


Figure 4.9: Superimposed voltages at bus 11 during Scenario 6, (a) PS, (b) NS.

• Scenario 7: This scenario investigates the performance of the proposed method during high-current external faults that saturate the measurement CTs of Line 6-11. External faults accompanied by CT saturation can incorrectly move the operating point in the differential-restraining plane of an LCDR into the trip zone. Therefore, LCDRs are always equipped with CT saturation detector to prevent false tripping during external faults [1, 66, 102]. Given that the proposed attack-detection method is activated only if an LCDR picks up, this scenario simulates a case in which the CT saturation detector fails to operate correctly during an external fault and thus the LCDR picks up incorrectly. This scenario

takes into account the worst CT-saturation case, in which only one of the CTs saturates. During this scenario, an ABG fault with a resistance of 1 Ω occurs at the middle of line 5-6 at $t = 50$ ms. This scenario involves three saturation levels for the CT installed at Bus 6: 1) VFS, which is defined to occur in less than 3 ms, 2) FS, which occurs before the fault current reaches its first extremum, and 3) MS, which occurs after the first extremum of the fault current [91]. Fig. 4.10 shows the primary and secondary currents of the CT installed at Bus 6 during these three cases. When the measured current is not distorted by CT saturation, the current defined in (4.23) is zero, resulting in zero calculated superimposed voltage. However, when the CT saturates, an error is created in $I^s_{k,pp}$; the faster the saturation level, the larger the error would be. This error leads to non-zero calculated PS and NS superimposed voltages at bus 11. Fig. 4.11 shows these voltages for VFS, FS, and MS. For both sequences and all saturation levels, there is a large difference between the measured and calculated superimposed voltages, indicating that the trip signal should be blocked. Therefore, a byproduct of the proposed method is blocking nuisance trip signals due to CT saturation during external faults.

4.3.2 Real-Time Simulation

This subsection utilizes an OPAL RTS to investigate the real-time performance of the proposed method. This approach utilizes a microprocessor that implements the proposed method and is connected to an RTS, thereby it constitutes a Hardware-In-The-Loop (HIL) verification environment. In the HIL setup (Fig. 4.12), a microprocessor emulates an LCDR that implements the proposed method, and verifies its performance using simulation signals obtained in real time. In addition to a new scenario, referred to as Scenario 8, Scenarios 1 and 6 of the previous subsection have been also carried out again using the HIL setup.

- Scenario 1 of the previous subsection is tested again by the HIL setup. After the relay picks up, the proposed method calculates $\Delta V^+_{1,c}$ and $\Delta V^-_{1,c}$, and measures $\Delta V^+_{1,m}$ and $\Delta V^-_{1,m}$. To illustrate these quantities using an oscilloscope, they are scaled down by a factor of 1/1000. Fig. 4.13 shows the PS and NS superimposed voltages at bus 11 obtained from the RTS. The green and purple curves represent the calculated and measured superimposed voltages, respectively. The time and voltage divisions for both channels in this figure are

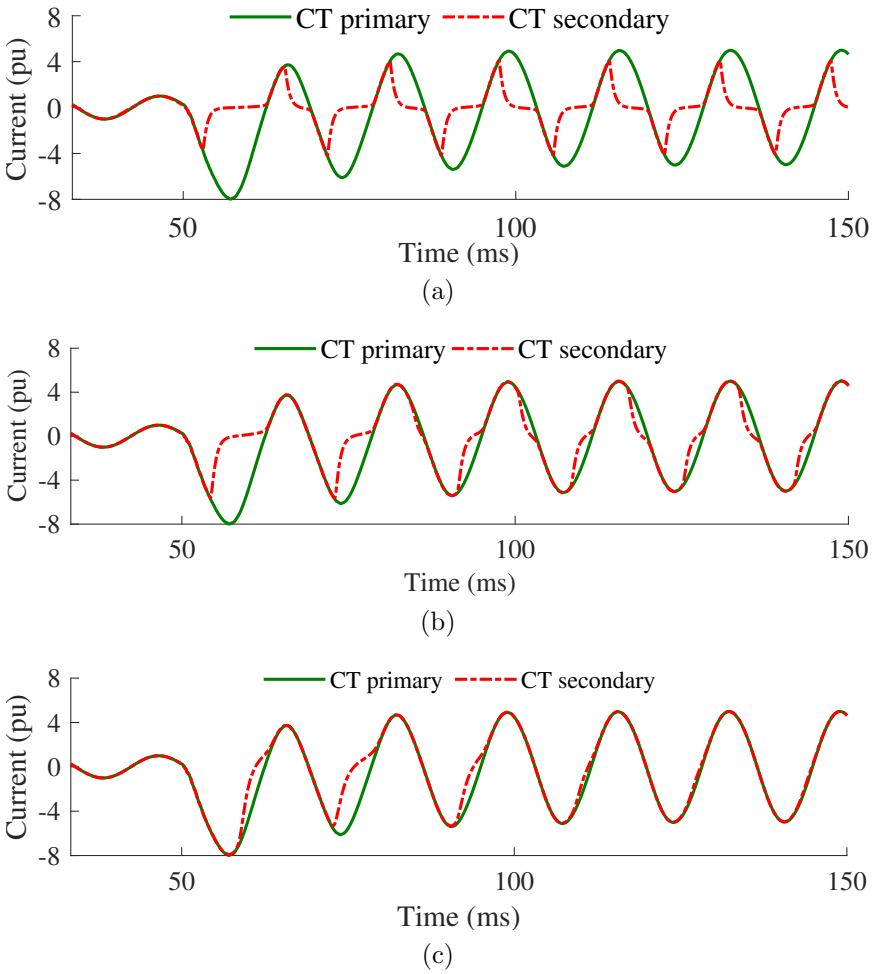


Figure 4.10: Primary and secondary currents of the CT installed at Bus 6 for different levels of saturation, (a) VFS, (b) FS, (C) MS.

10 ms and 500 mV. Comparing Fig. 4.5 and Fig. 4.13 reveals that the HIL testing of the proposed method yields the same results as obtained for Scenario 1 in the previous subsection, and indicates that the relay's pickup is due to an internal fault.

• For Scenario 6 of the previous subsection, immediately after the LCDRs picks up, the PS and NS superimposed voltages at local terminals are calculated. Fig. 4.14 shows the PS and NS superimposed voltages at bus 11 obtained from the RTS. The green and purple curves represent the calculated and measured superimposed voltages, respectively.

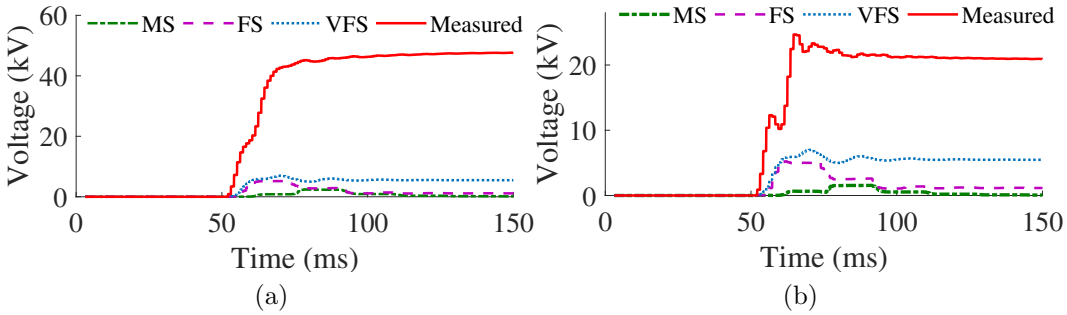


Figure 4.11: Superimposed voltages at bus 11 during Scenario 7, (a) PS, (b) NS.

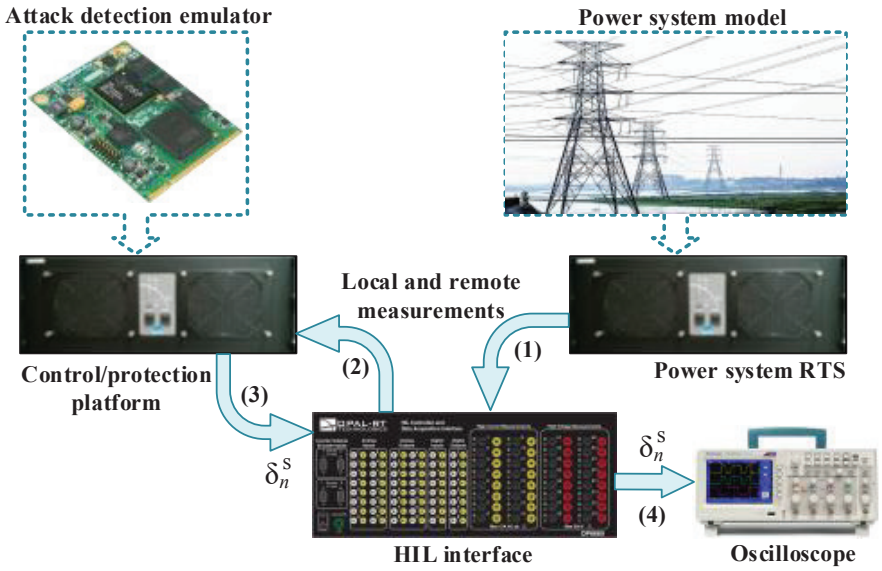
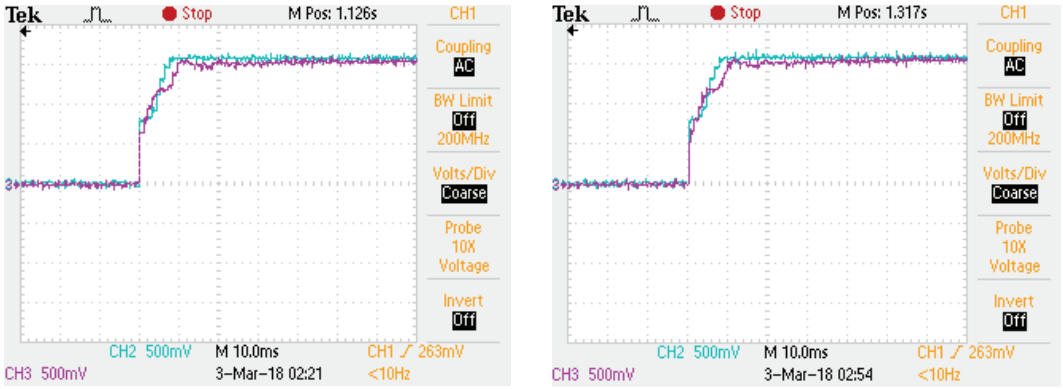


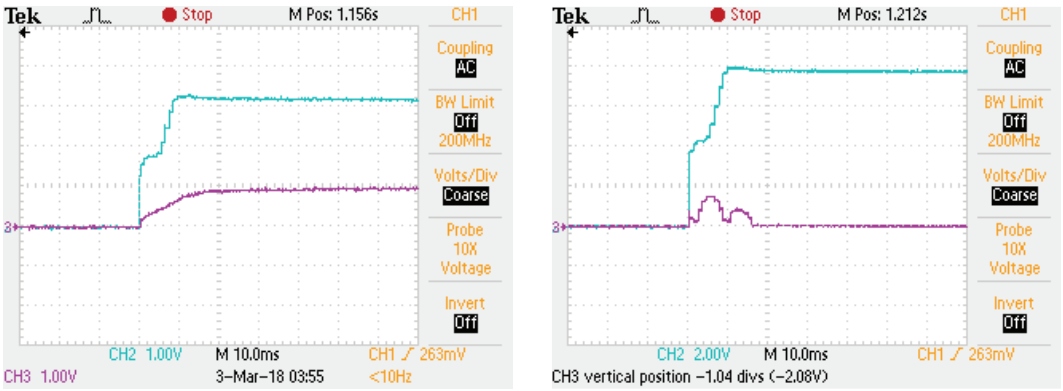
Figure 4.12: HIL setup.

The scaling factor for this scenario is 1/10000. The time division for both sub-figures is 10 ms; the voltage division for sub-figures 4.14a and 4.14b are 1 V and 2V, respectively. The obtained differences between the measured and calculated superimposed voltages for both sequences ($\delta_1^+ \approx 200\%$ and $\delta_1^- \approx \infty$) indicate that the pickup is due to an attack, so the trip signal should be blocked.



(a) (b)

Figure 4.13: Superimposed voltages at bus 11 obtained from RTS during Scenario 1, (a) PS, (b) NS.

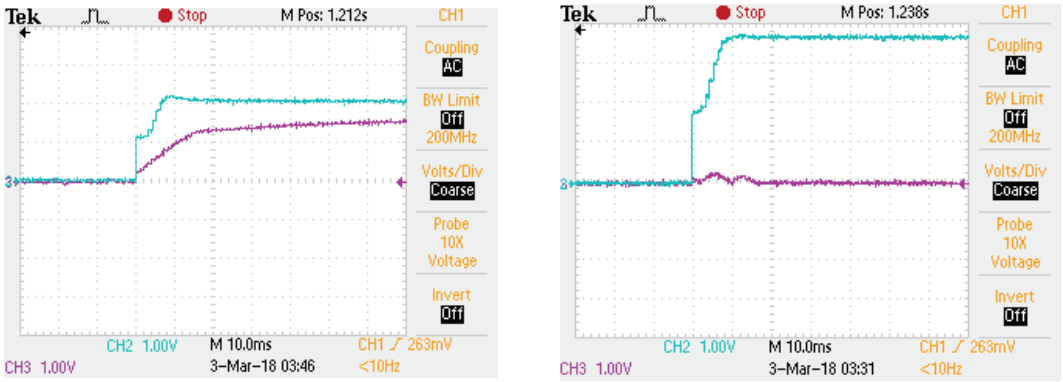


(a) (b)

Figure 4.14: Superimposed voltages at bus 11 obtained from RTS during Scenario 6, (a) PS, (b) NS.

• Scenario 8: In this scenario, an FDIA replaces real measured I_6 by the I_6 pertaining to an internal AG fault—with a resistance of 250 Ω happening at 90 km away from Bus 11 on Line 6-11. Fig. 4.15 illustrates the superimposed voltages obtained by measurement and calculation, shown by the green and purple curves, respectively. The voltage scaling factor is 1/1000 for this scenario. The time and voltage divisions for both channels are 10

ms and 1 V, respectively. As shown in Fig. 4.15a, $\Delta V_{1,c}^{+}$ is about 53% greater than $\Delta V_{1,m}^{+}$, indicating the occurrence of an attack. On the other hand, $\left|I_{2,pp}^{-}/I_{2,pp}^{+}\right|$ is 154%, because the FDIA emulates an asymmetrical fault. However, since only the remote measurements are manipulated, $\left|I_{1,pp}^{-}/I_{1,pp}^{+}\right|$ remains about zero. Therefore, the NS submodule is also active in this scenario. As $\Delta V_{1,m}^{-} \approx 0$, calculating δ_1^{-} for this scenario yields a very large number, which implies an attack. Thus, both the PS and NS submodules successfully detect the attack.



(a) (b)

Figure 4.15: Superimposed voltages at bus 11 obtained from RTS during Scenario 8, (a) PS, (b) NS.

4.4 Conclusion

This chapter presented a method to detect FDIAs and TSAs targeting AC LCDRs. The proposed method can be implemented by both SV-based and phasor-based AC LCDRs, and requires only local and remote current and local voltage measurements, which are all available in today's commercial relays. In the proposed method, when an AC LCDR's operating point enters the trip zone, instead of immediately tripping the line, its PS and NS submodules derive the superimposed voltages at the LCDR's terminal from two different ways, i.e., by measurement and calculation. Attacks are then detected if the difference

between the calculated and measured superimposed voltages in any sequence exceeds the defined threshold for that sequence. Off-line and real-time simulation results and case studies confirmed that the proposed method effectively detects attacks and differentiates them from faults.

Chapter 5

Attack Detection Method for DC LCDRs in Medium-Voltage DC Systems

In previous chapters, two methods were presented to detect cyber-attacks against AC LCDRs. This chapter, however, presents a method to detect attacks against DC LCDRs. The proposed method is comprised of POCs installed in series with each converter. During faults, the resultant RLC circuit causes the POCs to resonate and generate a damped sinusoidal component with a specific frequency, i.e., f_d. However, f_d is not generated during cyber-attacks or other events. Thus, LCDRs' pickup without detecting the f_d denotes a cyber-attack. Given that f_d is locally measured and analyzed by each LCDR, the attack-detection approach cannot be targeted by cyber-attacks.

On this basis, Section 5.1, explains the proposed attack detection method. Afterwards, Section 5.2 evaluates the proposed method's performance. Finally, Section 5.3 concludes this chapter.

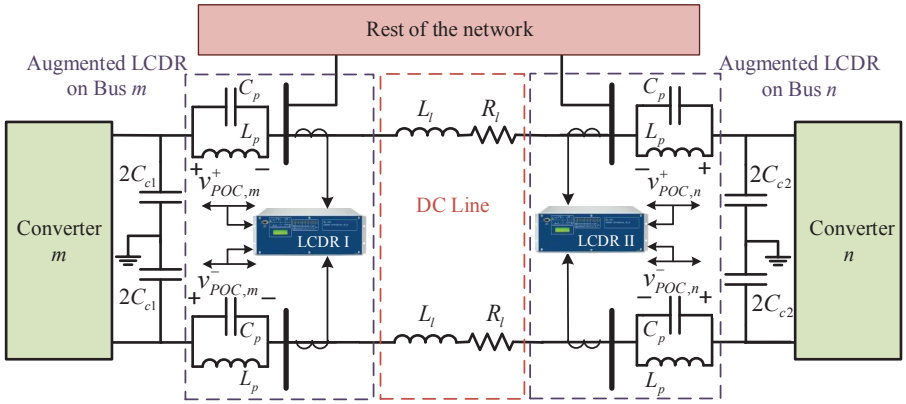


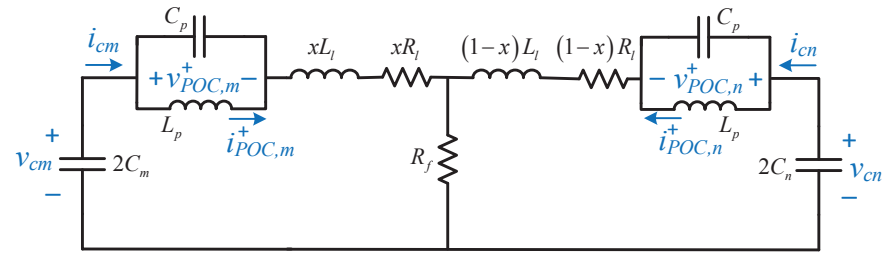
Figure 5.1: Attack Detection scheme for LCDRs of a DC Line after including POCs.

5.1 The Proposed Attack Detection Method for DC LCDRs

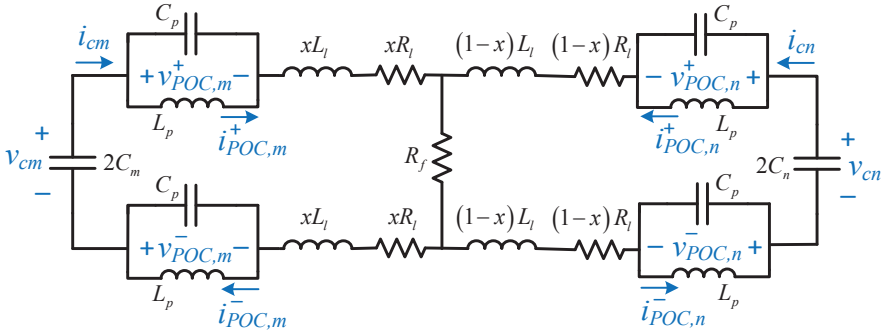
The proposed method's objective is to verify DC LCDRs' tripping decision via uncompromisable locally measured signals, while maintaining the LCDRs' high-speed response to faults. After implementing the proposed method, a DC LCDR trips the line that is protecting only if the LCDR picks up and its attack detection submodule verifies that the pickup is due to a real fault. To detect attacks accurately, the proposed method installs a POC on each converter's terminal, as discussed next.

5.1.1 Augmenting DC LCDRs with POCs

To verify the occurrence of faults, the proposed method installs two simple POCs—comprised of an inductor L_p in parallel with a capacitor C_p—on both poles of each converter's terminal in a DC system (Fig. 5.1). Therefore, LCDRs of all lines connected to a bus can measure the voltage across the POC installed on that bus locally. For example, a total of $2 \times 7 = 14$ POCs are required for the DC system of Fig. 2.22. When a fault occurs on the line between converters m and n in Fig 5.1, the RLC fault circuits shown in



(a)



(b)

Figure 5.2: System model during capacitor discharge stage, (a) PG fault, (b) PP fault.

Fig 5.2 are formed [103]. These figures illustrate the equivalent RLC circuit from the perspective of converters m and n under Pole-to-Ground (PG) and Pole-to-Pole (PP) faults in a DC system after the addition of POCs. The illustrated fault circuits are active during the capacitor discharge stage [103]. In these circuits, a fault with the resistance of R_f is located at a distance of $x\mathcal{L}_{dc}$ from converter m in Fig. 5.1, where $\mathcal{L}_{dc}$ is the length of the DC line and $0 < x < 1$. Each POC in Fig. 5.2 adds a set of complex poles, i.e., $\zeta \pm j2\pi f_d$. Thus, POCs resonate during faults and generate a damped sinusoidal component with the frequency of f_d [104]. Therefore, attack detection submodules of LCDRs on converters m and n can detect f_d by measuring the voltage across their associated POCs in Fig. 5.2.

On the other hand, at steady state, L_p and C_p behave like a short-circuit and an open-circuit, respectively, causing no effect on the grid operation. Similarly, POCs do

not resonate during load and generation changes, since the DC link capacitor filters the propagation of high-frequency components from the load and generation side to the DC grid. This will be shown later in Scenario 6 in Section 5.2. Thus, detecting f_d by measuring the voltage across POCs locally indicates the existence of a fault in neighboring lines, and is used to verify the occurrence of faults and detect attacks.

5.1.2 Selection Criteria for f_d

As explained in the previous section, adding POCs to the terminals of converters m and n in Fig. 5.1 results in generating a damped component with the frequency of f_d during faults. Because detection of f_d is going to be used to verify the occurrence of faults, f_d should be in a frequency range that does not overlap with any non-fault transient that can arise in a DC system. Doing so guarantees that f_d detection is by fault signature only, and thus can be used to verify LCDRs' pickup.

Since DC systems are usually fully interfaced with AC/DC Voltage-Source Converters (VSCs) and DC/DC converters, frequencies generated in DC line currents are defined by VSCs' switching frequency and the harmonics existing on the AC side. For AC/DC VSCs, the second and sixth harmonics are the most dominant ones [105]. Accordingly, 360 Hz is the highest frequency that can be imposed on a DC system by AC-side transients. For DC/DC converters, the generated angular frequencies are $1/(2\pi\sqrt{L_{conv}C_{conv}})$ or $(1-D)/(2\pi\sqrt{L_{conv}C_{conv}})$, depending on the converter type, where D, L_{conv}, and C_{conv} are the duty-cycle, inductance, and capacitance of the converter [106]. For example, for the DC system of Fig. 2.22, 125 Hz is the highest frequency component that can be generated by transients from the DC/DC converters. Hence, taking into account a 10% security margin, f_d should be higher than 400 Hz. f_d should also be different than the switching frequency of Insulated-Gate Bipolar Transistors (IGBTs), which is 5 kHz in the test system of Fig. 2.22, and its harmonics. Additionally, f_d should be lower than half of the maximum sampling rate of LCDRs, i.e., the Nyquist frequency, to adhere to the recommended sampling standards. Currently, commercially available LCDRs can sample up to 8 kHz [66].

On the other hand, given that f_d is generated due to the addition of POCs, the relation between f_d and POC parameters should be obtained. By doing so, C_p, and L_p can be

designed such that the desired f_d is generated during faults. In general, f_d is a function of the natural frequency $f_0 = 1/(2\pi\sqrt{L_pC_p})$ and the damping factor, ζ [104]. For high order circuits, obtaining the exact relation between ζ, f_0, and f_d is mathematically intractable. In Section 5.1.3, it is shown that if f_0 for the circuits of Fig. 5.2 is large enough, ζ would be negligible and f_d can be approximated by f_0. On the other hand, as stated above, f_0 is inversely proportional to C_p and L_p. Therefore, considering all the above-mentioned criteria, f_0 is selected to be 4 kHz, i.e., the upper frequency bound defined earlier, to maximize f_0 and to minimize the footprint and cost of the utilized passive elements. This selected f_0 can be achieved by choosing $C_p = 40$ μF and $L_p = 40$ μH. It is worth noting that any other combinations of L_p and C_p that results in this f_d can also be considered. The state-space analysis performed in Section 5.1.3 proves that selecting the above-mentioned values for L_p and C_p results in $f_d \approx 4$ kHz.

5.1.3 Relation between f_d and f_0

This section shows that if the selected C_p and L_p are small enough, the damping factor can be ignored, and thus f_d can be approximated by f_0. To prove the validity of this approximation, first the state-space models of the circuits of Fig. 5.2 during faults is found and their eigenvalues are obtained. Then, the f_d generated due to POCs is determined. Afterwards, the sensitivity of f_d to fault location and resistance, and to the variation of different parameters is studied, and the maximum error between f_d and f_0 during different cases is investigated. In the following, for the sake of brevity, detailed analysis is presented only for PG faults, yet the results are presented for both fault types.

To find the state-space model of the faulty line in Fig. 5.2a, the voltages of DC link capacitors of converters m and n, i.e., v_{cm} and v_{cn}, the currents of DC link capacitors of converters m and n, i.e., i_{cm} and i_{cn}, the voltages of POCs installed on the terminals of converters m and n, i.e., $v^+_{POC,m}$ and $v^+_{POC,n}$, and the currents of both POCs' inductors, i.e, $i^+_{POC,m}$ and $i^+_{POC,n}$, are chosen as system states and their respective differential equations are obtained and formed in a matrix form, as follows:

$$\dot{\mathbb{X}} = \mathbb{A}\mathbb{X} \tag{5.1}$$

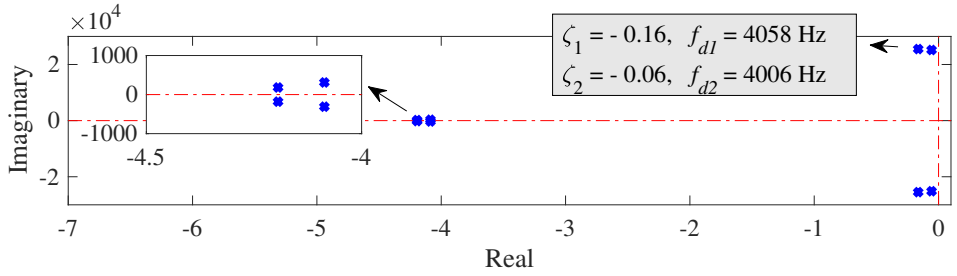


Figure 5.3: Eigenvalues of the system during capacitor discharge stage when a fault with $R_f = 0\ \Omega$ happens on Line 2-5 of the test system at $x = 0.25$.

where

$$\mathbb{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & \frac{-1}{2C_{c1}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{-1}{2C_{c2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{C_p} & 0 & \frac{-1}{C_p} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{C_p} & 0 & \frac{-1}{C_p} \\ \frac{1}{xL_l} & 0 & \frac{-1}{xL_l} & 0 & \frac{-R_l}{L_l} - \frac{R_f}{xL_l} & \frac{-R_f}{xL_l} & 0 & 0 \\ 0 & \frac{1}{(1-x)L_l} & 0 & \frac{-1}{(1-x)L_l} & \frac{-R_f}{(1-x)L_l} & \frac{-R_l}{L_l} - \frac{R_f}{(1-x)L_l} & 0 & 0 \\ 0 & 0 & \frac{1}{L_p} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{L_p} & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.2a}$$

$$\mathbb{X} = \begin{bmatrix} v_{cm} & v_{cn} & v^+_{POC,m} & v^+_{POC,n} & i_{cm} & i_{cn} & i^+_{POC,m} & i^+_{POC,n} \end{bmatrix}^T \tag{5.2b}$$

in which T denotes the transpose operator.

In the next step, the system's eigenvalues are found, and their behavior is investigated when system parameters change. The symbolic analysis of poles is intractable, since the mathematical expressions are large and complicated. Alternatively, this study uses numerical analysis. In order to mimic a typical MVDC line of Fig. 5.1, the cable parameters R_l, L_l, and $\mathcal{L}_{dc}$ are set as 0.017 Ω/km, 2 mH/km, and 1500 m, respectively. Additionally, $2C_{cm}$ and $2C_{cn}$ are set to 10 mF, representing the dc link capacitors of converters m and n. The POC elements are set as per the designed values, i.e., $L = 40\ \mu$H and $C = 40\ \mu$F. Under a PG bolted fault ($R_f = 0\ \Omega$) happening at $x = 0.25$ from converter m on line $m - n$, i.e., 375 m away from converter m, Fig. 5.3 shows that the eigenvalues of the fault circuit

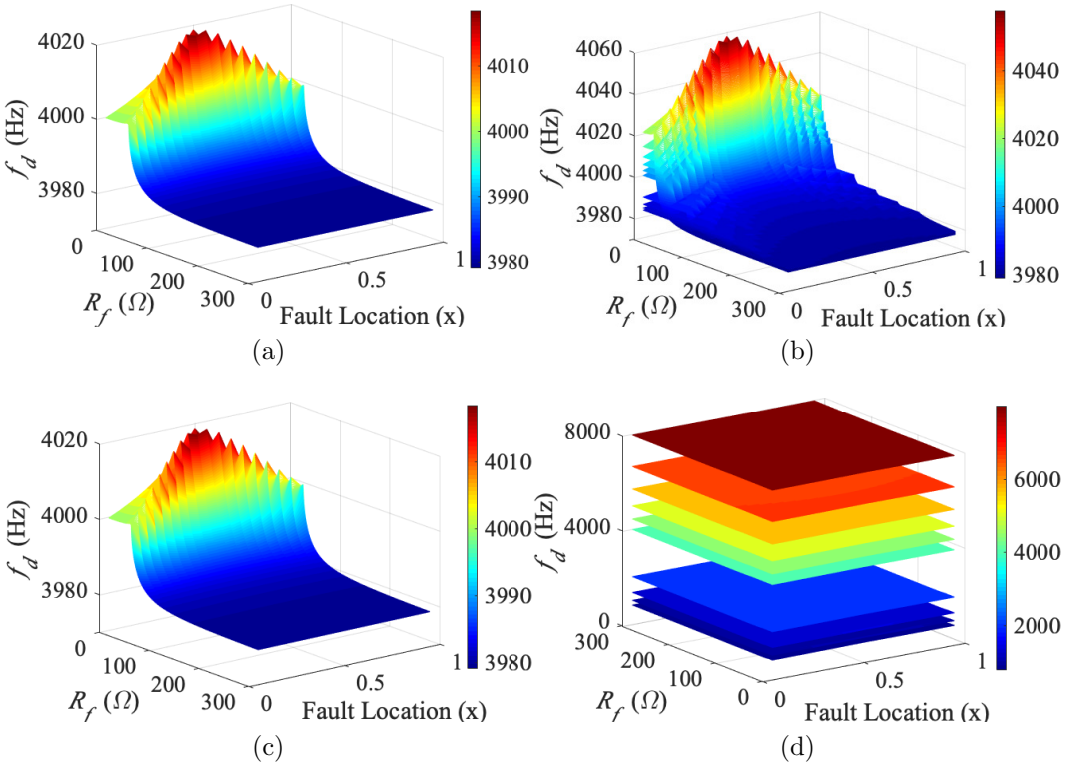


Figure 5.4: f_d generated during PG faults when, (a) only x and R_f change, (b) x, R_f, and line length ($\mathcal{L}_{dc}$) change, (c) x, R_f, and converters' capacitors (C_{c1} and C_{c2}) change, and (d) x, R_f, and f_0 change.

of Fig. 5.2a are equal to ($\zeta_1 = -0.16, f_{d1} = 4058$ Hz) and ($\zeta_2 = -0.06, f_{d2} = 4006$ Hz). Therefore, given that $f_0 = 1/\sqrt{L_p C_p} = 4$ kHz and alpha is negligible, f_d approximately equals f_0.

To assess the effect of various fault and system parameters on f_d during PG faults, a sensitivity analysis is conducted (Fig. 5.4). Fig. 5.4a shows f_d generated during PG faults, where R_f and x range from 0 to 300 Ω and 0 to 1, respectively: f_d changes between 3979 and 4018.5 Hz during different fault scenarios, where the maximum f_d is generated when the fault happens at $x = 0.5$ and $R_f = 0$ Ω. Thus, approximating f_d by f_0 causes maximum 0.46% error during PG faults. Additionally, the effect of line length on f_d should be investigated. To this aim, the original line length (1.5 km) is multiplied by a multiplier

$k \in \{0.5,\ 0.6,\ 0.7,\ 0.8,\ 0.9,\ 1,\ 2,\ 3,\ 4,\ 5\}$, and for each k, (f_d)s are obtained and plotted for all fault scenarios. As Fig. 5.4b illustrates, f_d for each line length remains almost the same, with the maximum f_d attained during a fault with 0 Ω resistance at the middle of the line. Moreover, the longer the line, the more accurate the approximation of f_d by f_0 would be. For example, for $k = 0.5$ and $k = 5$, the maximum errors are 1% and 0.1%, respectively. Similarly, the sensitivity of f_d during PG faults to variation of converters' capacitors (C_{c1} and C_{c2}) should be investigated as well. To do so, converters' capacitors are multiplied by the defined k multipliers, and (f_d)s are obtained and plotted for each k during all fault scenarios. As Fig. 5.4c shows, converters' capacitors do not affect f_d during faults, and the maximum attained error between f_d and f_0 for all fault scenarios is 0.46%. Finally, Fig. 5.4d investigates the effect of selecting different (f_0)s on the approximation error. To this aim, L_p and C_p are multiplied by the defined k multipliers, which is equivalent to multiplying f_0 by $1/k$. The (f_d)s generated during all fault scenarios are obtained and plotted in Fig. 5.4d: (f_d)s during all fault scenarios are very close to each other for each k. The approximation error, however, increases when k grows; for example, the maximum recorded errors between f_d and f_0 for $k = 0.5$, 1, and 5 are 0.2%, 0.48%, and 2.5%, respectively. This figure also confirms that if f_0 is large enough, ζ can be ignore, and so $f_d \approx f_0$.

To do the same analysis for PP faults, the state-space model of the circuit in Fig. 5.2b should be obtained. The state variables of this circuit are the states of the PG fault circuit, plus $v^-_{POC,m}$, $i^-_{POC,m}$, $v^-_{POC,n}$, and $i^-_{POC,n}$. Hence, f_d can be calculated by finding the new state matrix $\mathbb{A}$ and its eigenvalues. Fig. 5.5 investigates the sensitivity of f_d during PP faults to variation of different parameters. Similar to Fig. 5.4a, Fig. 5.5a shows (f_d)s during PP faults with R_f and x, ranging from 0 to 300 Ω and 0 to 1, respectively: f_d changes between 3980 and 4018.5 during different fault scenarios. Thus, approximating f_d by f_0 creates a maximum 0.5% error during various PP faults. Fig. 5.5b investigates the effect of different line lengths on the f_d generated during PP faults. To this aim, the defined k multipliers for PG faults are multiplied by the original line length (1.5 km), and for each k, f_d is obtained during various fault scenarios: for each k, f_d remains almost the same and very close to f_0 during all faults, and the approximation error decreases when k grows. For example, the maximum error of 1% occurs for $k = 0.5$. Fig. 5.5c indicates that f_d does not depend on converters' capacitors under PP faults—as previously concluded for

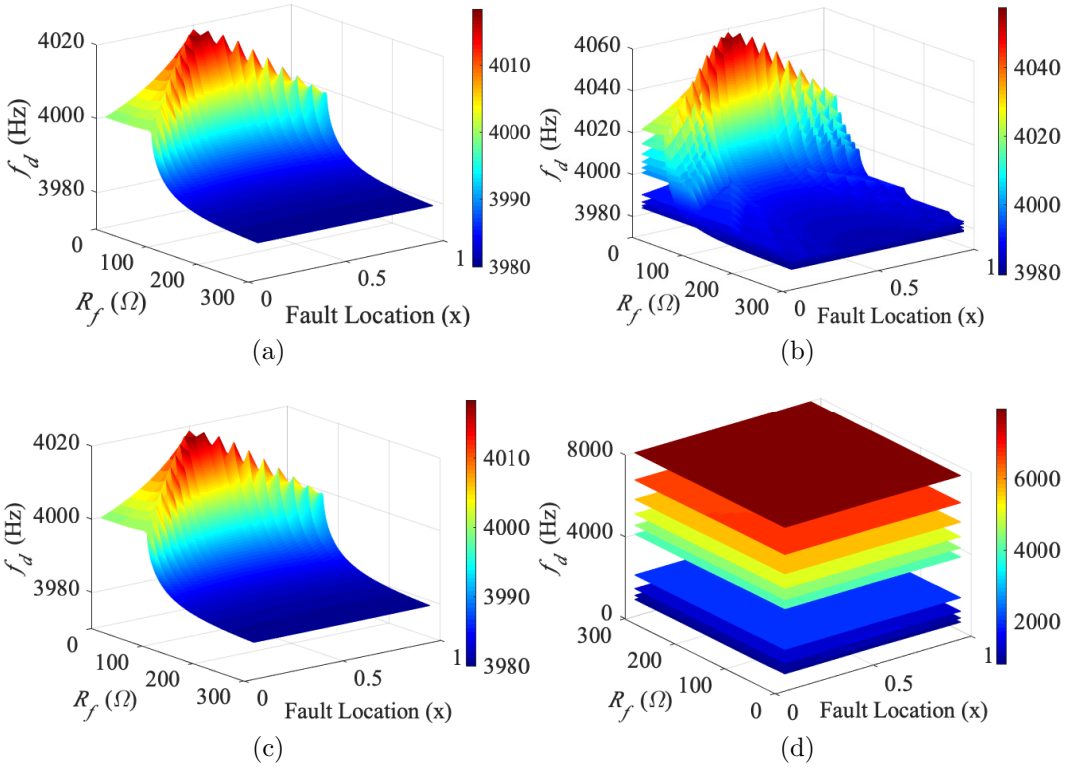


Figure 5.5: f_d generated during PP faults when, (a) only x and R_f change, (b) x, R_f, and line length ($\mathcal{L}_{dc}$) change, (c) x, R_f, and converters' capacitor (C_{c1} and C_{c2}) change, and (d) x, R_f, and f_0 change.

PG faults—and a maximum error of 0.5% occurs for all values of k. Finally, Fig. 5.5d investigates the effect of selected f_0 on the approximation error. To obtain this figure, L_p and C_p are multiplied by the defined k multipliers, which is equivalent to multiplying f_0 by $1/k$. As this figure shows, during all faults, f_d does not change much for each k. However, the smaller the k, the lower the the approximation error, as previously concluded for PG faults as well. For instance, the maximum recorded errors between f_d and f_0 for $k = 0.5$, 1, and 5 are 0.2%, 0.5%, and 2.4%, respectively. Thus, as previously concluded for PG faults, the larger the f_0, the less the error between f_d and f_0.

In conclusion, the analytical discussion and the sensitivity analysis presented in Sections 5.1.1, 5.1.2, and 5.1.3 show that f_d, i.e., the frequency of the damped sinusoidal

component generated by POCs during PG and PP faults, approximately equals f_0, which is independent from the system parameters and fault-conditions. Therefore, detecting f_d can be used to verify the pickup of LCDRs and detect cyber-attacks.

5.1.4 f_d Detection for Attack Diagnosis

As discussed in the previous section, generation of f_d can be used by the attack-detection submodule of LCDRs to verify the occurrence of faults and differentiate them from attacks. To detect f_d locally and determine the magnitude of the component that oscillates with this frequency, LCDRs can examine frequency content of the voltage across their local POCs using the FFT. To this aim, FFT computations are performed online, at each sampling instance, and are based on a sampled data window of the preceding input signal cycle. The length of the window should at least represent a period of $1/f_d$. On this basis, for a DC LCDR protecting a line connected to Bus b, the pickup for pole $p \in \{+, -\}$ is validated and a trip signal is sent to corresponding circuit breakers if the FFT element incorporated in the attack-detection submodule detects a component, with the frequency of f_d, whose magnitude satisfies the following equation:

$$V^p_{FFT,b} > tr^p_b \tag{5.3}$$

where $V^p_{FFT,b}$ is the magnitude of the component with the frequency of f_d obtained from the voltage across the POC installed at Bus b on pole p, and tr^p_b is its associated threshold. On the other hand, a cyber-attack is flagged and an LCDR's trip signal is blocked if the LCDR picks up and (5.3) is not met. The tripping logic of LCDRs after implementing the proposed method is illustrated in Fig. 5.6. The attack detection threshold in Fig. 5.6 and (5.3) should be found so as to minimize false attack detection during internal faults. The procedure for determining this threshold is explained in Section 5.2.

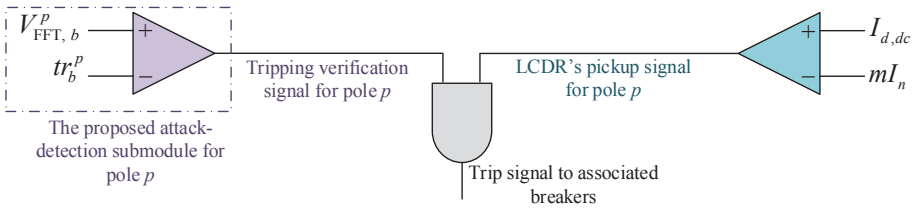


Figure 5.6: Tripping logic for each pole after implementing the proposed method.

5.2 Performance Evaluation

This section first determines thresholds associated with positive and negative poles for the LCDRs of Line 2-5 in the DC system of Fig. 2.22, and then investigates the performance of the proposed method during steady-state, faults, and cyber-attacks. Simulations are carried out using the PSCAD/EMTDC program on the test system of Fig. 2.22. To implement the proposed method as an extra layer of security against cyber-attacks, POCs are installed on each pole in series with converters, and LCDRs' tripping logic is modified as depicted in Fig. 5.6. Additionally, in accordance with the Nyquist criteria, f_d is selected to be equal to half of the sampling frequency, which is considered to be 8 kHz in this chapter [66]. Thus, $f_d = 4$ kHz is selected by choosing L_p=40 μH and C_p=40 μF, as discussed in Section 5.1.2.

In the first step, tr_b^+ and tr_b^- must be determined for all LCDRs from POCs' voltages. This section explains the procedure only for determining tr_2^+ and tr_2^- for the LCDR of Line 2-5 installed on Bus 2 using the voltage across the POCs installed on this Bus, yet the same procedure can be carried out for the remaining LCDRs. To accurately differentiate between attacks and faults, and to avoid false-positive and false-negative alarms, tr_2^+ and tr_2^- are selected such that they are (i) smaller than the least $V^+_{FFT,2}$ and $V^-_{FFT,2}$ that are generated during faults occurring on Line 2-5, and (ii) higher than non-fault measurement noise, which is modeled as white and Gaussian with the SNR of 85 dB [107]. To obtain the least $V^+_{FFT,2}$ and $V^-_{FFT,2}$ during faults, PP and Positive Pole-to-Ground (PPG) high-resistance far-end faults are simulated on Line 2-5. Considering $R_f = 200\ \Omega$ as the maximum fault resistance that could occur, $V^+_{FFT,2} = V^-_{FFT,2} = 6.5$ v are the least values obtained for these parameters, which are recorded during a 200 Ω PPG fault happening at $x = 5\%$

from Bus 5 on Line 2-5. Given that the measured error tolerance in commercial protective devices is often specified as ±5% of the measured value [108], a 5% security margin is also considered. Thus, tr_2^+ and tr_2^- for Line 2-5 are selected equal to 6.1 v. Considering the above-mentioned noise model and the determined thresholds, the false-negative alarm rate due to noise, i.e., the probability of $|\text{noise}| \geq tr_2^p$, is obtained to be practically zero. Thus, conditions (i) and (ii) are met if $tr_2^+ = tr_2^- = 6.1$ v. By following a similar procedure, tr_5^+, tr_5^-, tr_4^+, tr_4^-, are obtained to be 6.1 v, 6.1 v, 5.8 v, and 5.9 v, respectively.

To evaluate the performance of the proposed method, this section presents six scenarios: Scenarios 1 and 2 show how the proposed method thwarts cyber-attacks of Case Study 3 presented in section 2.6.3 of Chapter 2; Scenarios 3 and 4 investigate the effect of fault parameters; Scenario 5 investigates the effect of installed POCs on VSCs' transients; and Scenario 6 evaluates the performance of the proposed method during non-fault events.

• Scenario 1: This scenario shows how the proposed method can detect the FDIA that targeted Line 2-5 in Case study 3 in Section 2.6.3 of chapter 2, and thus prevent the voltage collapse happened in that case study. To this aim, this cyber-attack is carried out again; however, this time, the proposed method has been implemented for LCDRs of Line 2-5, and the POCs have already been installed on the terminals of the converters of Buses 2 and 5. When the attacker manipulates the remote measurements of Line 2-5, sent from Bus 2 to Bus 5, the operating point of the LCDR installed at Bus 5 enters the trip zone, thus it picks up. Yet, as Fig. 5.6 shows, after implementing the proposed method, the LCDR's pickup is not adequate to trip Line 2-5, and the proposed method's verification, i.e., satisfaction of (5.3), is also required. Fig. 5.7 shows $v_{POC,5}^+$, i.e., the voltage across the POC of Bus 5's converter on the positive pole, and the extracted $V_{FFT,5}^+$ from this voltage: $V_{FFT,5}^+$ does not exceed its associated threshold, so no fault is detected by the proposed method. The same result is obtained for the negative pole as well. Therefore, the relay flags a cyber-attack, and the trip signal of the LCDR is blocked. On the other hand, cyber-attacks cannot fool the proposed method by counterfeiting an $V_{FFT,5}^+$ and/or $V_{FFT,5}^-$ that satisfies (5.3), since these parameters are obtained locally, and are thus not attackable.

• Scenario 2: Similar to Scenario 1, this scenario shows how the proposed method detects the TSA targeted the GPS of Bus 3's substation in the case study of Section 2.6.3

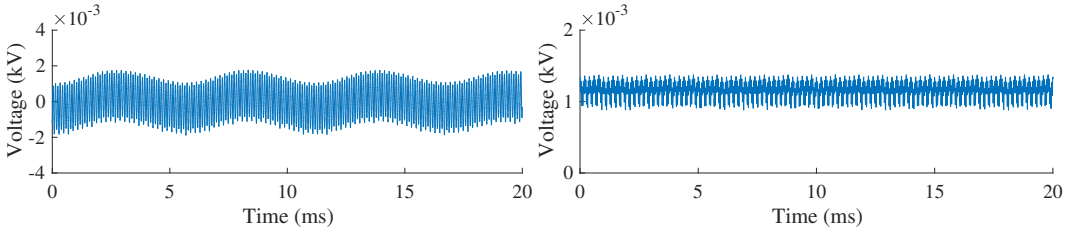


Figure 5.7: $v^{+}_{POC,5}$ and $V^{+}_{FFT,5}$ during Scenario 1 (a) $v^{+}_{POC,5}$, (b) $V^{+}_{FFT,5}$.

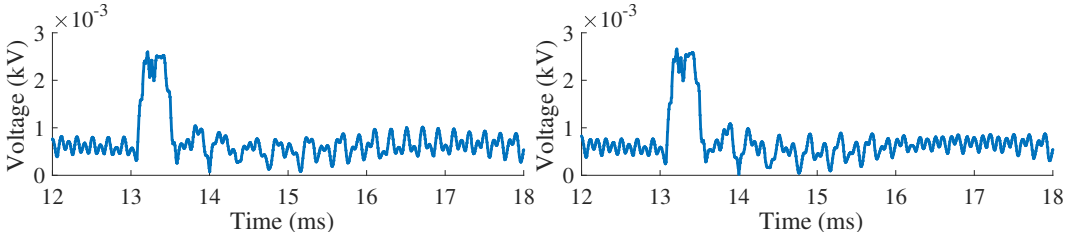


Figure 5.8: $V^{+}_{FFT,4}$ and $V^{-}_{FFT,4}$ during Scenario 2 (a) $V^{+}_{FFT,4}$, (b) $V^{-}_{FFT,4}$.

in Chapter 2 and prevents tripping of Line 4-3. To this aim, this scenario assumes that the LCDRs of Line 5-2 are not augmented by the proposed method, so this line is tripped by a cyber-attack (otherwise, the TSA cannot fool the LCDR installed at Bus 3 into picking up). As explained in Section 2.6.3, manipulating the time-stamp of measurements sent from Bus 3 to Bus 4 and tripping Line 2-5 at $t = 13$ ms move the operating point of Line 4-3's LCDR installed at Bus 4 into the trip zone, and the LCDR picks up. To trip the line, however, (5.3) must be met as well. Fig. 5.8 shows $V^{+}_{FFT,4}$ and/or $V^{-}_{FFT,4}$ during this cyber-attack: none of these parameters exceed their associated thresholds, so the proposed method does not detect any fault on Line 3-4. As a result, the relay flags a cyber-attack, and the trip signal is blocked.

• Scenario 3: This scenario investigates the effect of fault resistance and type on the proposed method's performance. To this aim, bolted PPG, Negative Pole-to-Ground (NPG), and PP faults are simulated at $x = 0.4$ from Bus 5 on Line 5-2. All faults happen at $t = 10$ ms, so the LCDRs of Line 2-5 both pick up. To verify the occurrence of the fault, the

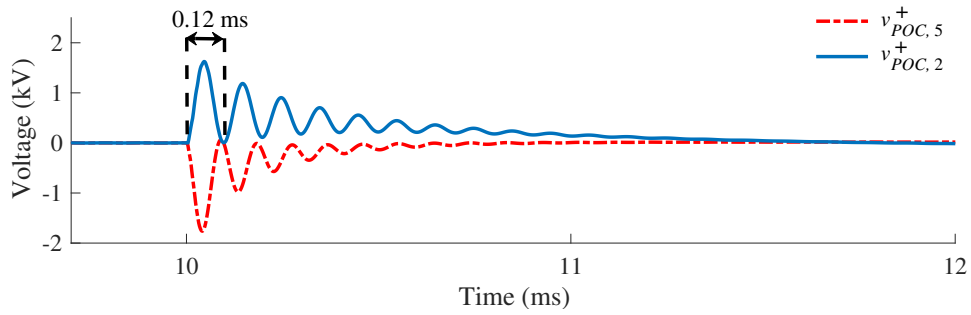


Figure 5.9: $v^+_{POC,5}$ and $v^+_{POC,2}$ during a PPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5.

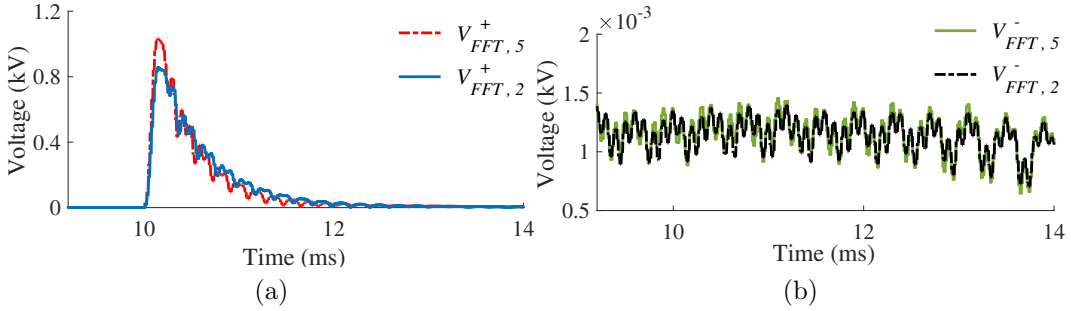


Figure 5.10: $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during a PPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$.

proposed method obtains $(V^p_{FFT,2})$s and $(V^p_{FFT,5})$s from voltages across POCs installed on Buses 2 and 5. Fig. 5.9 illustrates the voltages across the positive pole's POCs installed at Buses 5 and 2—i.e., $v^+_{POC,5}$ and $v^+_{POC,2}$, respectively—during the PPG fault: $v^+_{POC,5}$ and $v^-_{POC,5}$ start resonating at right after the fault occurs, and decay completely in about 4 ms. The period of this voltage component is almost 0.24 ms, which is associated with the $f_d = 4$ kHz. Fig. 5.10a shows $V^+_{FFT,5}$ and $V^+_{FFT,2}$: these parameters reach their associated thresholds (6.1 v) in less than a microsecond, so LCDRs of Buses 5 and 2 verify the occurrence of a fault on the positive pole very quickly. Fig. 5.10b shows that $V^-_{FFT,2}$ and $V^-_{FFT,5}$ do not exceed tr^-_2 and tr^-_5, i.e., 6.1 v, indicating that no fault has happened on the negative pole. Thus, the proposed method correctly identifies the fault type. Since LCDRs picked up and the fault was verified, the LCDRs trip the line. Similarly, Figs. 5.11 and 5.12 confirm similar results for NPG and PP faults: $V^-_{FFT,5}$ and $V^-_{FFT,2}$ exceed

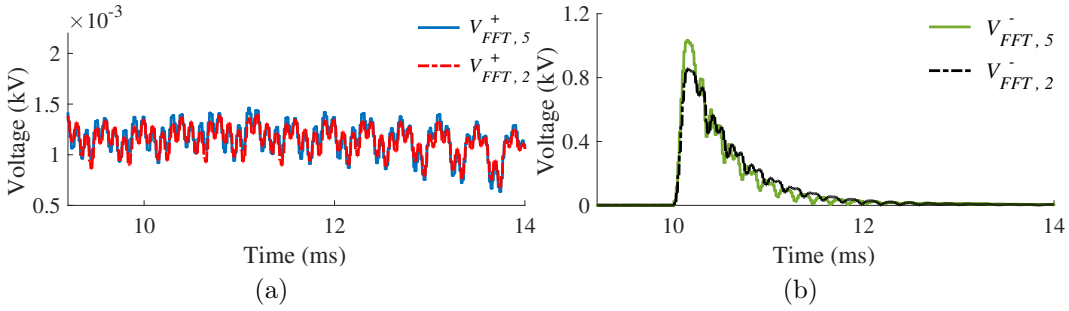


Figure 5.11: $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during an NPG fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$.

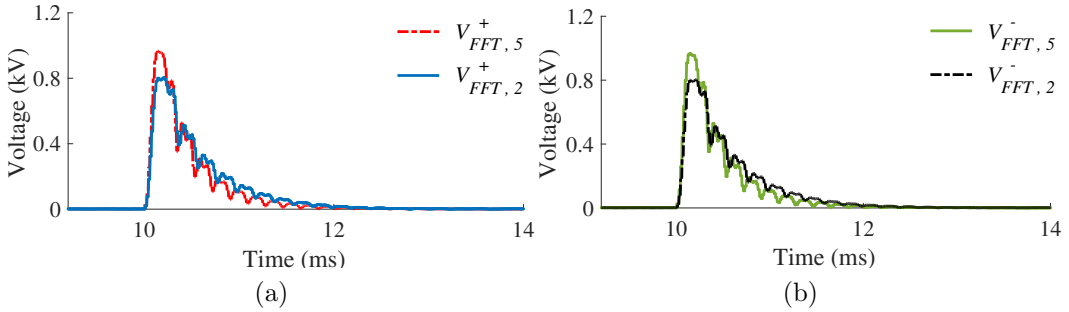


Figure 5.12: $V^+_{FFT,5}$, $V^+_{FFT,2}$, $V^-_{FFT,5}$, and $V^-_{FFT,2}$ during a PP fault with $R_f = 0\ \Omega$ at $x = 0.4$ from Bus 5, (a) $V^+_{FFT,5}$ and $V^+_{FFT,2}$, (b) $V^-_{FFT,5}$ and $V^-_{FFT,2}$.

their thresholds in a fraction of a microsecond if there is a fault on the negative pole, while $V^+_{FFT,5}$ and $V^+_{FFT,2}$ satisfy (5.3) only if a fault happens on the positive pole. To further investigate the performance of the proposed method, Table 5.1 presents $V^+_{FFT,5}$, $V^-_{FFT,5}$, $V^+_{FFT,2}$, and $V^-_{FFT,2}$ during faults with $R_f = 0$, 0.1, 0.5, 1, 5, 10, 20, 50, 100, 150, and 200 Ω, all at $x = 0.4$ from Bus 5 on Line 5-2: the larger the R_f, the smaller the magnitude of the f_d component. In all cases, (5.3) is satisfied at maximum 25 μs, and the components with the frequency of f_d decays by more than 90% in less than 4 ms. Thus, the proposed method correctly and quickly detects faults with various resistances.

• Scenario 4: This scenario investigates the effect of fault location on the proposed method's performance. To this aim, PP, PPG, and NPG faults with $R_f = 0$, 1, and 200 Ω are simulated at locations $x = 0.1,\ 0.2, \cdots,\ 0.9$ from Bus 5 on Line 5-2. Table 5.2 shows

Table 5.1: Maximum obtained $V^{+}_{FFT,5}$, $V^{+}_{FFT,2}$, $V^{-}_{FFT,5}$, and $V^{-}_{FFT,2}$ during various faults in Scenario 3 (all in volts).

R_f	PPG		NPG		PP			
	$V^{+}_{FFT,5}$	$V^{+}_{FFT,2}$	$V^{-}_{FFT,5}$	$V^{-}_{FFT,2}$	$V^{+}_{FFT,5}$	$V^{+}_{FFT,2}$	$V^{-}_{FFT,5}$	$V^{-}_{FFT,2}$
0	1032.3	855.8	1032.3	855.6	1032.3	855.7	1032.2	855.8
0.1	909.1	773.8	909.1	773.8	965.8	803.2	965.7	803.2
0.5	712.3	651.6	712.4	651.2	812.1	720.1	812.1	720.0
1	578.5	529.6	578.7	529.9	712.4	651.6	712.4	651.6
5	209.4	187.4	209.4	187.4	352.9	318.8	352.9	318.7
10	115.1	101.9	115.2	101.9	209.4	187.4	209.4	187.4
20	60.8	52.9	60.9	52.9	115.1	101.9	115.1	101.9
50	25.6	21.5	25.7	21.5	49.3	42.5	49.4	42.5
100	13.5	10.9	13.4	10.9	25.6	21.5	25.7	21.6
150	9.4	9.4	9.4	7.5	17.6	14.4	17.6	14.4
200	7.3	7.3	7.3	7.0	13.4	10.9	13.5	10.9

Table 5.2: Maximum obtained $V^{+}_{FFT,5}$ during PPG and PP faults, and captured $V^{-}_{FFT,5}$ during NPG faults of Scenario 4 (all in volts).

x	PPG			NPG			PP		
	0Ω	1Ω	200Ω	0Ω	1Ω	200Ω	0Ω	1Ω	200Ω
0.1	1467.0	637.4	9.2	1466.4	637.1	9.2	1466.7	813.8	16.9
0.2	1343.3	617.8	8.2	1343.1	617.6	8.2	1343.2	766.6	15.3
0.3	1181.7	603.9	7.8	1181.5	603.7	7.8	1181.6	737.4	14.4
0.4	1051.2	582.9	7.3	1051.0	582.8	7.3	1051.1	718.1	13.5
0.5	936.4	554.3	7.3	936.5	555.1	6.9	936.4	681.5	12.7
0.6	845.9	527.7	6.5	846.0	527.7	6.5	846.0	649.2	12.0
0.7	770.3	506.5	6.4	771.0	506.6	6.4	770.5	649.2	12.0
0.8	770.3	490.8	6.5	708.0	491.0	6.5	707.8	649.2	12.4
0.9	684.8	506.7	7.3	685.2	508.5	7.3	685.0	624.7	14.4

($V^{+}_{FFT,5}$)s obtained during PPG and PP faults, and ($V^{-}_{FFT,5}$)s captured during NPG faults. For a certain R_f, the farther the fault location to the POC, the smaller the magnitude of the f_d component; however, the obtained magnitudes in all cases exceed their associated thresholds in less than 25 μs, indicating that the proposed method correctly and timely detects faults with various resistances at different locations. Figs. 5.13a and 5.13b show $V^{+}_{FFT,5}$ during PP and PPG faults with $R_f = 200\ \Omega$ and 1 Ω, respectively.

• Scenario 5: This scenario investigates the effect of the proposed method on VSCs' transients. To this aim, a bolted fault is simulated at $x = 0.1$ from Bus 5, i.e., a fault that results in a very high current from Bus 5's VSC. Fig. 5.14a shows the current of this

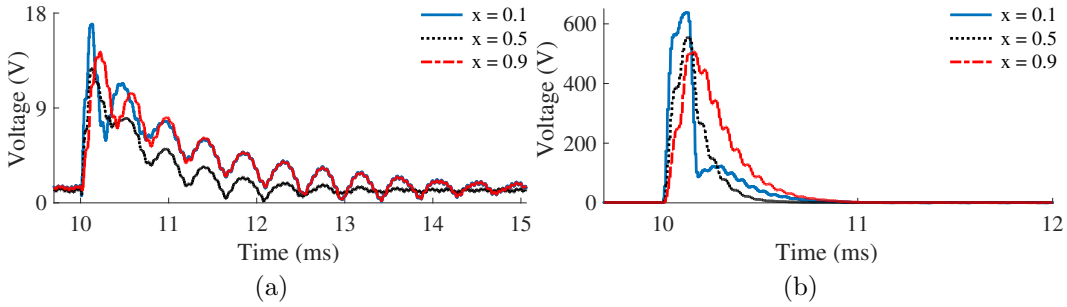


Figure 5.13: $V^{+}_{FFT,5}$ during (a) PP faults with $R_f = 200\ \Omega$, (b) PPG faults with $R_f = 1\ \Omega$.

VSC, with and without addition of POCs: the peak current is decreased by 30.7 kA after installing POCs, which is equivalent to 39% reduction in the maximum fault current, and the rise time becomes almost half. This happens due to the inductive behavior of POCs in frequencies lower than f_0. Thus, the POCs significantly reduce the risk of damaging IGBTs. Moreover, the proposed method does not affect the fault current, after the transient period is passed. To better evaluate the proposed method's effect on the VSC's peak current, Table 5.3 shows the peak current during PP($R_f = 0\ \Omega$) and NPG($R_f = 1\ \Omega$) faults at different locations, with and without installing POCs. This table also shows the reduction in the peak current after installing POCs. For both fault types, the higher the current, the more reduction in the peak current would happen. Additionally, in all cases, the peak current has been reduced, resulting in less damage to the system during faults. On the other hand, Fig. 5.14b shows the VSC's voltage during a bolted PP fault at $x = 0.1$. This fault results in the maximum difference between voltage of Bus 5's VSC in cases of with and without installing POCs. The VSC's voltage when POCs are installed undershoots 500 v more and settles down 4 ms later compared to when POCs are not utilized. However, this is not an issue since the voltage during faults is lower than the nominal voltage.

• Scenario 6: As explained in Section 5.1.1, converters filter transients happening due to a change in loads or generations. Thus, POCs do not resonate during events that occur on the other side of interfacing converters. This scenario investigates the performance of the proposed method implemented in LCDRs of Line 5-2 when (i) the generation of the PV installed at Bus 2 (the nearest generation unit to Line 5-2) increases by 25% at time $t = 10$ ms, and (ii) the load installed at Bus 5 (the nearest load to Line 5-2)

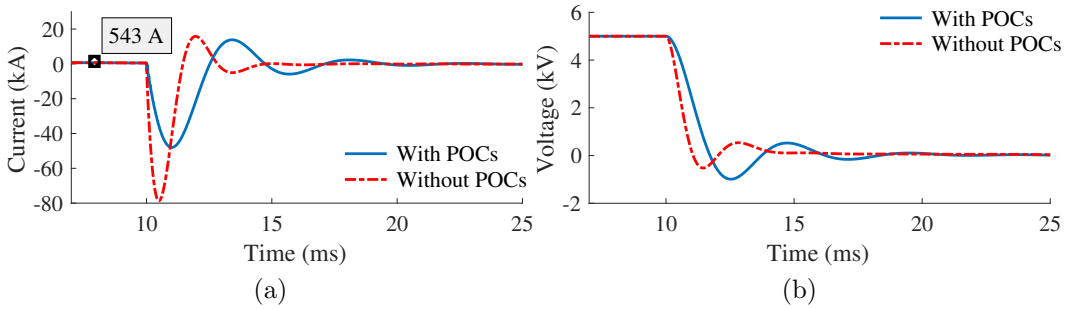


Figure 5.14: Current and voltage of Bus 5's VSC during a bolted PP fault at $x = 0.1$ from Bus 5 on Line 5-2, (a) Positive pole's current (b) voltage.

Table 5.3: Comparison between the peak current of Bus 5's VSC during faults, with and without installing POCs.

x	PP($R_f = 0\ \Omega$)			NPG($R_f = 1\ \Omega$)		
	With POCs (kA)	Without POCs(kA)	Peak reduction(%)	With POCs(kA)	Without POCs(kA)	Peak reduction(%)
0.1	47.99	78.65	-38.99	1.41	1.72	-18.33
0.2	35.27	46.54	-24.22	1.22	1.39	-12.69
0.3	27.50	33.39	-17.65	1.02	1.14	-10.04
0.4	22.61	26.21	-13.75	0.81	0.89	-9.67
0.5	19.19	21.65	-11.37	0.78	0.82	-4.36
0.6	16.74	18.51	-9.57	0.72	0.73	-1.46
0.7	14.79	16.13	-8.31	0.71	0.72	-0.95
0.8	13.23	14.30	-7.49	0.705	0.709	-0.49
0.9	12.00	12.90	-6.95	0.701	0.703	-0.28

increases by 25% at time $t = 30$ ms. Fig 5.15 shows $V^{+}_{FFT,5}$, $V^{-}_{FFT,5}$, $V^{+}_{FFT,2}$, and $V^{-}_{FFT,2}$ during the above-mentioned events: in non of the figures, the captured magnitudes for the component with the frequency of f_d exceed the determined thresholds. Therefore, this scenario confirms that load and generation changes at the other side of converters do not make POCs resonate.

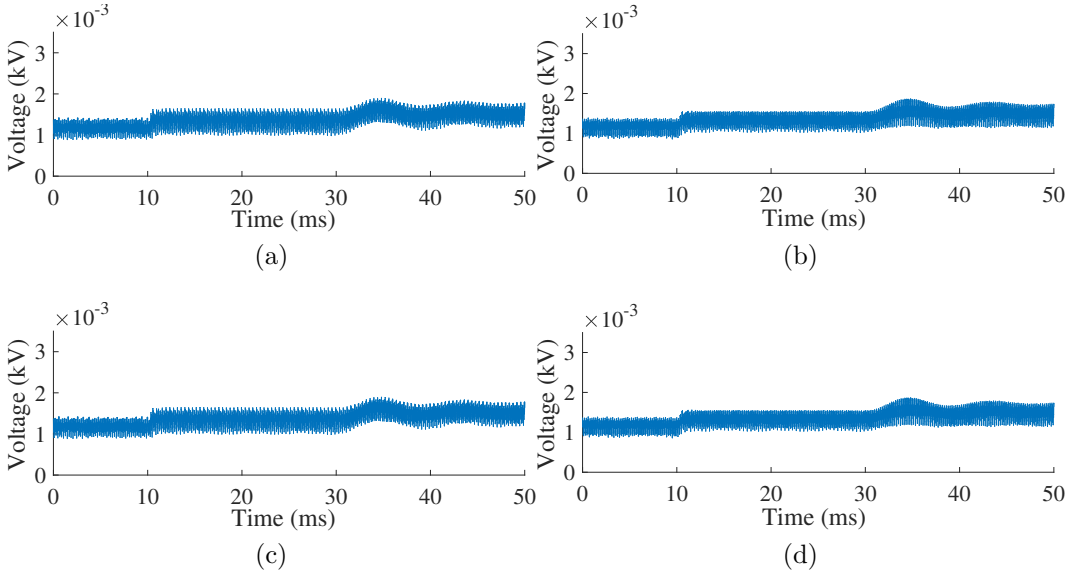


Figure 5.15: Magnitude of frequency component oscillating with f_d in Scenario 6: (a) $V^+_{FFT,5}$, (b) $V^-_{FFT,5}$, (c) $V^+_{FFT,2}$, and (d) $V^-_{FFT,2}$.

5.3 Conclusion

This chapter proposed a method for DC LCDRs to detect cyber-attacks, and to differentiate them from faults. The proposed method installs a POC on each pole in series with each converter. When a fault occurs in the grid, POCs resonate and a generate a sinusoidal damped component with a specific frequency. However, this specific frequency component is not generated by POCs during cyber-attacks, load-changes, and other non-fault events in the system, and thus it can be regarded as a fault signature. On this basis, the proposed attack-detection submodule incorporated in DC LCDRs verify the occurrence of faults by applying FFT to the voltage across POCs and capturing the magnitude of the component oscillating with this specific frequency. Thus, LCDRs' pickup without detecting this specific frequency denotes a cyber-attack. On the other hand, the proposed method cannot be compromised by FDIAs and TSAs, since the proposed method uses only local measurements, which are not attackable. Numerical analysis confirmed that the proposed method is system independent. Other salient features of the proposed method are (i) fast decision time, i.e., less than 25 μs, (ii) sensitivity to faults with resistance up to 200 Ohms, and

(iii) ability to determine fault types. The proposed scheme was tested on a multi-terminal DC system under various fault and cyber-attack scenarios.

Chapter 6

Vulnerability of AGC systems to Cyber-Attacks: Background, Problem Statement, and System Modeling

Chapters 2-4 unveiled a cyber-vulnerability of protection systems and proposed two solutions to address it. This chapter, on the other hand, introduces a vulnerability of control systems in power networks, and discusses its potential consequences.

Today's power grids are highly interconnected through a variety of communication systems for protection, monitoring, and control. One of these communication-dependent functions is that of AGC, which is carried out by the SCADA center [37]. AGC is the secondary controller of the LFC system and the only automatic closed loop between the cyber and physical parts of a power grid [39]. The AGC maintains tie-lines' powers at their scheduled values and regulates grid frequency by adjusting the set-points of a power plant's governors [109]. To calculate these set-points, the control center in each area receives sensor readings, i.e., frequency and tie-line power measurements, using communication systems. The calculated set-points are then sent back to AGCs. Although the AGC is developed for improving the system operation and economy, its dependence on communication in-

frastructure makes power systems susceptible to cyber-attacks.

This chapter first briefly explains the AGC system operating principal and alarms in Section 6.1. Afterwards, Section 6.2 investigates the vulnerability of AGC systems to cyber attacks, and Section 6.3 demonstrates how FDIAs against AGC systems can be destructive. Thus, some basic attacks against the AGC system are introduced, and their impacts on power system operation are studied. Next, Section 6.3.3 formulates and optimizes an SHA to disrupt normal operation of the AGC system *quickly* and *undetectably*. After unveiling the cyber-vulnerability problem of AGC systems, Section 6.4 introduces the LFC system state-space model in normal condition and during attacks. To this end, first the state-space model of the system is obtained for normal conditions. Then, the developed model is modified to represent the attacked system.

6.1 AGC System's Operating Principal and Alarms

Fig. 6.1 shows the AGC system architecture for an area of a power system. As shown in this figure, after receiving measurements, each area's control center forms an Area Control Error (ACE) signal and passes it through controllers, which are usually integrators. The output of the controllers are sent to the power plant as a set-point for governors, every 2 to 4 seconds [36]. The ACE signal of Area i is

$$ACE_i = B_i \Delta\omega_i + \sum_{j \in \delta_i} \Delta P_{tie_{i,j}} \tag{6.1}$$

where B_i and $\Delta\omega_i$ are Area i's frequency bias and angular frequency deviation, respectively; $\Delta P_{tie_{i,j}}$ is the active power deviation of the tie-line that connects areas i and j; and δ_i is the set of areas to which Area i is connected. The ACE signal and system frequency are permanently controlled, and an alarm is raised to notify the operator if:

- The change of frequency during a 15-second rolling time window exceeds a certain threshold, e.g., 0.3 Hz for Quebec in Canada [110].
- The system frequency deviation grows large, e.g., above ± 0.1 Hz [111].

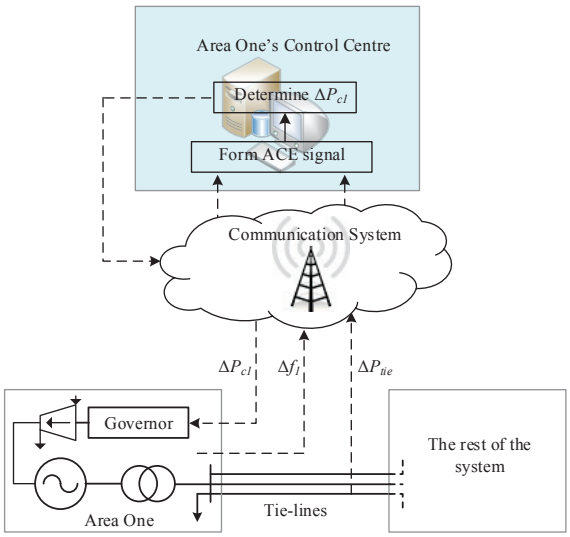


Figure 6.1: AGC system architecture.

- The ACE signal exceeds a predefined threshold, e.g., 0.05 p.u. [2].
- The ACE signal does not return to around zero within 10 minutes [36].
- The average of the ACE signal during 10-minute periods of each hour exceeds a specific limit, e.g., $5+0.025\Delta L$, where ΔL is the greatest hourly change in the area's load during its maximum summer or winter peak load [36].

6.2 Attack Model and Analysis

To regulate a system's frequency and tie-lines' power, an AGC receives measurements using communication system, through Distributed Network Protocol Version 3.0 (DNP3). This protocol is a part of IEC-60870-5 [112] and is widely deployed by North American electric utilities [113]. The dependence of the AGC on communication, however, makes the LFC system vulnerable to cyber-attacks [114]. Additionally, DNP3 vulnerabilities to cyber-attacks have been demonstrated in various studies [113, 115, 116].

AGC systems can be targeted by FDIAs and other types of intrusion such as denial-of-service, malware injection, spoofing, and insider attacks [37]. Although all of these attacks can impact AGC operation, FDIAs are more destructive, since an FDIA injects incorrect control or wrong measurements into the AGC data stream to cause undesired operation of this controller. Consequently, FDIAs can directly affect the frequency, stability, and economic operation of the grid [37].

6.2.1 Attackers' Motives and Objectives

As explained before, AGC is the secondary LFC loop with the additional objective of economic dispatch [36]. This controller operates in a closed automated loop and greatly depends on communication infrastructure. Since this controller directly adjusts the output power of generators, it can affect the stability of the system and its economic operation. Some of the objectives for an attacker to target AGC systems are as follows:

1. Creating frequency instability in the system.
2. Affecting power market by congesting some of the lines.
3. Gaining financial benefit by affecting power markets.
4. Causing financial loss for power networks by decreasing frequency such that under-frequency load shedding scheme operates.
5. Satisfying curiosity/building reputation, e.g., to increase the attacker's reputation in the hackers community

This section focuses on the first objective and shows that targeting AGC can lead to achieving such an objective.

6.2.2 Assumptions and Attackers' Capabilities and Constraints

This dissertation considers the following resource constraints and capabilities for attackers who are aiming to achieve any of the above objectives by targeting AGC systems:

1. Attackers cannot physically trip generators or initiate under-frequency load shedding scheme. Without this constraint, it is a trivial exercise to trigger cascading failures across the power grid.

2. Only some of the generators in each area are controlled by AGC.

3. An attacker's resources are restricted, so only the AGC system of one of the areas can be targeted.

4. Attackers can only tamper with remote frequency and tie-line power measurements by intruding into the communication links or breaking into substations networks.

5. System data including loads, generation, and configuration are available for attackers. Additionally, an attacker has knowledge about AGC alarms and settings. Selecting the optimal attack strategy is dependent on accessing this information.

6.3 FDIAs against AGC Systems

The following investigates the effect of FDIAs on AGC systems. All simulations for the entire section are carried out using MATLAB/Simulink on a three-area power system (Fig. 6.2), whose specifications are given in Appendix C

6.3.1 Over-/under-compensation attacks

During these attacks, the deviation of frequency and tie-line powers from their nominal values are multiplied by an ACE multiplier m before being sent to the control center. Therefore, ACE_i in (6.1) changes to $m_i \times ACE_i$, where $m_i > 1$ and $0 \leqslant m_i < 1$ result in over- and under-compensation attacks, respectively.

To investigate the behavior of frequency and ACE signal during over-/under-compensation attacks, assume that the mismatch between the load and generation of Area i in an N-area power system is ΔP_{L_i}, and B_1 to B_N are the frequency biases of Areas 1 to N. Under

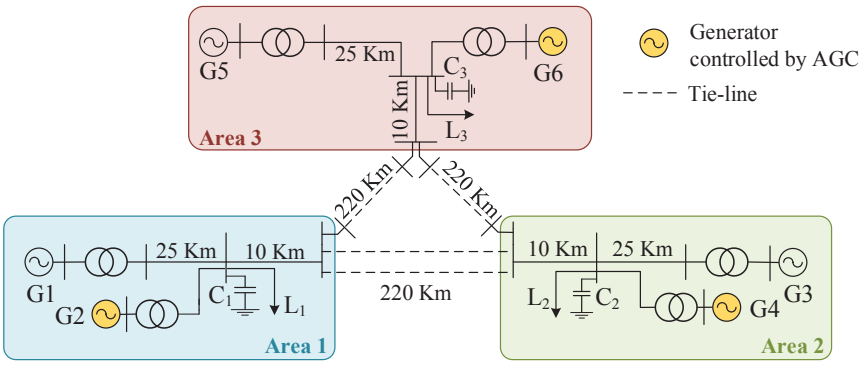


Figure 6.2: Single-line diagram of the three-area test system.

attack-free conditions, the angular frequency and tie-line power deviations in Area i are [109]:

$$\Delta\omega_i = \frac{-\Delta P_{L_i}}{\sum_{j=1}^{N} B_j} \tag{6.2a}$$

$$\Delta P_{tie_{ij}} = B_j \Delta\omega_i \qquad j \in \delta_i \tag{6.2b}$$

If the load changes by ΔP_{L_i} in Area i at time step k, substituting $\Delta\omega_i$ and $\Delta P_{tie_{ij}}$ from (6.2) into (6.1) results in $ACE_i = \Delta P_{L_i}$ for Area i, and zero for other areas' ACE signal [109]. Therefore, Area i's AGC system changes the generation of Area i by $-ACE_i^k$ in order to restore the frequency and tie-line power deviations to zero. However, if an over-/under-compensation attack initiates, ACE_i^k changes to $m_i \times ACE_i^k = m_i \Delta P_{L_i}$. As a result, the generation in Area i changes by $-m_i \Delta P_{L_i}$, instead of $-\Delta P_{L_i}$. Consequently, the mismatch between load and generation becomes $(1 - m_i)\Delta P_{L_i}$. In the next time step, the new ACE_i equals $ACE_i^{k+1} = (1-m_i)\Delta P_{L_i}$ before the attacker injects new false measurements. However, after manipulating the measurements by over-/under-compensation attacks, the ACE signal becomes $m_i(1-m_i)\Delta P_{L_i}$. Therefore, the AGC operation changes the generation by $-m_i(1-m_i)\Delta P_{L_i}$, resulting in $(1-m_i)^2 \Delta P_{L_i}$ mismatch between the load and generation.

The above trend continues in subsequent time steps. The results have been summarized in Table 6.1. As seen in this table, the over-compensation attack makes the frequency oscillate, and the under-compensation attack causes the AGC system to work asymptotically

(by decreasing the AGC operation speed). Therefore, over-/under-compensation attacks negatively affect the frequency and the AGC's normal operation.

Table 6.1: Area i's Frequency Deviation and ACE Signal During Over-/Under-/Negative-Compensation Attacks

Time step	ACE_i during attack	$(\Delta P_{L_i} - \Delta P_{G_i})$ after AGC operation	Frequency deviation from nominal value
k	$m_i \times ACE_i^k$	$(1-m_i)\Delta P_{L_i}$	$-\frac{(1-m_i)\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$
$k+1$	$m_i(1-m_i)ACE_i^k$	$(1-m_i)^2\Delta P_{L_i}$	$-\frac{(1-m_i)^2\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k+\eta$	$m_i(1-m_i)^{\eta-1}ACE_i^k$	$(1-m_i)^{\eta}\Delta P_{L_i}$	$-\frac{(1-m_i)^{\eta}\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$

The frequency deviations during over-/under-compensation attacks with $m_1 = 0.5, 2$ and 1 (i.e., no attack) are shown in Fig. 6.3. The attack targets Area 1 at $t = 30$ s and continues until $t = 100$ s. Fig. 6.4 displays the ACE signal of Area 1, which is normalized based on the active power rating of the generator in this area. As shown in Figs. 6.3 and 6.4, under-compensation FDIAs do not change the frequency and ACE signal noticeably because they improve the system's operation in the same direction as normal AGC operation does, but less effectively. In contrast, over-compensation FDIAs make the frequency and ACE_1 oscillate largely. When the load changes during an over-compensation attack, the AGC system alters the generation set-points m times more than needed, so deteriorates the frequency deviations. However, the risk of this attack being detected is high, since the ACE changes noticeably.

6.3.2 Negative-compensation attacks

These attacks resemble over-/under-compensation attacks, but the ACE multiplier m is a negative number. Substituting a negative m_i in Table 6.1 indicates that such attacks amplify the expected effect of the AGC on power system operation, but in the reverse direction. Additionally, smaller values of m_i impact frequency profoundly over a shorter time. These attacks can either increase or decrease system frequency, depending on the ACE_i^k,

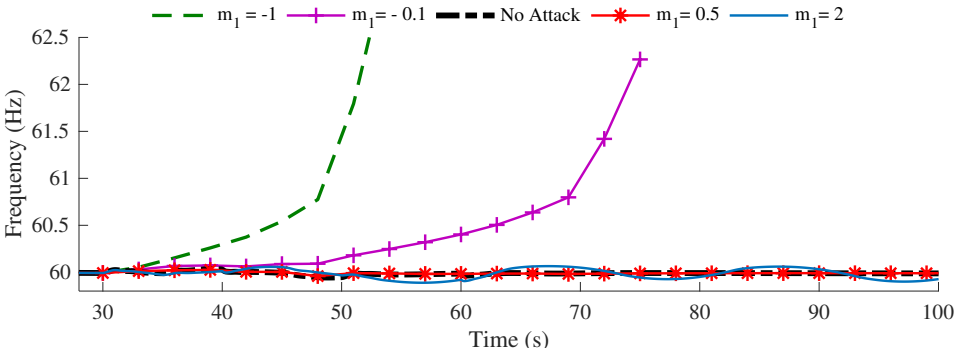


Figure 6.3: System frequency during over-/under-/negative-compensation attacks.

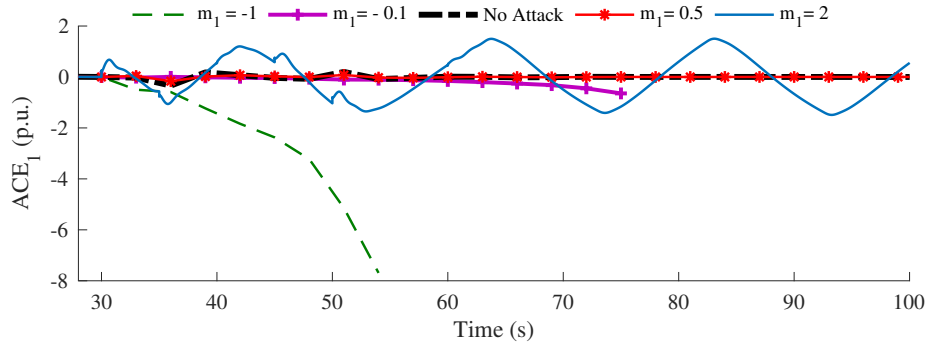


Figure 6.4: ACE signal of Area 1 during over-/under-/negative-compensation attacks.

or equivalently ΔP_{L_i}, at the attack's start time. For example, if a negative-compensation attack targets Area 1's AGC after a load-increase (-decrease) in Area 1, the frequency drops (grows), and ACE_1^k becomes positive (negative).

Fig. 6.3 shows frequency deviations during negative-compensation attacks with $m_1 = -0.1$ and -1. These attacks target Area 1 after this area's load decreases. In both attacks, frequency increases such that the over-frequency elements of a generators protective relay, discussed in [117], trip the generators. During these FDIAs, the primary frequency control, i.e., the governor, does not help in recovering the frequency, because the governor receives erroneous set-points from the attacked AGC system. In fact, FDIAs effectively shift the droop characteristic of a governor up or down to affect frequency regulation negatively. Thus, not only does the governor fail to regulate the frequency when an AGC is attacked,

but also makes the frequency deviate from its nominal value by trying to follow erroneous set-points.

As seen in Fig 6.3, during negative-compensation attacks, different values of m_1 change the frequency at different rates, i.e, the smaller m_1 is in a negative-compensation attack, the faster the system becomes unstable. However, as Fig. 6.4 shows, a smaller m_1 increases the absolute value of the ACE signal more than a bigger m_1, which is undesirable from detectability viewpoint. Thus, greater values of m_1, e.g., -0.1, can change the frequency to an extent that frequency relays operate, while $|ACE_1|$ is small.

6.3.3 Formulation of an SHA

The SHA presented next can target AGC systems destructively and undetectably, by combining under- and negative-compensation through an optimization process. Instead of a constant ACE multiplier m, an SHA utilizes a time-variant multiplier m_i^{k+s} (attack starts at time step k, and $k+s$ indicates the s-th time-step after its start time). An SHA takes into account the physical characteristics of the LFC system and existing alarms in the control center in order to damage the system as fast as possible without being detected. An SHA is able to either increase or decrease the frequency, depending on the ACE signal value at the attack's start time, and consequently can trigger the over-/under-frequency elements of protective relays. To compute the optimal m_i^{k+s}, an attacker must have access to the values of frequency bias B and the AGC controller's gain. Both parameters can be estimated by intruding into the communication system and using the frequency and tie-line power measurements sent to the control center, and the set-points sent to the generators.

Considering the detection alarms discussed in Section 6.1, the multiplier m_i^{k+s} during an SHA should be determined for all $s \in \{1, \cdots, \eta\}$ such that

(i) the ACE signal does not exceed its maximum permissible value, $ACE_{\max}$, i.e.,

$$-ACE_{\max} \leqslant ACE_i^{k+s} \leqslant ACE_{\max} \tag{6.3}$$

Table 6.2: Area i's ACE and frequency deviation during an SHA

Time step	ACE_i after manipulation	Frequency deviation (Δf_i)
k	$m_i^k \times ACE_i^k$	$-\frac{(1-m_i^k)\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$
$k+1$	$m_i^{k+1}(1-m_i^k)ACE_i^k$	$-\frac{(1-m_i^k)(1-m_i^{k+1})\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$
$k+2$	$m_i^{k+2}\prod_{j=k}^{k+1}(1-m_i^j)ACE_i^k$	$\prod_{j=k}^{k+2}(1-m_i^j)\frac{-\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$
$\vdots$	$\vdots$	$\vdots$
$k+\eta$	$m_i^{k+\eta}\prod_{j=k}^{k+\eta-1}(1-m_i^j)ACE_i^k$	$\prod_{j=k}^{k+\eta}(1-m_i^j)\frac{-\Delta P_{L_i}}{\sum_{j=1}^{N} B_j}$

(ii) the ACE signal rate of change does not overstep a certain threshold, λ, i.e.,

$$\left|\frac{ACE_i^{k+s} - ACE_i^{k+s-1}}{T_{AGC}}\right| \leqslant \lambda \tag{6.4}$$

where T_{AGC} is the interval between two successive operations of the AGC, and λ is the maximum permissible ACE curve's slope.

(iii) the frequency deviation sent to the control center remains within an acceptable range, i.e.,

$$-\Delta f_{\max} < m_i^{k+s}\Delta f_i^{k+s} < \Delta f_{\max} \tag{6.5}$$

where $\Delta f_{\max}$ is the maximum frequency deviation that does not raise an alarm.

(iv) the rate of change of the received frequency does not overstep a certain threshold, that is,

$$\left|\frac{m_i^{k+s}\Delta f_i^{k+s} - m_i^{k+s+1}\Delta f_i^{k+s+1}}{T_{AGC}}\right| \leqslant \gamma \tag{6.6}$$

where γ is the maximum permissible slope of the frequency curve.

(v) the frequency approaches the attacker's target frequency, Δf^*, at the end of the attack:

$$\Delta f_i^{k+\eta} = \Delta f^* \tag{6.7}$$

Satisfying conditions (i) to (v) during an SHA guarantees attack's stealth while the attacker's desired frequency is reached. However, to carry out the attack in the shortest possible time, the SHA must be formulated as an optimization problem to find the optimal attack multipliers. To this end, Table 6.1 is modified for the case of using time-variant multipliers m_i^{k+s}, so Table 6.2 is obtained. Using this table, an SHA against Area i of an N-area system can be formulated as the following optimization problem that minimizes the attack duration:

$$\begin{cases} \underset{m_i^k, m_i^{k+1}, \cdots, m_i^{k+\eta}}{\text{minimize}} \ \eta \\ \text{subject to: (i) to (v)} \end{cases} \tag{6.8}$$

where η is the required number of time steps for the attack, which is a function of m_i^k to $m_i^{k+\eta}$, and k represents the time step at which the attack starts. To formulate conditions (i) to (v) using attack multipliers during the attack, these conditions are represented using the results in Table 6.2. Condition (i) is rewritten by substituting ACE_i from the middle column of Table 6.2 at each time step in (6.3), resulting in

$$\left| m_i^{k+s} \prod_{j=k}^{k+s-1} \left(1 - m_i^j\right) ACE_i^k \right| \leq ACE_{\max} \qquad s \in \{1, 2, \cdots, \eta\} \tag{6.9}$$

With the same procedure, condition (ii) is formulated as

$$\left| m_i^{k+s} \prod_{j=k}^{k+s-1} \left(1 - m_i^j\right) - m_i^{k+s-1} \prod_{j=k}^{k+s-2} \left(1 - m_i^j\right) \right| \leq \frac{\lambda T_{AGC}}{\left|ACE_i^k\right|} \qquad s \in \{2, \cdots, \eta\} \tag{6.10}$$

Additionally, given that ACE_i^k before the attack equals ΔP_{L_i}, condition (iii) can be rewritten by substituting Δf_i from the third column of Table 6.2 at each time step in (6.5), i.e.,

$$\left| m_i^{k+s} \prod_{j=k}^{k+s} \left(1 - m_i^j\right) \right| \leq \frac{\Delta f_{max} \sum_{j=1}^{N} B_j}{\left|ACE_i^k\right|} \qquad s \in \{1, 2, \cdots, \eta\} \tag{6.11}$$

Similarly, condition (iv) can be represented by

$$\left| m_i^{k+s} \prod_{j=k}^{k+s} \left(1 - m_i^j\right) - m_i^{k+s+1} \prod_{j=k}^{k+s+1} \left(1 - m_i^j\right) \right| \leq \frac{\gamma T_{AGC} \sum_{j=1}^{N} B_j}{\left| ACE_i^k \right|} \qquad s \in \{1, 2, \cdots, \eta\} \tag{6.12}$$

Finally, condition (v) in (2.20) can be rewritten using the third column of Table 6.2 as

$$\prod_{j=k}^{k+\eta} \left(1 - m_i^j\right) = \frac{\Delta f^* \sum_{j=1}^{N} B_j}{\left| ACE_i^k \right|} \tag{6.13}$$

To simulate the proposed SHA for Area 1 of the three-area test system, $\text{ACE}_{\max}$, T_{AGC}, λ, $\Delta f_{\max}$, and γ are considered to be 0.05 p.u., 2 s, 0.02 p.u./s, 0.1 Hz, and 0.05 Hz/s, respectively [36, 2, 111, 110]. The attack starts after a 0.1 p.u. load increase in Area 1. The target frequency for the end of this attack is set to 62 Hz. Fig. 6.5 illustrates the real and manipulated frequencies of Area 1 after being targeted by the proposed SHA: deviation of the frequency received by the control center from 60 Hz is acceptable, but the real frequency of the system is growing noticeably. This figure also illustrates the real and manipulated system frequencies if the attack starts after a 0.1 p.u. load decrease in Area 1, and the target frequency at the end of the attack is set to 59 Hz. During this attack, the frequency decreases, initiating load-shedding schemes. The ACE of Area 1 during the SHA that increases the frequency is shown in Fig. 6.6: the ACE does not exceed the defined $\text{ACE}_{\max}$ at any time, and its rate of change also is controlled. Therefore, no alarm is raised and the SHA remains undetected.

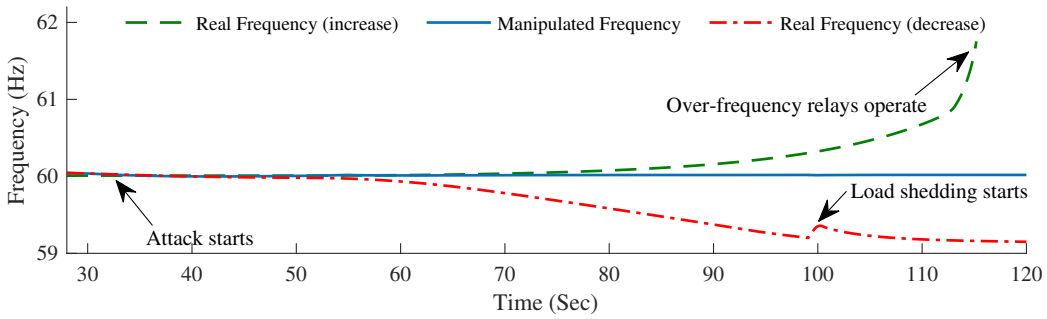


Figure 6.5: The real and manipulated frequencies during an SHA.

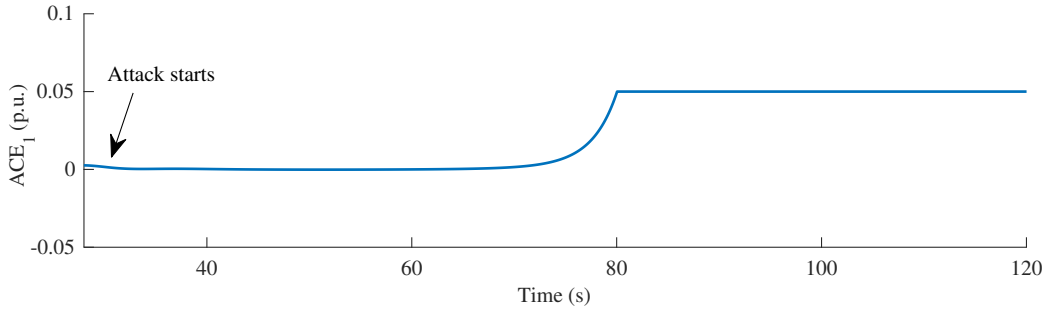


Figure 6.6: ACE signal of Area 1 during an SHA that increase the frequency.

6.4 LFC System Modeling

An AGC system deals with relatively small disturbances [118]. Therefore, for LFC studies, each area of a power network can be represented by a linear model comprised of an equivalent rotating mass, governors, turbines, and the AGC system. Additionally, the LFC control loop can be decoupled from the AVR loop, since the AVR system's time constants are appreciably smaller than the LFC system's. Thus, it is possible to consider only the steady-state operating point of the AVR [119]. Therefore, a linearized model decoupled from voltage dynamics can be used to detect and identify FDIAs targeting LFC systems (Fig. 6.7). This model is sufficiently accurate for LFC studies [36, 109].

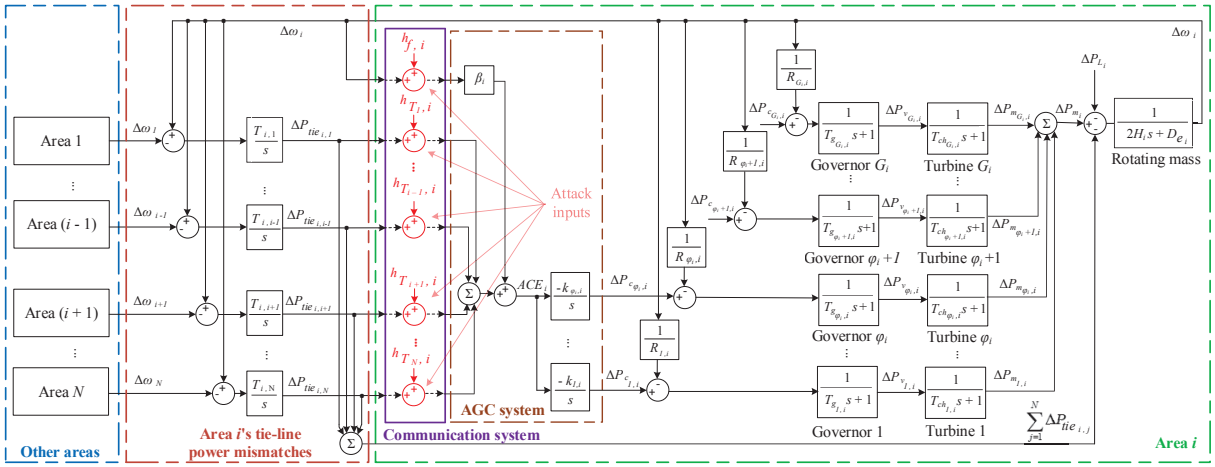


Figure 6.7: Linearized model of LFC system for area i.

6.4.1 The State-Space Model of an N-Area LFC System During Normal Condition

This section first presents the continuous LFC system model for each area during attack-free conditions, and then it combines the LFC models of all areas to form the state-space model of the N-area system. Afterwards, the developed model is modified to incorporate noise. Finally, the continuous models are discretized to accommodate numerical implementation.

The continuous model of the system

The LFC system in each area can be represented by an equivalent linear model shown in Fig. 6.7 [36, 109]. In this figure, G_i generators are committed in Area i, among which generators 1 to Φ_i are controlled by the AGC. The load-frequency dynamic For Area i is as follows [36]:

$$\Delta\dot{\omega}_i = \frac{1}{2H_i}\left(\Delta P_{m_i} - \Delta P_{tie_i} - \Delta P_{L_i} - D_{e_i}\Delta\omega_i\right) \tag{6.14}$$

where $\Delta\dot{\omega}_i$ is the derivative of $\Delta\omega_i$ with respect to time; ΔP_{L_i}, $\Delta\omega_i$, H_i and D_{e_i} are Area i's load change, angular frequency deviation, equivalent inertia constant, and equivalent damping coefficient, respectively; and ΔP_{tie_i} and ΔP_{m_i} are the sum of Area i's tie-lines'

power and generators' mechanical power deviations, respectively, defined as

$$\Delta P_{tie_i} = \sum_{j \in \delta_i} \Delta P_{tie_{i,j}} \tag{6.15}$$

$$\Delta P_{m_i} = \sum_{g=1}^{G_i} \Delta P_{m_{g,i}} \tag{6.16}$$

where $\Delta P_{m_{g,i}}$ is the mechanical power deviation of the g-th generator in Area i, and $\Delta P_{tie_{i,j}}$ is the power deviation of the tie-line connecting Areas i and j. The power flow dynamic of this tie-line is

$$\Delta \dot{P}_{tie_{i,j}} = T_{ij} \left(\Delta \omega_i - \Delta \omega_j \right) \tag{6.17}$$

where T_{ij} is the synchronizing power coefficient between areas i and j. Tie-lines can be either modeled in the state-space equation separately, or as the sum of all tie-line powers.

To restore the frequency to its nominal value, each generator's governor adjusts its turbine's valve position $\Delta P_{v_{g,i}}$ by sensing $\Delta \omega_i$ and power generation set points $\Delta P_{c_{g,i}}$ using the following equation:

$$\Delta \dot{P}_{v_{g,i}} = -\frac{1}{T_{g_{g,i}}} \left(\frac{1}{R_{g,i}} \Delta \omega_i + \Delta P_{v_{g,i}} - \Delta P_{c_{g,i}} \right) \tag{6.18}$$

where $T_{g_{g,i}}$ and $R_{g,i}$ signify the droop coefficient and the governor's time constant of the g-th generator. Adjusting $\Delta P_{v_{g,i}}$ controls the mechanical power by regulating the steam flowing into its turbine. The g-th generator's turbine dynamic can be modeled by

$$\Delta \dot{P}_{m_{g,i}} = -\frac{1}{T_{ch_{g,i}}} \Delta P_{m_{g,i}} + \frac{1}{T_{ch_{g,i}}} \Delta P_{v_{g,i}} \tag{6.19}$$

where $T_{ch_{g,i}}$ is the turbine's time constant of generator g. Meanwhile, assuming that the g-th generator is equipped with an AGC, its governor's $\Delta P_{c_{g,i}}$ is tuned by the AGC to make the generator's mechanical power track the load changes ΔP_{L_i}, and so tie-lines power and the frequency are regulated. The AGC integrator block receives ACE_i as its input and its

dynamic can be expressed by

$$\Delta \dot{P}_{c_{\phi,i}} = -k_{\phi,i} \times ACE_i \tag{6.20}$$

where $k_{\phi,i}$ is the ϕ-th AGC's gain. The formation of the ACE_i was shown (6.1), in which the frequency bias is

$$B_i = D_{e_i} + \sum_{j=1}^{G_i} \frac{1}{R_{g,i}} \tag{6.21}$$

However, if a generator is not controlled by an AGC, its governor set-point, $\Delta P_{c_{g,i}}$, is a known input to the system.

To find the state-space model of Area i, the following parameters are selected as this area's states: $\Delta\omega_i$, ΔP_{tie_i}, $\Delta P_{m_{g,i}}$ and $\Delta P_{v_{g,i}}$ for all generators, and $\Delta P_{c_{g,i}}$ for generators that are controlled by the AGC system. Instead of using ΔP_{tie_i}, it is also possible to consider each tie-line power as a system state individually. The system's known inputs are $\Delta P_{c_{g,i}}$ for all generators that are controlled manually. ΔP_{L_i} is the unknown input for Area i. As an example, considering ΔP_{tie_i} as a system state, the state-space equation of Area 1 of the three-area power system introduced in Appendix I is given by

$$\dot{\mathbb{X}}_1(t) = \mathbb{A}_{11}\mathbb{X}_1(t) + \mathbb{B}_{u,1}\mathbb{U}_{u,1}(t) + \mathbb{B}_{n,1}\mathbb{U}_{n,1}(t) + \sum_{j=2,3} \mathbb{A}_{1j}\mathbb{X}_j(t) \tag{6.22}$$

In the above equation, $\mathbb{U}_{u,1}(t)$ and $\mathbb{U}_{n,1}(t)$ are the unknown and known inputs of Area 1, which are ΔP_{L_1} and $\Delta P_{c_{1,1}}$, respectively. Additionally, all the elements of $\mathbb{A}_{1j} \in \mathbb{R}^{7\times 7}$ are zero, except the element at row 1 and column 2, which is $-T_{1j}$. This element is multiplied by $\Delta\omega_j$. The other parameters in (6.22) are

$$\mathbb{X}_1 = [\Delta P_{tie_1}\ \Delta\omega_1\ \Delta P_{m_{1,1}}\ \Delta P_{m_{2,1}}\ \Delta P_{v_{1,1}}\ \Delta P_{v_{2,1}}\ \Delta P_{c_{2,1}}]^T \tag{6.23a}$$

$$\mathbb{B}_{u,1} = \begin{bmatrix} 0 & \frac{-1}{2H_1} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{6.23b}$$

$$\mathbb{B}_{n,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & \frac{1}{T_{g_{1,1}}} & 0 & 0 \end{bmatrix}^T \tag{6.23c}$$

$$\mathbb{A}_{11} = \begin{bmatrix} 0 & \sum_{j\in\delta_i} T_{ij} & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{2H_1} & \frac{-D_{e_1}}{2H_1} & \frac{1}{2H_1} & \frac{1}{2H_1} & 0 & 0 & 0 \\ 0 & 0 & \frac{-1}{T_{ch_{1,1}}} & 0 & \frac{1}{T_{ch_{1,1}}} & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_{ch_{2,1}}} & 0 & \frac{1}{T_{ch_{2,1}}} & 0 \\ 0 & \frac{-1}{R_{1,1}T_{g_{1,1}}} & 0 & 0 & \frac{-1}{T_{g_{1,1}}} & 0 & 0 \\ 0 & \frac{-1}{R_{2,1}T_{g_{2,1}}} & 0 & 0 & 0 & \frac{-1}{T_{g_{2,1}}} & \frac{1}{T_{g_{2,1}}} \\ -k_1 & -k_1B_1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{6.23d}$$

As seen in (6.23), other areas' state variables are involved in Area 1's state-space model. These variables are received by the communication system to form the ACE_1.

In addition to the state-space equation of (6.22), the output equation of each area must be determined. Each system output is a physical measurable quantity that can be modeled by a linear combination of system states and inputs. For example, the outputs of each area can be considered as $\Delta P_{c_{g,i}}$ for generators that are controlled by the AGC, $\Delta\omega_i$, and ΔP_{tie_i}. These states are all related to the AGC system and are already available in control centers. Using these parameters, Area 1's output equation in the three-area test system is as follows

$$\mathbb{Y}_i(t) = \mathbb{C}_i\mathbb{X}_i(t) \tag{6.24}$$

where $\mathbb{Y}_i(t)$ is the output vector of Area i, and $\mathbb{C}_i$ is the output matrix relating the state and output vectors. For example, for the three-area test system, $\mathbb{C}_1$ matrix for Area 1 is

$$\mathbb{C}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{6.25}$$

In the case of modeling each tie-line power individually as a system state, all tie-line powers can be considered as system outputs as well.

Using matrices $\mathbb{A}_{ii}$, $\mathbb{A}_{ij}$, $\mathbb{B}_{n,i}$, $\mathbb{B}_{u,i}$, and $\mathbb{C}_i$ and vectors $\mathbb{X}_i$, $\mathbb{U}_{u,i}$, and $\mathbb{U}_{n,i}$ in (6.22), (6.23) and (6.24) for all areas $i \in \{1, \cdots N\}$, the state-space model of an N-area power system in

the absence of FDIAs can be obtained using [120]:

$$\dot{\mathbb{X}}(t) = \mathbb{A}_c \mathbb{X}(t) + \mathbb{B}_{c,u} \mathbb{U}_u(t) + \mathbb{B}_{c,n} \mathbb{U}_n(t) \tag{6.26a}$$

$$\mathbb{Y}(t) = \mathbb{C}\mathbb{X}(t) \tag{6.26b}$$

in which $\mathbb{X}(t) \in \mathbb{R}^n$ and $\mathbb{Y}(t) \in \mathbb{R}^p$ are the state and output vectors, defined as

$$\mathbb{X} = \begin{bmatrix} \mathbb{X}_1^T & \mathbb{X}_2^T & \dots & \mathbb{X}_N^T \end{bmatrix}^T \tag{6.27a}$$

$$\mathbb{Y} = \begin{bmatrix} \mathbb{Y}_1^T & \mathbb{Y}_2^T & \dots & \mathbb{Y}_N^T \end{bmatrix}^T \tag{6.27b}$$

Moreover, $\mathbb{U}_u(t) \in \mathbb{R}^N$ and $\mathbb{U}_n(t) \in \mathbb{R}^m$ in (6.26) represent the unknown and known input vector, which include all areas' load-change and the governor set-points of all manually controlled generators, respectively, and are expressed by

$$\mathbb{U}_u = \begin{bmatrix} \Delta P_{L_1} & \Delta P_{L_2} & \dots & \Delta P_{L_N} \end{bmatrix}^T \tag{6.28a}$$

$$\mathbb{U}_n = \begin{bmatrix} \Delta P_{c_{1,1}} \cdots \Delta P_{c_{\psi_1,1}} \cdots \Delta P_{c_{1,N}} \cdots \Delta P_{c_{\Phi_N,N}} \end{bmatrix}^T \tag{6.28b}$$

where Φ_i represents the number of generators controlled by AGC systems in area i. Other parameters in (6.26), i.e., $\mathbb{A}_c \in \mathbb{R}^{n\times n}$, $\mathbb{B}_{c,u} \in \mathbb{R}^{n\times N}$, $\mathbb{B}_{c,n} \in \mathbb{R}^{n\times m}$, and $\mathbb{C} \in \mathbb{R}^{p\times n}$ are the state, unknown input, known input, and output matrices, defined as follows

$$\mathbb{A}_c = \begin{bmatrix} \mathbb{A}_{11} & \mathbb{A}_{12} & \dots & \mathbb{A}_{1N} \\ \mathbb{A}_{21} & \mathbb{A}_{22} & \dots & \mathbb{A}_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{A}_{N1} & \mathbb{A}_{N2} & \cdots & \mathbb{A}_{NN} \end{bmatrix} \tag{6.29a}$$

$$\mathbb{B}_{c,u} = diag \begin{bmatrix} \mathbb{B}_{u,1} & \mathbb{B}_{u,2} & \cdots & \mathbb{B}_{u,N} \end{bmatrix} \tag{6.29b}$$

$$\mathbb{B}_{c,n} = diag \begin{bmatrix} \mathbb{B}_{n,1} & \mathbb{B}_{n,2} & \cdots & \mathbb{B}_{n,N} \end{bmatrix} \tag{6.29c}$$

$$\mathbb{C} = diag \begin{bmatrix} \mathbb{C}_1 & \mathbb{C}_2 & \cdots & \mathbb{C}_N \end{bmatrix} \tag{6.29d}$$

To take into account the effect of noise, the process and measurement noise vectors—which are zero-mean, independent, white, and Gaussian—are added to the system model. Thus, the state-space representation of an N-area power system in the presence of Noise is given by

$$\dot{\mathbb{X}}(t) = \mathbb{A}_c \mathbb{X}(t) + \mathbb{B}_{c,u} \mathbb{U}_u(t) + \mathbb{B}_{c,n} \mathbb{U}_n(t) + \mathbb{W}_c(t) \tag{6.30a}$$

$$\mathbb{Y}(t) = \mathbb{C}\mathbb{X}(t) + \mathbb{V}_c(t) \tag{6.30b}$$

where $\mathbb{W}_c(t) \in \mathbb{R}^n$ and $\mathbb{V}_c(t) \in \mathbb{R}^p$ are the noise vectors with covariance matrices $\mathbb{Q}_c(t) \in \mathbb{R}^{n \times n}$ and $\mathbb{R}_c(t) \in \mathbb{R}^{p \times p}$, respectively. The covariance matrices $\mathbb{Q}_c(t)$ and $\mathbb{R}_c(t)$ indicate how the elements of $\mathbb{W}_c(t)$ and $\mathbb{V}_c(t)$ are correlated with each other and how they are spread around their mean values. Therefore, they are required for modeling noise.

Discretization of the Continuous Model

For implementation using digital computers, matrices $\mathbb{A}_c$, $\mathbb{B}_{c,u}$ and $\mathbb{B}_{c,n}$ in (6.26) and (6.30) are discretized using

$$\mathbb{A} = e^{\mathbb{A}_c \times T_s} \tag{6.31a}$$

$$\mathbb{B}_u = \int_{\tau=0}^{T_s} e^{\mathbb{A}_c \times \tau} \mathbb{B}_{c,u} d\tau \tag{6.31b}$$

$$\mathbb{B}_n = \int_{\tau=0}^{T_s} e^{\mathbb{A}_c \times \tau} \mathbb{B}_{c,n} d\tau \tag{6.31c}$$

where T_s is the discretization time step [79]. Thus, using (6.26) and (6.31), the discretized model of an N-area power system in the absence of FDIAs and noise is

$$\mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \mathbb{B}_u \mathbb{U}_u[k] + \mathbb{B}_n \mathbb{U}_n[k] \tag{6.32a}$$

$$\mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] \tag{6.32b}$$

where $\mathbb{X}[k] \in \mathbb{R}^n$, $\mathbb{U}_u[k] \in \mathbb{R}^N$, $\mathbb{U}_n[k] \in \mathbb{R}^m$, and $\mathbb{Y}[k] \in \mathbb{R}^p$ are the state, unknown input, known input, and output vectors at time step k, respectively. Similarly, discretization of (6.30) using (6.31) results in

$$\mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \mathbb{B}_u \mathbb{U}_u[k] + \mathbb{B}_n \mathbb{U}_n[k] + \mathbb{W}[k] \tag{6.33a}$$

$$\mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] + \mathbb{V}[k] \tag{6.33b}$$

where $\mathbb{W}[k]$ and $\mathbb{V}[k]$ are noise vectors at time step k, whose covariance matrices $\mathbb{Q}[k]$ and $\mathbb{R}[k]$ are obtained by discretizing $\mathbb{Q}_c(t)$ and $\mathbb{R}_c(t)$.

In the rest of this thesis, (6.32) and (6.33) are used for representing the LFC system model in the absence and presence of noise during normal conditions.

6.4.2 The State-Space Model of an *N*-Area LFC system during FDIAs

In this section, FDIAs against the frequency and tie-line power measurements are modeled by adding appropriate attack inputs to the LFC system, as shown in Fig. 6.7. These inputs are represented by $h_{T_1,i}$ to $h_{T_N,i}$ for tie-line power measurements of Area i, and by $h_{f,i}$ for frequency measurements. When the AGC system is targeted, attack inputs $h_{T_1,i}$ to $h_{T_N,i}$, and $h_{f,i}$ are no longer zero, thus the ACE_i is affected. The addition of these inputs changes (6.20) into

$$\Delta\dot{P}_{\mathbb{C}_{\phi,i}} = -k_i \underbrace{\left(B_i \Delta\omega_i + \sum_{j\in\delta_i} \Delta P_{tie_{i,j}} + B_i h_{f,i} + \sum_{j\in\delta_i} h_{T_j,i} \right)}_{ACE_i \text{ during FDIAs}} \tag{6.34}$$

Since only AGC measurements can be targeted in LFC systems, all other state equations in (6.14)-(6.19) remain unchanged. Using (6.34) and (6.14)-(6.19), Area i during an FDIA can be modeled by

$$\dot{\mathbb{X}}_i(t) = \mathbb{A}_{ii}\mathbb{X}_i(t) + \mathbb{B}_{u,i}\mathbb{U}_{u,i}(t) + \mathbb{B}_{n,i}\mathbb{U}_{n,i}(t) + \sum_{j\in\delta_i} \mathbb{A}_{ij}\mathbb{X}_j(t) + \mathbb{B}_{hc,i}\mathbb{H}_i(t) \tag{6.35}$$

where $\mathbb{H}_i(t)$ is the attack vector expressed by

$$\mathbb{H}_i(t) = \begin{bmatrix} h_{T_1,i} & h_{T_2,i} & \cdots & h_{T_N,i} & h_{f,i} \end{bmatrix}^T \tag{6.36}$$

and $\mathbb{B}_{hc,i}$ is the attack matrix that relates the attack vector to the states. For example, for

the three-area test system, $\mathbb{B}_{hc,1}$ is

$$\mathbb{B}_{hc,1} = \begin{bmatrix} 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \\ -k_1 & -k_1 & -k_1 B_1 \end{bmatrix} \tag{6.37}$$

Meanwhile, the output equation during an FDIA remains unchanged, as in (6.26b) or (6.30b) depending on noise being modeled or not. If noise is not considered, the addition of $\mathbb{B}_{hc,i}\mathbb{H}_i(t)$ to (6.26a) during an FDIA changes this equation to

$$\dot{\mathbb{X}}(t) = \mathbb{A}_c\mathbb{X}(t) + \mathbb{B}_{c,u}\mathbb{U}_u(t) + \mathbb{B}_{c,n}\mathbb{U}_n(t) + \mathbb{B}_{hc}\mathbb{H}(t) \tag{6.38}$$

where $\mathbb{B}_{hc} \in \mathbb{R}^{n\times z}$ and $\mathbb{H} \in \mathbb{R}^{z}$ are the attack matrix and vector, defined as follows:

$$\mathbb{B}_{hc} = diag\begin{bmatrix} \mathbb{B}_{hc,1} & \mathbb{B}_{hc,2} & \cdots & \mathbb{B}_{hc,N} \end{bmatrix} \tag{6.39a}$$

$$\mathbb{H}(t) = \begin{bmatrix} \mathbb{H}_1^T(t) & \mathbb{H}_2^T(t) & \cdots & \mathbb{H}_N^T(t) \end{bmatrix}^T \tag{6.39b}$$

To find the discretized system model during attacks, (6.38) should be discretized. The discretization of $\mathbb{A}_c$, $\mathbb{B}_{c,n}$, and $\mathbb{B}_{c,u}$ was already explained in (6.31), and $\mathbb{B}_{hc}$ can be discretized by substituting it with $\mathbb{B}_{c,u}$ in (6.31b), resulting in $\mathbb{B}_h$. Therefore, using (6.38), (6.31), and (6.30b), the discretized state equation of an N-area power system without considering noise in the presence of FDIAs can be expressed by

$$\mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \mathbb{B}_u\mathbb{U}_u[k] + \mathbb{B}_n\mathbb{U}_n[k] + \mathbb{B}_h\mathbb{H}[k] \tag{6.40a}$$

$$\mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] \tag{6.40b}$$

With the same procedure, the discretized state equation of an N-area power system in the presence of noise and FDIAs can be expressed by

$$\mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \mathbb{B}_u\mathbb{U}_u[k] + \mathbb{B}_n\mathbb{U}_n[k] + \mathbb{B}_h\mathbb{H}[k] + \mathbb{W}[k] \tag{6.41a}$$

$$\mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] + \mathbb{V}[k] \tag{6.41b}$$

In the rest of this thesis, (6.40) and (6.41) are used for representing the LFC system model during FDIAs in the absence and presence of noise, respectively.

6.5 Conclusion

This chapter first briefly explained the AGC system operating principal and alarms. Additionally, it investigated vulnerabilities of AGC systems to cyber attacks, and demonstrated how FDIAs against AGC systems can be destructive. On this basis, some basic attacks against the AGC system were introduced, and their impacts on power system operation were studied. Afterwards, an SHA was formulated and optimized to disrupt the normal operation of AGC systems quickly and undetectably. This chapter also introduced the LFC system state-space model in normal condition and during attacks.

Chapter 7

Attack Detection and Identification for Automatic Generation Control Systems

Chapter 6 unveiled the vulnerability of AGC systems to cyber attacks and showed how FDIAs against this controller can endanger the integrity of the entire system. To address this problem, this chapter proposes an anomaly-based attack-detection and -identification method for protecting the AGC system against cyber vulnerabilities. The proposed method in this chapter does not consider the effect of noise, and can be implemented within control-center computing facilities to check the authenticity of frequency and tie-line power measurements sent to the AGC system, before they are used for control purposes. To detect attacks, the proposed method estimates the LFC system's states using a UIO and remote frequency and tie-line power measurements, and calculates the UIO's RF. A discrepancy between the RFs and a predefined threshold signifies an FDIA. The proposed method also utilizes different identification UIOs to determine the attack type, i.e., which system parameter(s) is (are) targeted by the attack.

The proposed method can run in parallel with network-based techniques, such as encryption techniques, which use a system's cyber characteristics and constitute the first layer of security. However, encryption methods are not sufficient to ensure cyber-security

for all conditions, and their vulnerabilities have been demonstrated in various publications [121, 122, 123]. Additionally, if attackers circumvent encryption and intrude into the system, these methods are unable to detect malicious activities. Thus, the proposed method works differently from encryption techniques, since the latter reduce attack likelihood by preventing illegitimate users from entering the system, while the former detects attacks if they pass through the first layer of security.

This chapter first develops a UIO for LFC systems in Section 7.1. Afterwards, Section 7.2 discusses the proposed attack-detection and -identification schemes for AGC systems. Section 7.3 then evaluates the performance of the proposed method using simulation results for a three-area power system and the 39-bus New England network. Finally, Section 7.4 concludes this chapter.

7.1 Development of a UIO for LFC Systems

This section uses a UIO, which was previously introduced in Section 3.2, for estimating the states of the LFC system based on (6.32). As explained before, a UIO estimates a system's states without requiring its unknown inputs, using only the system outputs and initial states [80, 124]. Therefore, as the real-time load is not normally available in power systems, UIOs are appropriate tools for estimating the states of the LFC system. Moreover, as will be shown in Section 7.2.2, this independence from inputs makes a UIO useful for attack identification, thus facilitating attack mitigation.

The design procedure for the UIO is similar to what explained in Section 3.2, but with some minor modifications. This section thus explains only the modifications. To develop a UIO for (6.32), the system outputs given by this equation for the duration of the UIO's window, i.e., from k to $k+\alpha$, should be organized in matrix form, as follows

$$\mathcal{Y}[k:k+\alpha] = \mathcal{O}_\alpha \mathbb{X}[k] + \mathcal{J}_{n,\alpha}\mathcal{U}_n[k:k+\alpha] + \mathcal{J}_{u,\alpha}\mathcal{U}_u[k:k+\alpha] \tag{7.1}$$

In this relation,

$$\mathcal{Y}[k:k+\alpha] = \begin{bmatrix} \mathbb{Y}[k]^T & \mathbb{Y}[k+1]^T & \cdots & \mathbb{Y}[k+\alpha]^T \end{bmatrix}^T \tag{7.2a}$$

$$\mathcal{O}_\alpha = \begin{bmatrix} \mathbb{C}^T & (\mathbb{C}\mathbb{A})^T & \cdots & (\mathbb{C}\mathbb{A}^\alpha)^T \end{bmatrix}^T \tag{7.2b}$$

$$\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{p\times N} & O_{p\times N} & \cdots & O_{p\times N} \\ \mathbb{C}\mathbb{B}_u & O_{p\times N} & \cdots & O_{p\times N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \cdots & O_{p\times N} \end{bmatrix} \tag{7.2c}$$

$$\mathcal{J}_{n,\alpha} = \begin{bmatrix} O_{p\times m} & O_{p\times m} & \cdots & O_{p\times m} \\ \mathbb{C}\mathbb{B}_n & O_{p\times m} & \cdots & O_{p\times m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_n & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_n & \cdots & O_{p\times m} \end{bmatrix} \tag{7.2d}$$

$$\mathcal{U}_u\left[k:k+\alpha\right] = \begin{bmatrix} \mathbb{U}_u\left[k\right]^T & \mathbb{U}_u\left[k+1\right]^T & \cdots & \mathbb{U}_u\left[k+\alpha\right]^T \end{bmatrix}^T \tag{7.2e}$$

$$\mathcal{U}_n\left[k:k+\alpha\right] = \begin{bmatrix} \mathbb{U}_n\left[k\right]^T & \mathbb{U}_n\left[k+1\right]^T & \cdots & \mathbb{U}_n\left[k+\alpha\right]^T \end{bmatrix}^T \tag{7.2f}$$

The UIO's equation is selected as in (3.8). Therefore, the UIO's error for LFC systems, i.e., $e\left[k+1\right] = \hat{\mathbb{X}}[k+1] - \mathbb{X}[k+1]$, is as follows:

$$e\left[k+1\right] = \underbrace{\left(\mathbb{A} - \mathcal{L}\mathcal{O}_\alpha\right)}_{\mathbb{A}'} e\left[k\right] + \mathcal{L}\mathcal{J}_{u,\alpha}\mathcal{U}_u\left[k:k+\alpha\right] - \mathbb{B}_u\mathbb{U}_u\left[k\right] \tag{7.3}$$

As a result, the explained accuracy condition in Section 3.2.1 is met for LFC systems and $e\left[k+1\right]$ approaches zero if the last two terms on the right side of (7.3) cancel out each other, i.e.,

$$\mathcal{L}\mathcal{J}_{u,\alpha} = \begin{bmatrix} \mathbb{B}_u & O_{n\times N} & \cdots & O_{n\times N} \end{bmatrix} \tag{7.4}$$

Theorem 4 showed that there is an $\mathcal{L}$ that satisfies (7.4) if (7.5) is satisfied [81].

$$rank\left(\mathcal{J}_{u,\alpha}\right) - rank\left(\mathcal{J}_{u,\alpha-1}\right) = N \tag{7.5}$$

In (7.5), $\mathcal{J}_{u,\alpha-1}$ is obtained using $\mathcal{J}_{u,\alpha}$ in (7.2c) and is as follows:

$$\mathcal{J}_{u,\alpha-1} = \begin{bmatrix} O_{p\times N} & O_{p\times N} & \cdots & O_{p\times N} \\ \mathbb{C}\mathbb{B}_u & O_{p\times N} & \cdots & O_{p\times N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_u & \cdots & O_{p\times N} \end{bmatrix} \tag{7.6}$$

Theorem 4. *There is a matrix $\mathcal{L}$ that satisfies (3.11) if and only if (3.12) is satisfied.* □

Proof. The proof is similar to the proof of Theorem 1 in Section 3.2.1. ■

Equation (7.5) indicates a necessary condition for developing a UIO for an LFC system. In other words, if this condition is not met, it will not be possible to estimate the states of a system without requiring its unknown inputs.

Theorem 5. *Regardless of the number of areas and generators under AGC control in each area, an LFC system satisfies condition (7.5), therefore the system is invertible/observable and its states can be estimated by a UIO.* □

Proof. The proof is presented in Appendix D. ■

As shown in Appendix D, $\alpha = 2$ satisfies condition (7.5) for LFC systems. Additionally, as Theorem 2 proved, an $\mathcal{L}$ in the following form satisfies (7.4):

$$\mathcal{L} = [\mathcal{L}_1 \quad \mathcal{L}_2] \times \mathcal{Q} \tag{7.7}$$

in which $\mathcal{L}_2 = \mathbb{B}_u$, $\mathcal{L}_1$ is a free $n \times (\alpha - 1)N$ matrix from the perspective of the UIO's error, and $\mathcal{Q}$ is an $\alpha N \times (\alpha + 1)p$ matrix that satisfies

$$\mathcal{Q}\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{(\alpha-1)N\times N} & O_{(\alpha-1)N\times \alpha N} \\ I_{N\times N} & O_{N\times \alpha N} \end{bmatrix} \tag{7.8}$$

As explained in Section 3.2.2, $\mathcal{L}_1$ can be used to stabilize the UIO. Substituting $\mathcal{L}$ from (7.7) into $\mathbb{A}'$ in (7.3) and decomposing $\mathcal{Q}\mathcal{O}_\alpha$ into two sub-matrices S_1 and S_2, with $(\alpha-1)N$

and N rows, respectively, result in

$$\mathbb{A}' = (\mathbb{A} - \mathbb{B}_u S_2) - \mathcal{L}_1 S_1 \tag{7.9}$$

As proven in [85], there is an $\mathcal{L}_1$ that satisfies this condition and stabilizes the eigenvalues of (2.22) if

$$rank \begin{pmatrix} \mathbb{A} - zI_n & \mathbb{B}_u \\ \mathbb{C} & 0 \end{pmatrix} = n + N, \quad \forall z \in \mathcal{C}, \, |z| \geqslant 1 \tag{7.10}$$

in which $\mathcal{C}$ is the set of all complex numbers.

Theorem 6. *Regardless of the number of areas and generators under AGC control in each area, the condition given by (7.10) is satisfied for the state-space equation of LFC systems, given in (6.40), when $\alpha = 2$.* □

Proof. The proof is very similar to the proof of Theorem 3. ■

Therefore, there exists an $\mathcal{L}_1$ that stabilizes the UIO. The procedure for designing such an $\mathcal{L}_1$ is explained in Section 3.2.2. Once $\mathcal{L}_1$ is designed, the UIO's gain is available and, and the system states can be estimated.

7.2 Proposed Detection and Identification Schemes

7.2.1 Attack Detection Scheme

As shown in Section 6.4.2, during an FDIA, a new terms is added to the system model in (6.32), resulting in (6.40). The addition of this terms adds a new term to the system outputs, $\mathcal{Y}_{k:k+\alpha}$ in (7.1):

$$\tilde{\mathcal{Y}}\left[k : k+\alpha\right] = \mathcal{Y}\left[k : k+\alpha\right] + \mathcal{M}_\alpha \mathcal{H}\left[k : k+\alpha\right] \tag{7.11}$$

where $\tilde{\mathcal{Y}}\left[k : k+\alpha\right]$ is the system outputs vector under an FDIA, and $\mathcal{H}\left[k : k+\alpha\right]$ and $\mathcal{M}_\alpha$ are

$$\mathcal{H}\left[k : k+\alpha\right] = \begin{bmatrix} \mathbb{H}\left[k\right]^T & \mathbb{H}\left[k+1\right]^T & \cdots & \mathbb{H}\left[k+\alpha\right]^T \end{bmatrix}^T \tag{7.12a}$$

$$\mathcal{M}_\alpha = \begin{bmatrix} O_{p\times z} & O_{p\times z} & \cdots & O_{p\times z} & O_{p\times z} \\ \mathbb{C}\mathbb{B}_h & O_{p\times z} & \cdots & O_{p\times z} & O_{p\times z} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_h & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_h & \cdots & O_{p\times z} & O_{p\times z} \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_h & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_h & \cdots & \mathbb{C}\mathbb{B}_h & O_{p\times z} \end{bmatrix} \tag{7.12b}$$

If no attack occurs, all elements of $\mathcal{H}\left[k:k+\alpha\right]$ are zero, and so $\mathcal{Y}\left[k:k+\alpha\right]$ and $\tilde{\mathcal{Y}}\left[k:k+\alpha\right]$ become equal. However, during FDIAs, these two matrices differ. As $\mathcal{L}$ is designed according to (7.4) such that $\mathcal{L}\mathcal{J}_{u,\alpha}\mathcal{U}_u\left[k:k+\alpha\right] - \mathbb{B}_u\mathbb{U}_u\left[k\right] = 0$, the UIO's error during FDIAs changes from (7.3) to

$$e\left[k+1\right] = \mathbb{A}'e\left[k\right] + \mathcal{L}\mathcal{M}_\alpha\mathcal{H}\left[k:k+\alpha\right] - \mathbb{B}_h\mathbb{H}\left[k\right] \tag{7.13}$$

It is evident from (7.13) that a UIO's error deviates from zero in the event of an FDIA, resulting in inaccurate state estimation. This inaccuracy can be used for detecting attacks by defining the following RF:

$$r\left[k\right] = \mathbb{Y}\left[k\right] - \mathbb{C}\hat{\mathbb{X}}\left[k\right] \tag{7.14}$$

where $\mathbb{Y}\left[k\right]$ is the measured outputs of the system, represented by (6.32b). Therefore, By substituting $\mathbb{Y}\left[k\right]$ into (7.14), $r\left[k\right]$ is equal to $\mathbb{C}e\left[k\right]$, which approaches zero in the absence of FDIAs. However, $r\left[k\right]$ grows during FDIAs due to the addition of non-zero terms $\mathcal{L}\mathcal{M}_\alpha\mathcal{H}\left[k:k+\alpha\right]$ and $\mathbb{B}_h\mathbb{H}\left[k\right]$ to $r\left[k\right]$. Therefore, attacks can be detected by monitoring the RF and comparing it with a predefined threshold, tr^*. In other words, an attack has occurred if

$$\left\|r\left[k\right]\right\| > tr^* \tag{7.15}$$

where tr^* is the detection threshold, which is a unit-less number, and operator $||.||$ determines the norm of vectors. This threshold should be found so as to minimize false attack-detection during non-attack conditions, e.g., existence of noise, load changes, and system disturbances. The procedure for determining this threshold will be explained in Section 7.3.

In the rest of this chapter, the UIO designed based on (6.32), (7.14), and (7.15) is called the *Main UIO* and is used for detecting FDIAs against AGC systems.

7.2.2 Type Identification Scheme

The method presented in Section 7.2.1 can only detect FDIAs, not identify their types. Identification helps to mitigate attacks more quickly by indicating which sensor measurements have been targeted. To identify attacks, possible attack types and their corresponding distribution matrix $\mathbb{B}_h$ should be determined, as per Section 6.4.2. Then, assuming that z is the number of possible attacks targeting the system, z separate type-identification UIOs should be designed using (6.40). Each UIO is associated with one of the attack inputs of $\mathbb{H}[k]$, and is designed based the following equation

$$\begin{cases} \mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + [\mathbb{B}_u \quad \mathbb{B}_h^{-j}] \begin{bmatrix} \mathbb{U}_u[k] \\ \mathbb{H}^{-j}[k] \end{bmatrix} + \mathbb{B}_n \mathbb{U}_n[k] \\ \mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] \end{cases} \tag{7.16}$$

where $\mathbb{B}_h^{-j}$ is an $n \times (z-1)$ matrix that includes all columns of $\mathbb{B}_h$ except the j-th one, and $\mathbb{H}^{-j}[k]$ is a $(z-1) \times 1$ vector that comprises all elements of $\mathbb{H}[k]$ except the j-th one. The input vector $\left[\mathbb{U}_u[k]^T \quad (\mathbb{H}^{-j}[k])^T\right]^T$ in (7.16) is unknown. Designing the j-th UIO yields a UIO that is insensitive to all attacks associated with $\mathbb{H}[k]$, except the j-th attack. Therefore, if any attack associated with $\mathbb{H}^{-j}[k]$ happens, the j-th UIO's RF does not increase since such attacks and their impacts on the system are modeled in the j-th UIO's state-space equations, as shown in (7.16). However, the occurrence of the attack respective to the j-th element of $\mathbb{H}[k]$ increases the j-th UIO's RF, since this UIO is designed based on (7.16), but the system's model during the j-th attack is as shown by

$$\begin{cases} \mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \begin{bmatrix} \mathbb{B}_u & \mathbb{B}_h^{-j} \end{bmatrix} \begin{bmatrix} \mathbb{U}_u[k] \\ \mathbb{H}^{-j}[k] \end{bmatrix} + \mathbb{B}_h^j \mathbb{H}^j[k] + \mathbb{B}_n \mathbb{U}_n[k] \\ \mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] \end{cases} \tag{7.17}$$

in which $\mathbb{B}_h^j$ denotes the j-th column of $\mathbb{B}_h$, respectively, and $\mathbb{H}^j[k]$ denotes the j-th element of $\mathbb{H}[k]$.

In this method, attacks associated with the j-th input of $\mathbb{H}[k]$ are modeled in all identification UIO's except in the j-th UIO. Consequently, if the j-th attack occurs, only

the RF of the j-th UIO increases. Therefore, the j-th attack can be identified if the RF of the Main UIO and the j-th UIO exceed their thresholds, i.e.,

$$\|r\,[k]\| > tr^* \quad and \quad \|r_j\,[k]\| > tr_j^* \tag{7.18}$$

where $r_j\,[k]$ and tr_j^* are the j-th UIO's RF and its threshold.

The designed UIOs are able to identify attacks. However, if any non-attack event—such as a fault—happens, the RFs of all of them increase, since other events are not modeled in these UIOs's state-space equations. Therefore, it is impossible to understand whether all AGC parameters are targeted or a non-attack event is in progress. To address this shortcoming, another UIOs that includes all attack inputs in its model is designed based on the following state-space model:

$$\begin{cases} \mathbb{X}\,[k+1] = \mathbb{A}\mathbb{X}\,[k] + [\mathbb{B}_u \;\; \mathbb{B}_h] \begin{bmatrix} \mathbb{U}_u\,[k] \\ \mathbb{H}\,[k] \end{bmatrix} + \mathbb{B}_n\mathbb{U}_n\,[k] \\ \mathbb{Y}\,[k] = \mathbb{C}\mathbb{X}\,[k] \end{cases} \tag{7.19}$$

Since this UIO includes all possible attack inputs, the RF of this UIO does not increase during attacks. However, if any non-attack event, such as a fault, happens, the RF of this UIO increases.

For example, there are three attack inputs for Area 1 of the three-area power system mentioned in Chapter 6. Thus, three UIOs should be designed for this area, as denoted in Table 7.1 by *UIOs A* to *C*. In this table, $h_{T_2,1}$, $h_{T_3,1}$, and $h_{f,1}$ are attack inputs that represent FDIAs targeting $\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$, and Δf_1, respectively. The state-space equation of each UIO models the attack inputs shown in column 2. Hence, each UIO's model in Table 7.1 includes a combination of FDIAs that can target the parameters presented in column 4. The unknown inputs of each UIO are the attack inputs associated with that UIO as well as the system unknown input vector $\mathbb{U}_u\,[.]$. As a result of this design, when Area 1 is targeted, the RF of *UIO A* does not increase for its respective attacks, since its state-space equation includes those attacks in its model as unknown inputs. In other words, the RF of *UIO A* increases only if the power measurements of the tie-line connecting Areas 1 and 2 are targeted. As a result, if the RFs of the main UIO and *UIO A* increase over their

thresholds, it signifies that measurements associated with $\Delta P_{tie_{1,2}}$ are being manipulated.

Table 7.1: UIOs for Area 1 of the Three-Area Power System

UIO	Considered attack input(s)	unconsidered attack input(s)	Parameters whose attacks are modeled	parameter whose attack is not modeled	Unknown inputs
A	$h_{T_3,1}$, $h_{f,1}$	$h_{T_2,1}$	$\Delta P_{tie_{1,3}}$, Δf_1	$\Delta P_{tie_{1,2}}$	$h_{T_3,1}$, $h_{f,1}$, ΔP_{L_1},$\mathbb{U}_u$
B	$h_{T_2,1}$, $h_{f,1}$	$h_{T_3,1}$	$\Delta P_{tie_{1,2}}$, Δf_1	$\Delta P_{tie_{1,3}}$	$h_{T_2,1}$, $h_{f,1}$, ΔP_{L_1},$\mathbb{U}_u$
C	$h_{T_2,1}$,$h_{T_3,1}$	$h_{f,1}$	$\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$	Δf_1	$h_{T_2,1}$, $h_{T_3,1}$, ΔP_{L_1},$\mathbb{U}_u$
D	$h_{T_2,1}$,$h_{T_3,1}$, $h_{f,1}$	-	$\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$,Δf_1	-	$h_{T_2,1}$, $h_{T_3,1}$, $h_{f,1}$, ΔP_{L_1},$\mathbb{U}_u$

Table 7.2: Identification Logic for Area 1 of The Three-Area Test System

Targeted parameter(s)	RF increase for UIOs			
	A	*B*	*C*	*D*
$h_{T_2,1}$	✓	-	-	-
$h_{T_3,1}$	-	✓	-	-
$h_{f,1}$	-	-	✓	-
$h_{T_2,1}$, $h_{T_3,1}$	✓	✓	-	-
$h_{T_2,1}$, $h_{f,1}$	✓	-	✓	-
$h_{T_3,1}$, $h_{f,1}$	-	✓	✓	-
$h_{T_2,1}$, $h_{T_3,1}$, $h_{f,1}$	✓	✓	✓	-
Other events, such as faults	✓	✓	✓	✓

Using UIOs designed in Table 7.1, attacks are identified according the RF-increase for the UIOs, as indicated in Table 7.2. For example, in Table 7.2, an increase in the RFs of *UIOs B*, *C*, accompanied by less-than-threshold RFs for the rest of the UIOs, indicates that $h_{T_3,1}$ and $h_{f,1}$ are targeted. Similarly, a simultaneous increase in the RFs of *UIOs A* to *C*, while the RF of *UIO D* is less than its threshold, indicates that all three parameters—i.e., $h_{T_2,1}$, $h_{T_3,1}$, and $h_{f,1}$—are targeted. Additionally, as shown in Table 7.2, *UIO D*'s RF does not increase during any attack, since its state-space model includes all possible attacks inputs as unknown inputs. Based on this design, the RF of *UIO D* does not increase during normal conditions or modeled FDIAs. Therefore, any increase in the RF of this UIO signifies other abnormal non-attack events, such as faults.

7.3 Performance evaluation

This section investigates the performance of the proposed method on 39-bus New England and the three-area test systems.

7.3.1 Three-Area Test System

The specifications of this test system is given in Appendix C. There are two generators in each area of this system. Thus, including each tie-line separately in state-space equation, the number of states in each area is 8. Moreover, the number of known and unknown inputs for each area is 1 and 1, and the number of outputs is 4.

As explained in Section 7.2, FDIAs targeting the power and frequency measurements of Area 1 in the test system are modeled by attack inputs $h_{T_2,1}$, $h_{T_3,1}$, and h_{f_1}. Three similar attack inputs are defined for each other areas as well. The AGC system operates every 2 seconds [36]. Before the attacks start, all attack inputs are zero and the ACE signal is calculated as shown in (6.1). However, the attack inputs become non-zero following the attacks' inception, and thus the ACE signal becomes as shown in (6.34). Using the procedure elaborated in Section V-B, four identification UIOs are designed for each area, whose specifications are summarized in Table 7.1.

To detect and identify cyber-attacks, thresholds tr^* and $tr_j^*(j = A, \ldots, D)$ in (7.15) and (7.18) must be found—as explained in Section 7.2—such that false-positive and false-negative alarms are minimized. Load change does not affect these thresholds because they are unknown inputs in all UIOs, and thus their effects are eliminated. Therefore, these thresholds are determined in the presence of process and measurements noise, and parameter uncertainties. In order to consider the effect of noise on LFC systems, (6.41) is used to model noise, which is represented by its mean and covariance. The process noise added to each area's state equations in (6.41) is zero-mean and Gaussian with the covariance matrix of $Cov_1 = 0.03 \times diag\begin{bmatrix} 1 & 1 & 0.03 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$, i.e., the covariance of the noise corresponding to the frequency is 0.009 and the covariance of the noise corresponding to other parameters is 0.03 [125]. Similarly, the measurement noise affecting each area's outputs in (6.41) is zero-mean and Gaussian with the covariance matrix of

$Cov_2 = 0.03 \times diag\begin{bmatrix} 1 & 1 & 0.03 & 1 \end{bmatrix}$ [125]. in addition to load changes and measurement and process noise, parameter uncertainties are also factored in. This uncertainty is modeled for each parameter by a percentage error that is normally distributed around zero, with 5% standard deviation. To obtain the above-mentioned thresholds, the designed UIOs' RFs were recorded for 1000 seconds in the presence of noise and by considering parameter uncertainties during normal condition. The largest recorded RF for each UIO plus a 20% security margin was assigned to the threshold of that UIO. Afterwards, to verify the obtained thresholds, the above-mentioned procedure was repeated two more rounds, each for 1000 seconds. If the obtained thresholds in the test rounds are greater than the initial ones, the initial thresholds are replaced by the larger recorded ones. This procedure was continued until the test rounds verified the obtained thresholds, and resulted in $tr^* = 0.6$ and $tr_j^* = 0.7$. As an example, Fig. 7.1 illustrates the Main UIO's RF with and without noise for 200 seconds: without noise, the Main UIO's RF is zero; however, when measurements are noisy, its RF increases.

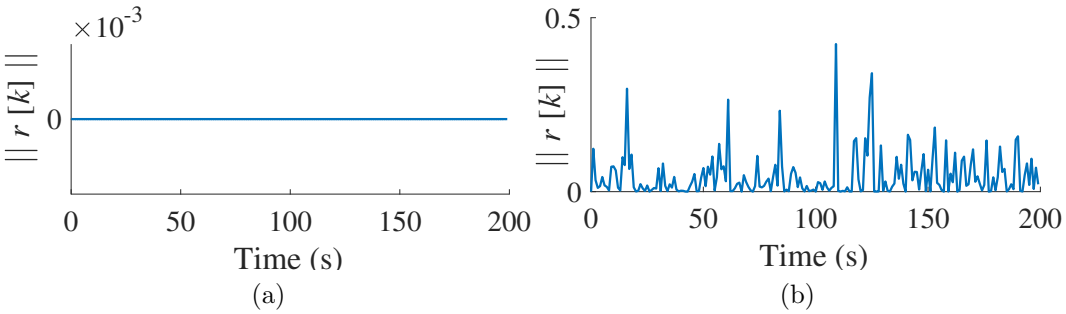


Figure 7.1: Main UIO's RF, (a) Without noise, (b) With noise.

The following scenarios are carried out against Area 1:

• Scenario 1: The SHA introduced in Section 6.3.3 targets the frequency and both tie-line power measurements of Area 1. This attack starts at $t = 30$ s and lasts until $t = 200$ s. The measurements are manipulated such that conditions (6.3)-(6.7) are satisfied. As Fig. 7.2 illustrates, the RFs of all detection and identification UIOs exceed their thresholds since this kind of attack multiplies Δf_1, $\Delta P_{tie_{12}}$, and $\Delta P_{tie_{13}}$ by m_1^k. With a similar pattern to frequency deviations in Fig. 6.5, as the attack starts, the RF of the detection and

identification UIOs increase (with a small rate at the beginning and faster ones afterwards, until they become constant). Therefore, the proposed method correctly identifies that all three measurements for Area 1 are attacked.

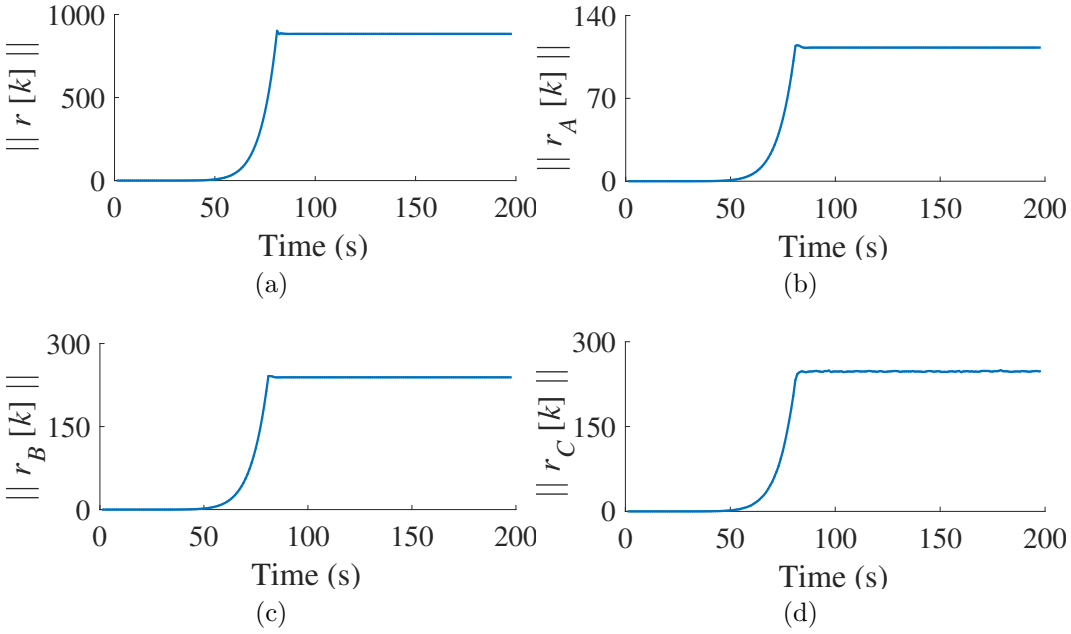


Figure 7.2: Scenario 1's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C.

• Scenario 2: The AGC system is targeted by an over-compensation attack, in which Δf_1, $\Delta P_{tie_{12}}$, and $\Delta P_{tie_{13}}$ are all multiplied by $m_{k,1} = 1.002$. The reason for selecting such a small attack multiplier is to show how small manipulations can affect the main and identification UIOs' RFs. The attack starts at $t = 30$ s and lasts until $t = 200$ s. The results of this scenario are shown in Fig. 7.3: as the attack starts, the RFs of all UIOs exceeds the detection and identification thresholds, signifying that all measurements are manipulated. since the attack multiplier in this scenario is very close to one, the increase in this scenario's RFs is less than in Scenario 1.

• Scenario 3: The measured frequency is manipulated and decreased by 0.12 Hz between $t = 30$ and $t = 120$ s. Fig. 7.4 shows the RFs of the Main UIO, as well as UIOs A, B, and C for this scenario: the RFs of the Main UIO and UIO C surpass their thresholds during

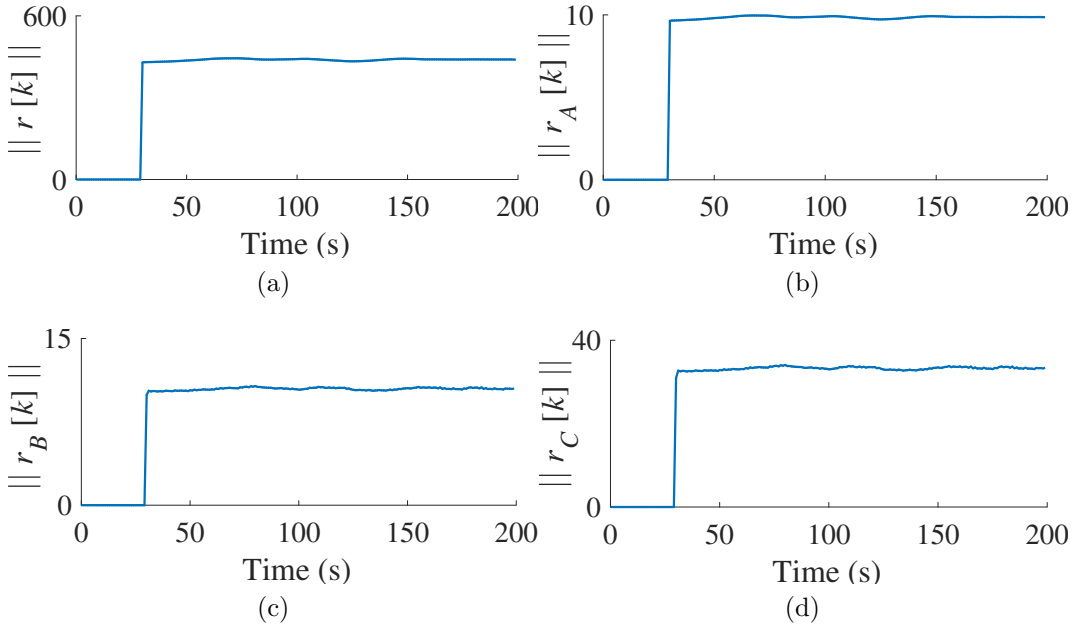


Figure 7.3: Scenario 2's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C.

this interval, signifying that frequency measurements are targeted. In addition, the RFs of UIOs A and B do not increase, as their corresponding attacks are inactive.

• Scenario 4: The attacks corresponding to UIOs A and B are active, and each tie-line power measurement is increased by 5% during $30 \leqslant t \leqslant 120$ s. Fig. 7.5 shows that the RFs of the Main UIO as well as UIOs A and B exceed their thresholds during the attack, but the RF of UIO C remains small, as its corresponding attack is inactive. As a result, the proposed scheme is able to detect and identify FDIAs and also determine their start and end times.

7.3.2 39-Bus New England Test System

This section evaluates the performance of the proposed method using 39-bus New England system, whose specifications can be found in Appendix A. The generators that are controlled by AGC and the tie-lines between the three areas of this system are shown in Fig. 7.6. For each area, governor and turbine time constants as well as droop and damping

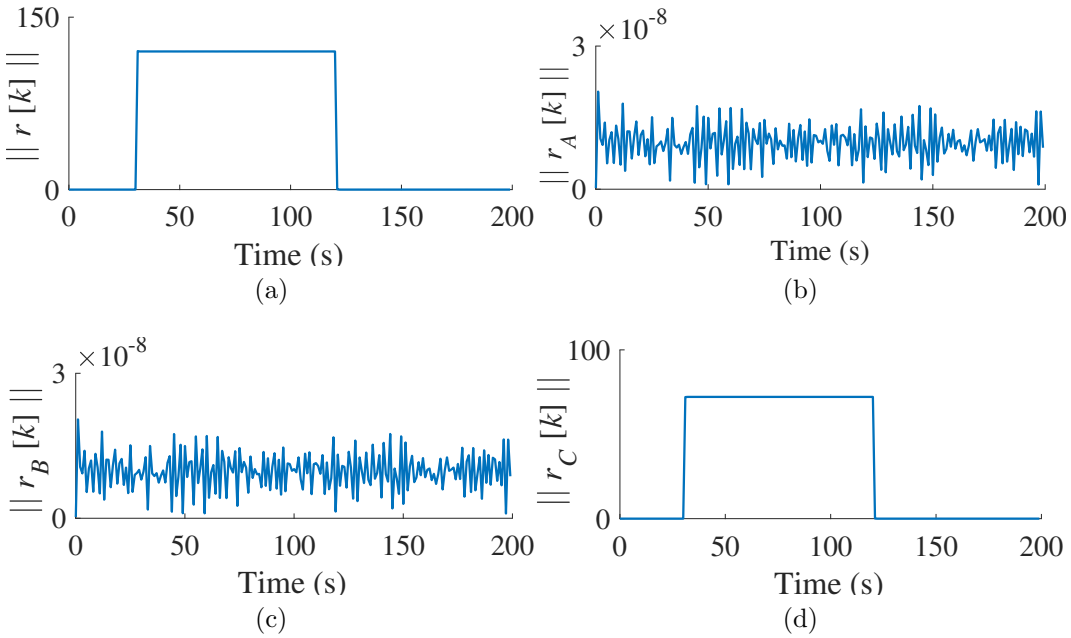


Figure 7.4: Scenario 3's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C.

coefficients have been considered similar to those of the three-area test system (Table C.2). Additionally, the same protective relays as in the three-area system with the same settings have been used for the 39-bus New England network as well.

Areas 1, 2, and 3 include 3, 6, and 1 generators, resulting in 13, 23, and 7 states for these areas, respectively. The number of unknown inputs for each area is 1, which is that area's load change, and the known inputs in each area are the set-point of the generators that are controlled manually. The number of attack inputs for Areas 1 to 3 are 4, 5, and 4, respectively. As a result, 5, 6, and 5 identification UIOs must be designed for these areas, respectively. For example, using the procedure elaborated in Section 7.2.2, five identification UIOs are designed for Area 3, as follows:

- *UIO E*, identifies FDIAs targeting the power measurement of the tie-line that connects Buses 5 and 8.
- *UIO F*, identifies FDIAs targeting the power measurement of the tie-line that connects Buses 7 and 8.

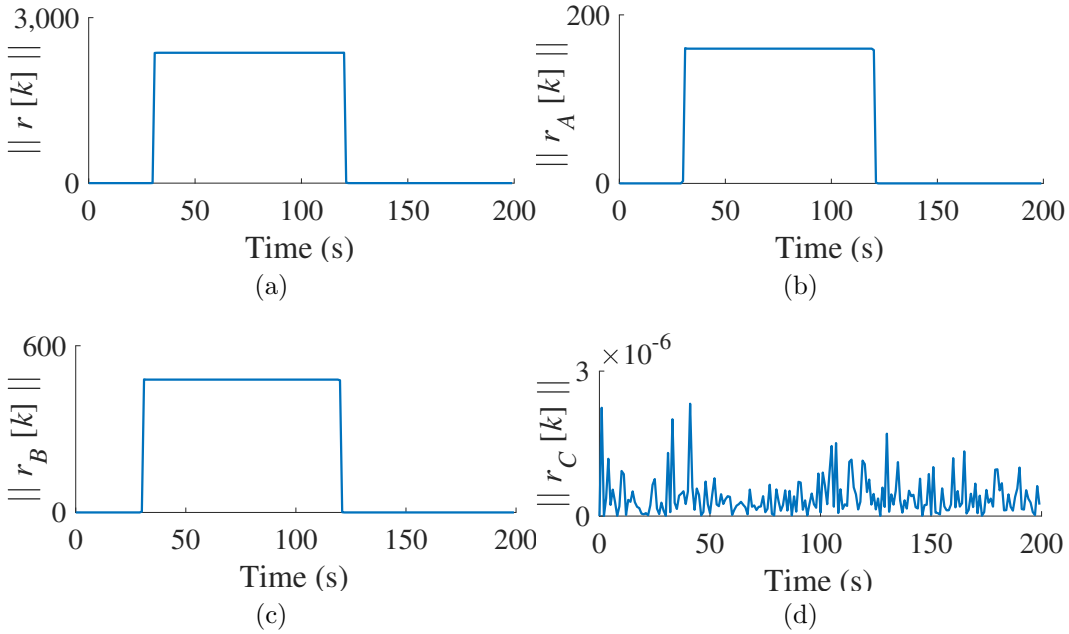


Figure 7.5: Scenario 4's RFs, (a) Main UIO, (b) UIO A, (c) UIO B, (d) UIO C.

- *UIO G*, identifies FDIAs targeting the power measurement of the tie-line that connects Buses 1 and 2.
- *UIO H*, identifies FDIAs targeting Area 3's frequency.
- *UIO I*, identifies other abnormal non-attack events and differentiates them from attacks.

The detection and identification thresholds, i.e., r^* and $r_j^*(j = E, \ldots, I)$ in (7.15) and (7.18), are determined with the same technique used for the three-area test system. Using similar noise mean and variance values, the RF of Main UIO was obtained $tr^* = 1.8$, and identification UIOs' RFs were set to 1.5.

In the following, three scenarios involving FDIAs against Area 3's measurements are investigated. For each scenario, only the RF of UIOs E, F, G, and H are presented.

• Scenario 5: Similar to Scenario 1, the SHA introduced in Section 6.3.3 targets the frequency and all tie-line power measurements of Area 3. The attack starts at $t = 30$ s and

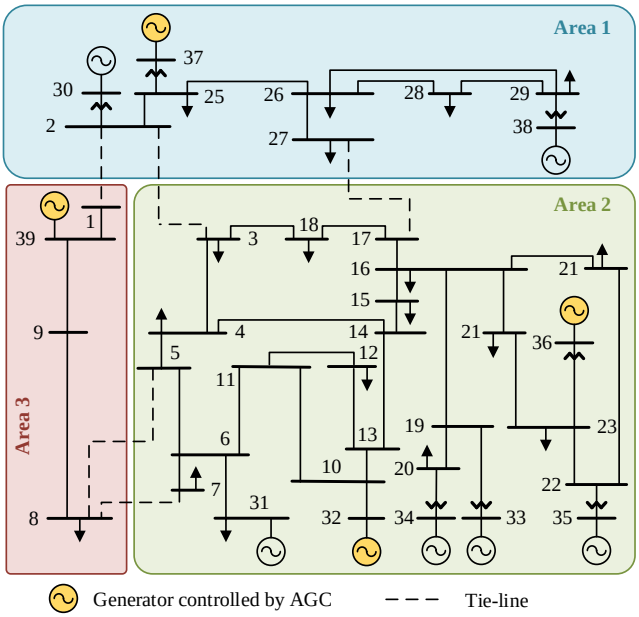


Figure 7.6: Single-line diagram of 39-bus New England test system.

lasts until $t = 200$ s. As the attack starts, the Main UIO's and the identification UIOs' RFs in Figs. 7.7a to 7.7d exceed their thresholds, indicating that all AGC measurements are erroneous.

• Scenario 6: The power measurements of Tie-lines 5-8 and 7-8, both of which connect Areas 3 and 2, are manipulated by $+5\%$ and -10%, respectively. The attack starts at $t = 40$ s and lasts until $t = 140$ s. As Fig. 7.8 illustrates, the RFs of UIOs E and F increase above the determined thresholds, indicating that their corresponding measurements are erroneous. Meanwhile, the two other identification UIOs do not detect any attack, since the power measurements of Tie-line 1-2 and frequency measurements are correct.

• Scenario 7: This scenario involves an attack against all measurements. The attack starts at $t = 40$ s with all attack inputs equal to zero. Then, the attack inputs are raised continuously until $t = 100$ s, when tie-line power and frequency measurements are increased by 5% and 0.12 Hz, respectively. Afterwards, the attack inputs are lowered continuously until $t = 140$ s, when they reach zero. As Fig. 7.9 shows, the RFs of Main UIO and identification UIOs follow the same pattern as the attack inputs, correctly identifying the

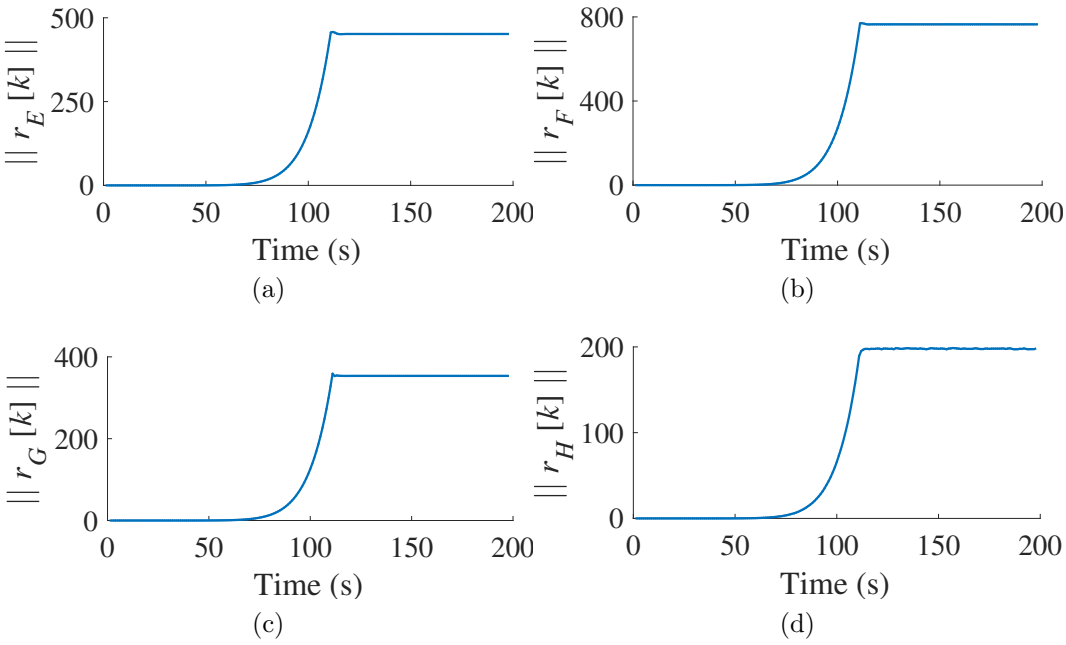


Figure 7.7: Scenario 5's RFs, (a) UIO E, (b) UIO F, (c) UIO G, (d) UIO H.

attack type, start time, and end time, and illustrating the high correlation between the attack inputs and RFs. However, as Fig. 7.10 shows, the RF of UIO I remains less than its threshold, meaning that the increase in the RFs of all identification UIOs is due to an attack that targets all parameters, not due to an abnormal non-attack event.

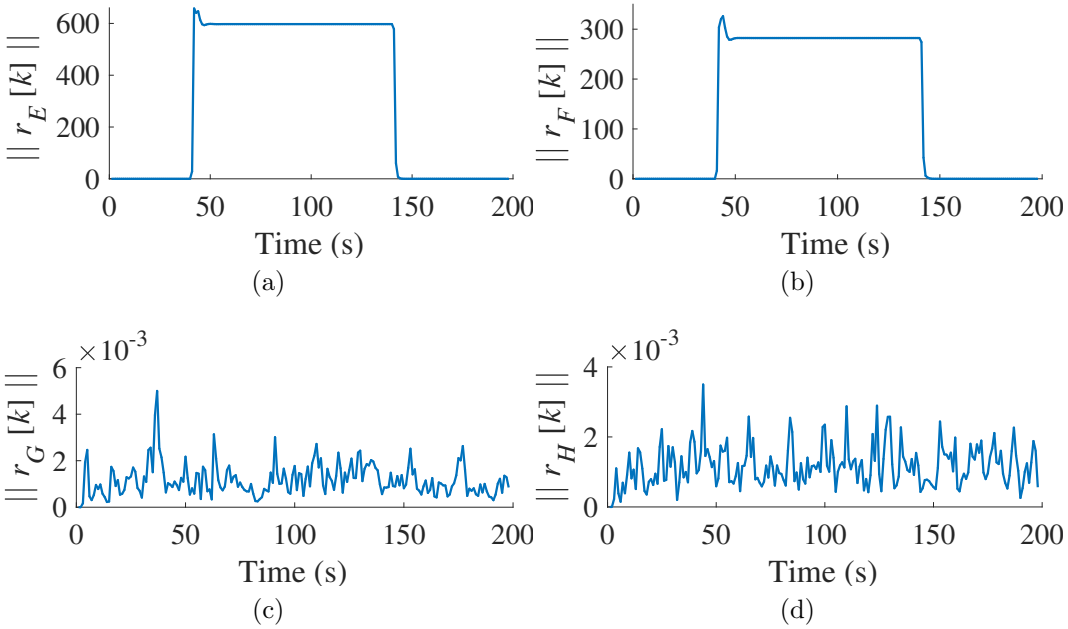


Figure 7.8: Scenario 6's RFs, (a) UIO E, (b) UIO F, (c) UIO G, (d) UIO H.

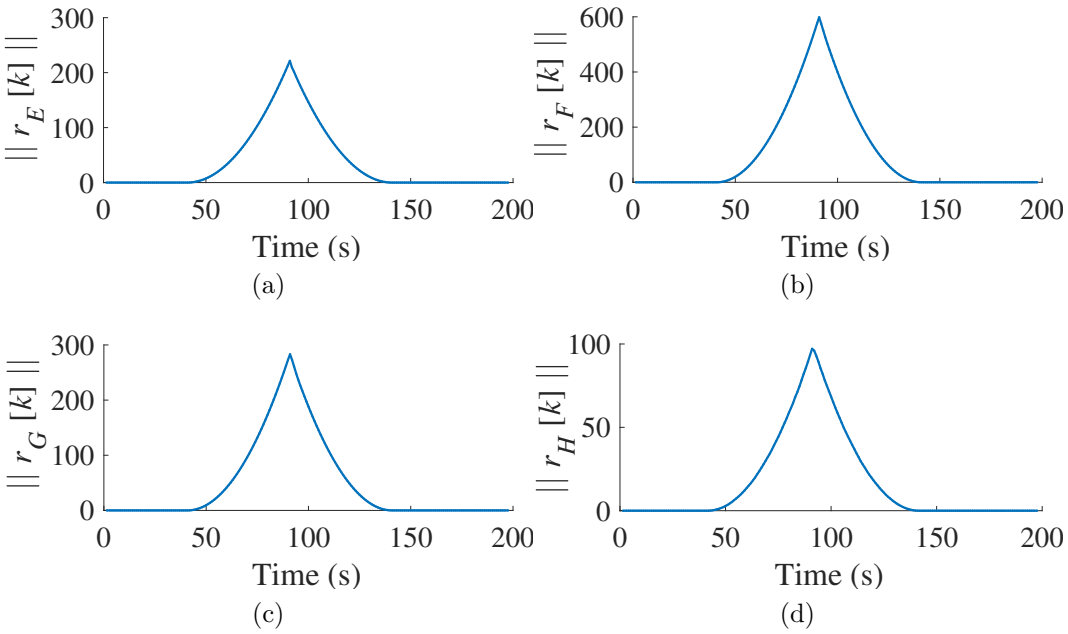


Figure 7.9: Scenario 7's RFs, (a) UIO E, (b) UIO F, (c) UIO G, (d) UIO H.

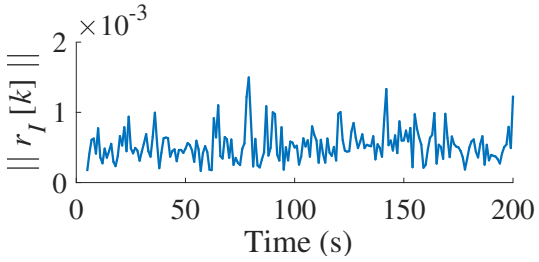


Figure 7.10: RF of UIO I during Scenario 7.

7.4 Conclusion

To protect an AGC systems against cyber-intrusions, this chapter proposed an attack-detection and -identification method that detects FDIAs by estimating the LFC system's states and comparing the estimator's RF with a predefined threshold. For estimating the LFC system's states, the proposed method uses a UIO that does not require the LFC system's inputs. This independence from inputs was also used for identifying FDIAs using identification UIOs. To design these UIOs, the potential attack types were determined first. Then, each identification UIO was designed based on the LFC system's state-space model that includes all potential attack inputs except one of them as its unknown inputs. Hence, each UIO's RF increases when the attack excluded from its unknown inputs occurs. The simulation results showed that the proposed method effectively detects attacks targeting AGC systems, identifies their types, and determines their start and end times.

Chapter 8

Attack Detection and Identification for Automatic Generation Control Systems in the Presence of Noise

Chapter 7 presented an attack-detection and -identification method for AGC systems. However, this method did not take into account the effect of noise, while noise considerably affects UIOs' RF, as shown in Fig. 7.1, and consequently influences the attack-detection accuracy.

To address this issue, this chapter presents a method to detect FDIAs targeting AGC systems by developing a SUIE. A SUIE estimates the states of the LFC system, which contains the AGC as a control loop. An increase in the SUIE's RF beyond a defined threshold signifies an FDIA. A SUIE is designed such that it works independently from some or all inputs to the system's state-space model. In addition, the effect of process and measurement noise on the estimated states is minimized through an optimal gain setting technique for the SUIE. Therefore, not only does the SUIE eliminate the need for information about real-time load changes throughout the grid, it also maximizes the state estimation accuracy. The combination of these features distinguishes the proposed method from existing FDIA-detection techniques for AGC systems. This chapter also develops a number of AISUIEs to determine which measurements are compromised by an FDIA, thus

facilitating FDIA mitigation strategies. The AISUIEs model FDIAs targeting each AGC measurement by an attack input. These inputs serve as the unknown inputs of different AISUIEs, whose RFs indicate the type of attack. The designed AISUIEs also differentiate between attacks and non-attack abnormalities, such as faults. In fact, the proposed method utilizes the physical characteristics of the LFC system and runs in parallel with intrusion-detection and prevention strategies that exploit the cyber-attributes of the system.

On this basis, Section 8.1 develops a SUIE for LFC systems. Afterwards, Section 8.2 elaborates on the proposed FDIA diagnosis technique and develops AISUIEs. Finally, using simulation analysis of the three-area power system, Section 8.3 corroborates the effectiveness of the proposed method. Additionally, Section 8.3 tests the performance of the proposed method using OPAL RTS, and compares it with another technique from the literature.

8.1 Development of a SUIE for LFC system

This section develops a SUIE for estimating the states of the LFC system. A SUIE is robust against process and measurement noise, and can accurately estimate the states of a system using the outputs and initial states of that system, i.e., without requiring the unknown inputs [126]. Therefore, a SUIE is suitable for attack-identification, as an attack is practically an unknown input. Equally important, a SUIE's independence from system inputs makes it suitable for estimating the states of the LFC system, since it eliminates the need for information about real-time load changes, which are not usually available.

As explained in Chapter 3, accurate state estimation without using system inputs is possible only by introducing a delay, denoted by α, to the estimator [82]. Thus, a window of $\alpha+1$ sampling instants from time step k to $k+\alpha$ is considered. This $(\alpha+1)$-sample-long window, referred to as the SUIE window, moves with time. Its length depends on system parameters and is explained later in this section. The objective of the following SUIE is to estimate the system states at the beginning of the SUIE window, i.e., $\mathbb{X}[k]$, using system outputs within the SUIE window, i.e., $\mathbb{Y}[k]$ to $\mathbb{Y}[k+\alpha]$, and the states at time step $k-1$, i.e., $\mathbb{X}[k-1]$.

To develop a SUIE for the LFC system presented in (6.41), which considers the effect of noise, the system outputs given in this equation for the duration of the SUIE window should be obtained based on $\mathbb{X}[k]$. To do this for time step k, $\mathbb{X}[k]$ should be substituted into (6.41b). The system states at the subsequent time steps are obtained based on $\mathbb{X}[k]$ using (6.41a) and substituted in (6.41b). Following the same procedure until time step $k+\alpha$ and organizing the results in a matrix form gives the output vector over $\alpha+1$ time steps of the window:

$$\mathcal{Y}[k:k+\alpha] = \mathcal{O}_\alpha \mathbb{X}[k] + \mathcal{J}_{u,\alpha}\mathcal{U}_u[k:k+\alpha] + \mathcal{V}[k:k+\alpha]$$
$$+ \mathcal{J}_{n,\alpha}\mathcal{U}_n[k:k+\alpha] + \mathcal{N}_{w,\alpha}\mathcal{W}[k:k+\alpha-1] \tag{8.1}$$

where

$$\mathcal{Y}[k:k+\alpha] = \begin{bmatrix} \mathbb{Y}[k]^T & \mathbb{Y}[k+1]^T & \cdots & \mathbb{Y}[k+\alpha]^T \end{bmatrix}^T \tag{8.2a}$$

$$\mathcal{U}_u[k:k+\alpha] = \begin{bmatrix} \mathbb{U}_u[k]^T & \mathbb{U}_u[k+1]^T & \cdots & \mathbb{U}_u[k+\alpha]^T \end{bmatrix}^T \tag{8.2b}$$

$$\mathcal{U}_n[k:k+\alpha] = \begin{bmatrix} \mathbb{U}_n[k]^T & \mathbb{U}_n[k+1]^T & \cdots & \mathbb{U}_n[k+\alpha]^T \end{bmatrix}^T \tag{8.2c}$$

$$\mathcal{V}[k:k+\alpha] = \begin{bmatrix} \mathbb{V}[k]^T & \mathbb{V}[k+1]^T & \cdots & \mathbb{V}[k+\alpha]^T \end{bmatrix}^T \tag{8.2d}$$

$$\mathcal{W}[k:k+\alpha-1] = \begin{bmatrix} \mathbb{W}[k]^T & \mathbb{W}[k+1]^T & \cdots & \mathbb{W}[k+\alpha-1]^T \end{bmatrix}^T \tag{8.2e}$$

$$\mathcal{O}_\alpha = \begin{bmatrix} \mathbb{C}^T & (\mathbb{C}\mathbb{A})^T & \cdots & (\mathbb{C}\mathbb{A}^\alpha)^T \end{bmatrix}^T \tag{8.2f}$$

$$\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{p\times N} & O_{p\times N} & \cdots & O_{p\times N} & O_{p\times N} \\ \mathbb{C}\mathbb{B}_u & O_{p\times N} & \cdots & O_{p\times N} & O_{p\times N} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_u & \cdots & O_{p\times N} & O_{p\times N} \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \cdots & \mathbb{C}\mathbb{B}_u & O_{p\times N} \end{bmatrix} \tag{8.2g}$$

$$\mathcal{J}_{n,\alpha} = \begin{bmatrix} O_{p\times m} & O_{p\times m} & \cdots & O_{p\times m} & O_{p\times m} \\ \mathbb{C}\mathbb{B}_n & O_{p\times m} & \cdots & O_{p\times m} & O_{p\times m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_n & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_n & \cdots & O_{p\times m} & O_{p\times m} \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_n & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_n & \cdots & \mathbb{C}\mathbb{B}_n & O_{p\times m} \end{bmatrix} \tag{8.2h}$$

$$\mathcal{N}_{w,\alpha} = \begin{bmatrix} O_{p\times 1} & O_{p\times 1} & \cdots & O_{p\times 1} & O_{p\times 1} \\ \mathbb{C} & O_{p\times 1} & \cdots & O_{p\times 1} & O_{p\times 1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2} & \mathbb{C}\mathbb{A}^{\alpha-1} & \cdots & \mathbb{C} & O_{p\times 1} \\ \mathbb{C}\mathbb{A}^{\alpha-1} & \mathbb{C}\mathbb{A}^{\alpha-2} & \cdots & \mathbb{C}\mathbb{A} & \mathbb{C} \end{bmatrix} \tag{8.2i}$$

In the next step, the SUIE's general form and its gain should be designed such that (i) the SUIE is unbiased and independent from the system inputs, i.e., the expected value of SUIE's error approaches zero when $k \to \infty$, (ii) the noise on the SUIE's error is white, and (iii) the SUIE is accurate, i.e., the mean square error between the estimated and actual states is minimized. Accordingly, using (8.1), the general form of a SUIE for estimating the state vector $\mathbb{X}[k+1]$ in (6.41) can be

$$\hat{\mathbb{X}}[k+1] = \mathbb{A}\hat{\mathbb{X}}[k] + \mathbb{B}_n\mathbb{U}_n[k] + \mathcal{L}[k]\Big(\mathcal{Y}[k:k+\alpha] - \mathcal{O}_\alpha\hat{\mathbb{X}}[k] - \mathcal{J}_{n,\alpha}\mathcal{U}_n[k:k+\alpha]\Big) \tag{8.3}$$

where $\hat{\mathbb{X}}[k]$ is the estimate given by the SUIE for $\mathbb{X}[k]$, and $\mathcal{L}[k]$ is the SUIE's gain [126]. To satisfy condition (i), the SUIE's error, i.e., $\hat{\mathbb{X}}[k+1] - \mathbb{X}[k+1]$, is derived using (6.41a) and (8.3):

$$e[k+1] = (\mathbb{A} - \mathcal{L}[k]\mathcal{O}_\alpha)\hat{\mathbb{X}}[k] + \mathcal{L}[k]\mathcal{Y}[k:k+\alpha] - \mathbb{A}\mathbb{X}[k] - \mathbb{B}_u\mathbb{U}_u[k] - \mathbb{W}[k] \tag{8.4}$$

Substituting $\mathcal{Y}[k:k+\alpha]$ from (8.1) into (8.4) yields

$$e[k+1] = \underbrace{(\mathbb{A} - \mathcal{L}[k]\mathcal{O}_\alpha)}_{\mathbb{A}'}e[k] + \mathcal{L}[k]\mathcal{V}[k:k+\alpha] + \mathcal{L}[k]\mathcal{J}_{u,\alpha}\mathcal{U}_u[k:k+\alpha] +$$

$$\mathcal{L}[k]\mathcal{N}_{w,\alpha}\mathcal{W}[k:k+\alpha-1] - \mathbb{W}[k] - \mathbb{B}_u\mathbb{U}_u[k] \tag{8.5}$$

For an unbiased SUIE, the expected value of $e[k]$, i.e., $E\{e[k]\}$, must be zero. As measurement and process noise are white, independent, and have zero mean, the expected values of $\mathcal{V}[k:k+\alpha]$, $\mathcal{W}[k:k+\alpha-1]$, and $\mathbb{W}[k]$ in (8.5) are zero. Rewriting $\mathbb{B}_u\mathbb{U}_u[k]$ as $\begin{bmatrix} \mathbb{B}_u & O_{n\times N} & \cdots & O_{n\times N} \end{bmatrix}\mathcal{U}_u[k:k+\alpha]$ and substituting it in (8.5) demonstrates that the following condition must be satisfied in order for $E\{e[k]\}$ to be zero:

$$\mathcal{L}[k]\,\mathcal{J}_{u,\alpha} = \begin{bmatrix} \mathbb{B}_u & O_{n\times N} & \cdots & O_{n\times N} \end{bmatrix} \tag{8.6}$$

Theorem 7 showed that there is a matrix $\mathcal{L}[k]$ at time-step k that satisfies (8.6) if (8.7) is satisfied [81].

$$rank\,(\mathcal{J}_{u,\alpha}) - rank\,(\mathcal{J}_{u,\alpha-1}) = N \tag{8.7}$$

in which $\mathcal{J}_{u,\alpha-1}$ is obtained using $\mathcal{J}_{u,\alpha}$ in (8.2g) and is as follows:

$$\mathcal{J}_{u,\alpha-1} = \begin{bmatrix} O_{p\times N} & O_{p\times N} & \cdots & O_{p\times N} & O_{p\times N} \\ \mathbb{C}\mathbb{B}_u & O_{p\times N} & \cdots & O_{p\times N} & O_{p\times N} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-4}\mathbb{B}_u & \cdots & O_{p\times N} & O_{p\times N} \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_u & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_u & \cdots & \mathbb{C}\mathbb{B}_u & O_{p\times N} \end{bmatrix} \tag{8.8}$$

Theorem 7. *There is a matrix $\mathcal{L}[k]$ at time-step k that satisfies (8.6) if and only if (8.7) is satisfied.* □

Proof. The proof is similar to the proof of Theorem 1 in Section 3.2.1. ■

Equation (8.7) indicates a necessary condition for developing a SUIE for an LFC system. In other words, if this condition is not met, it will not be possible to estimate the states of a system without requiring its unknown inputs.

Theorem 8. *Regardless of the number of areas and generators under AGC control in each area, an LFC system satisfies condition (8.7), therefore the system is invertible/observable and its states can be estimated by a SUIE.* □

Proof. The proof is presented in Appendix D. ■

As shown in Appendix D, $\alpha = 2$ satisfies condition (8.7) for LFC systems. To satisfy condition (ii), the noise on the SUIE's error should be investigated. Noise can affect the estimation error commensurate with its mean and variance. There are two types of noise: white and colored [127]. Either type increases the SUIE's error, but colored noise is more undesirable and increases the estimation error more than white noise does [128]. To investigate the SUIE's type-of-noise, the noise on its error should be found. If $\mathcal{L}[k]$ is designed such that (8.6) is satisfied, the SUIE's error in (8.5) is expressed by the following state-space model:

$$e[k+1] = \mathbb{A}' e[k] + \Gamma[k]\xi[k] \tag{8.9}$$

where A' is as shown in (8.5). Additionally, $\xi[k]$ and $\Gamma[k]$ are the SUIE's error noise vector and matrix, and are defined as

$$\xi[k] = \left[\begin{array}{c|c} \mathbb{W}[k:k+\alpha-1]^T & \mathcal{V}[k:k+\alpha]^T \end{array} \right]^T \tag{8.10a}$$

$$\Gamma[k] = \left[\delta_{1:n}[k] - I_{n\times n} \quad \delta_{n+1:2n}[k] \quad \cdots \quad \delta_{(\alpha-1)n+1:\alpha n}[k] \;\middle|\; \mathcal{L}[k] \right] \tag{8.10b}$$

in which $\delta_{i:j}[k]$ is a sub-matrix of $\mathcal{L}[k]\mathcal{N}_{w,\alpha}$ that contains columns i to j. The noise vector $\xi[k]$ is called colored if it is characterized by the state-space equation shown in (8.11) [127]:

$$\xi[k] = \mathbb{J}[k-1]\xi[k-1] + \mathbb{P}_n n[k] \tag{8.11}$$

where $\xi_{-1} = 0$, and $n[k]$ is a noise vector that is uncorrelated, zero-mean, Gaussian, and white. By rewriting $\xi[k]$ in (8.10a) in the form of (8.11), $\mathbb{P}_n$, $n[k]$, and $\mathbb{J}[k-1]$ are as follows

$$\mathbb{P}_n = \left[\begin{array}{ccccc|ccccc} O_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} & I_{n\times n} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} & O_{n\times p} \\ O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times n} & O_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} & I_{p\times p} \end{array} \right]^T \tag{8.12a}$$

$$n[k] = \left[\begin{array}{cc} \mathbb{W}[k+\alpha-1]^T & \mathbb{V}[k+\alpha]^T \end{array} \right]^T \tag{8.12b}$$

$$\mathbb{J}[k-1]=\left[\begin{array}{ccccc|ccccc}
O_{n\times n} & I_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\
O_{n\times n} & O_{n\times n} & I_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
O_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots & I_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\
O_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\
\hline
O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & I_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} \\
O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & I_{p\times p} & \cdots & O_{p\times p} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & O_{p\times p} & \cdots & I_{p\times p} \\
O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & O_{p\times p} & \cdots & O_{p\times p}
\end{array}\right] \tag{8.12c}$$

Satisfying (8.11) indicates that the SUIE's noise is colored, and thus condition (ii) is not satisfied. This problem can be solved by modifying the LFC system states to form an Augmented LFC system (ALFCS), as discussed in the next subsection.

8.1.1 Development of a SUIE for ALFCS

An ALFCS addresses the above problem of colored noise by eliminating $\mathbb{J}[k-1]\xi[k-1]$ from the noise vector in (8.11) and including it in the LFC's state-space equations, given by (6.41) [127]. Thus, the noise vector $n[k]$ in (8.11) is dealt with as noise, and the other noise elements in $\xi[k]$, i.e., $\mathcal{W}[k:k+\alpha-2]$ and $\mathcal{V}[k:k+\alpha-1]$, are regarded as system states that should be estimated [126]. Therefore, the condition of (8.11) no longer holds, and condition (ii) in Section 8.1 is satisfied. The states of the LFC can be obtained using the ALFCS states, as later discussed in Section 8.1.2. To differentiate between the parameters of the ALFCS and LFC, all parameters of the ALFCS are presented by an over-line.

The ALFCS is developed from LFC using:

$$\overline{\mathbb{X}}[k+1]=\overline{\mathbb{A}}\,\overline{\mathbb{X}}[k]+\overline{\mathbb{B}}_u\mathbb{U}_u[k]+\overline{\mathbb{B}}_n\mathbb{U}_n[k]+\mathbb{P}_n n[k] \tag{8.13a}$$

$$\mathbb{Y}[k]=\overline{\mathbb{C}}\,\overline{\mathbb{X}}[k] \tag{8.13b}$$

where $\mathbb{P}_n$ and $n\,[k]$ are defined in (8.12), and

$$\overline{\mathbb{X}}\,[k] = \left[\mathbb{X}\,[k]^T \;\; \mathcal{W}\,[k:k+\alpha-2]^T \;\middle|\; \mathcal{V}\,[k:k+\alpha-1]^T\right]^T \tag{8.14a}$$

$$\overline{\mathbb{A}} = \left[\begin{array}{ccccc|ccccc} \mathbb{A} & I_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\ O_{n\times n} & O_{n\times n} & I_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ O_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots & I_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\ O_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} & O_{n\times p} & O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} \\ \hline O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & I_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} \\ O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & I_{p\times p} & \cdots & O_{p\times p} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & O_{p\times p} & \cdots & I_{p\times p} \\ O_{p\times n} & O_{p\times n} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times p} & O_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} \end{array}\right] \tag{8.14b}$$

$$\overline{\mathbb{B}}_n = \left[\begin{array}{ccccc|ccccc} \mathbb{B}_n^T & O_{m\times n} & \cdots & O_{m\times n} & O_{m\times n} & O_{m\times p} & O_{m\times p} & \cdots & O_{m\times p} & O_{m\times p} \end{array}\right]^T \tag{8.14c}$$

$$\overline{\mathbb{B}}_u = \left[\begin{array}{ccccc|ccccc} \mathbb{B}_u^T & O_{N\times n} & \cdots & O_{N\times n} & O_{N\times n} & O_{N\times p} & O_{N\times p} & \cdots & O_{N\times p} & O_{N\times p} \end{array}\right]^T \tag{8.14d}$$

$$\overline{\mathbb{C}} = \left[\begin{array}{ccccc|ccccc} \mathbb{C} & O_{p\times n} & \cdots & O_{p\times n} & O_{p\times n} & I_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} & O_{p\times p} \end{array}\right] \tag{8.14e}$$

As seen in (8.13b), the system outputs are the same in both LFC and ALFCS; thus, no new measurements are required for the ALFCS. As $\mathbb{X}\,[k] \in \mathbb{R}^n$, $\mathcal{W}\,[k:k+\alpha-2] \in \mathbb{R}^{(\alpha-1)n\times 1}$, and $\mathcal{V}\,[k:k+\alpha-1] \in \mathbb{R}^{\alpha p\times 1}$, the dimension of $\overline{\mathbb{X}}$ in (8.13a) is $\overline{n} = \alpha\,(n+p)$. Similar to the LFC system, the ALFCS's SUIE has the general form of

$$\hat{\overline{\mathbb{X}}}\,[k+1] = \overline{\mathbb{A}}\,\hat{\overline{\mathbb{X}}}\,[k] + \overline{\mathbb{B}}_n\mathbb{U}_n\,[k] + \overline{\mathcal{L}}\,[k]\left(\mathcal{Y}\,[k:k+\alpha] - \overline{\mathcal{O}}_\alpha\hat{\overline{\mathbb{X}}}\,[k] - \mathcal{J}_{n,\alpha}\mathcal{U}_n\,[k:k+\alpha]\right) \tag{8.15}$$

where $\overline{\mathcal{L}}\,[k] \in \mathbb{R}^{\alpha(n+p)\times(\alpha+1)p}$ is the SUIE's gain. Moreover, $\mathcal{Y}\,[k:k+\alpha]$ must be found based on $\overline{\mathbb{X}}[k]$, as follows:

$$\mathcal{Y}\,[k:k+\alpha] = \overline{\mathcal{O}}_\alpha\overline{\mathbb{X}}\,[k] + \mathcal{J}_{u,\alpha}\mathcal{U}_u\,[k:k+\alpha] + \overline{\mathcal{N}}_{n,\alpha}n\,[k] + \mathcal{J}_{n,\alpha}\mathcal{U}_n\,[k:k+\alpha] \tag{8.16}$$

In (2.3), $\overline{\mathcal{N}}_{n,\alpha}$ and $\overline{\mathcal{O}}_{\alpha}$ are

$$\overline{\mathcal{N}}_{n,\alpha} = \begin{bmatrix} O_{n\times p} & O_{n\times p} & \cdots & O_{n\times p} & \mathbb{C}^T \\ O_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} & I_{p\times p} \end{bmatrix}^T \tag{8.17a}$$

$$\overline{\mathcal{O}}_{\alpha} = \left[\begin{array}{cccc|cccc} \mathbb{C} & O_{p\times n} & \cdots & O_{p\times n} & I_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} \\ \mathbb{C}\mathbb{A} & \mathbb{C} & \cdots & O_{p\times n} & O_{p\times p} & I_{p\times p} & \cdots & O_{p\times p} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-1} & \mathbb{C}\mathbb{A}^{\alpha-2} & \cdots & \mathbb{C} & O_{p\times p} & O_{p\times p} & \cdots & I_{p\times p} \\ \mathbb{C}\mathbb{A}^{\alpha} & \mathbb{C}\mathbb{A}^{\alpha-1} & \cdots & \mathbb{C}\mathbb{A} & O_{p\times p} & O_{p\times p} & \cdots & O_{p\times p} \end{array}\right] \tag{8.17b}$$

Since condition (ii) was held by developing the ALFCS, the SUIE's gain $\overline{\mathcal{L}}\,[k]$ in (8.15) should be designed such that conditions (i) and (iii) in Section III-A are also fulfilled for this system. To design $\overline{\mathcal{L}}\,[k]$, the SUIE's error must be found first, using (8.13), (8.15), and (8.16) with the same process carried out for the LFC in (8.5). Then, $\mathcal{Y}\,[k:k+\alpha]$ from (8.16) must be substituted in the SUIE's error, leading to

$$\overline{e}\,[k+1] = \left(\overline{\mathbb{A}} - \overline{\mathcal{L}}\,[k]\overline{\mathcal{O}}_{\alpha}\right)\overline{e}\,[k] + \left(\overline{\mathcal{L}}\,[k]\overline{\mathcal{N}}_{n,\alpha} - \mathbb{P}_n\right) n\,[k] +$$

$$\left(\overline{\mathcal{L}}\,[k]\mathcal{J}_{u,\alpha} - \begin{bmatrix} \overline{\mathbb{B}}_u & O_{\alpha(n+p)\times N} & \cdots & O_{\alpha(n+p)\times N} \end{bmatrix}\right)\mathcal{U}_u\,[k:k+\alpha] \tag{8.18}$$

Satisfying condition (i) and developing an unbiased SUIE entails equating the expected value of the SUIE's error in (8.18) with zero, which results in

$$\overline{\mathcal{L}}\,[k]\,\mathcal{J}_{u,\alpha} = \begin{bmatrix} \overline{\mathbb{B}}_u & O_{\alpha(n+p)\times N} & \cdots & O_{\alpha(n+p)\times N} \end{bmatrix} \tag{8.19}$$

As explained in the previous subsection, (8.19) entails satisfaction of (8.7). With a similar approach as in Appendix D, it can be shown that $\alpha = 2$ satisfies (8.7). Additionally, as Theorem 2 proved, an $\overline{\mathcal{L}}[k]$ in the following form fulfills the unbiasedness condition of (8.19):

$$\overline{\mathcal{L}}\,[k] = \begin{bmatrix} \overline{\mathcal{L}}_1\,[k] & \overline{\mathcal{L}}_2\,[k] \end{bmatrix}\overline{\mathcal{Q}} \tag{8.20}$$

where $\overline{\mathcal{L}}_2\,[k] = \overline{\mathbb{B}}_u$ and $\overline{\mathcal{L}}_1\,[k] \in \mathbb{R}^{\alpha(n+p)\times(p-N)}$ is a free matrix from the perspective of the

SUIE's error. Additionally, $\overline{\mathcal{Q}} \in \mathbb{R}^{p\times(\alpha+1)p}$ is a matrix that satisfies

$$\overline{\mathcal{Q}}\mathcal{J}_{u,\alpha} = \begin{bmatrix} O_{(p-N)\times N} & O_{(p-N)\times\alpha N} \\ I_{N\times N} & O_{N\times\alpha N} \end{bmatrix} \tag{8.21}$$

Hence, for any value of $\overline{\mathcal{L}}_1[k]$, multiplying $\overline{\mathcal{L}}[k]$ by $\mathcal{J}_{u,\alpha}$ results in the right hand side of (8.19), and condition (i) in Section 8.1 is satisfied. Since $\overline{\mathcal{L}}_1[k]$ does not affect the unbiasedness condition of the SUIE, it can be chosen such that condition (iii) in Section 8.1 is met. To this end, the mean square error between the estimated and actual states—or equivalently the trace of error's covariance matrix—should be minimized [129]. Thus, the SUIE's error covariance matrix should be found. By substituting $\overline{\mathcal{L}}[k]$ from (8.20) into (8.18), the SUIE's error is

$$\overline{e}[k+1] = \left(\overline{\mathbb{A}} - \begin{bmatrix} \overline{\mathcal{L}}_1[k] & \overline{\mathbb{B}}_u \end{bmatrix} \overline{\mathcal{Q}}\,\overline{\mathcal{O}}_\alpha\right)\overline{e}[k] + \left(\begin{bmatrix} \overline{\mathcal{L}}_1[k] & \overline{\mathbb{B}}_u \end{bmatrix} \overline{\mathcal{Q}}\,\overline{\mathcal{N}}_{n,\alpha} - \mathbb{P}_n\right) n[k] \tag{8.22}$$

To take $\overline{\mathcal{L}}_1[k]$ out of $\begin{bmatrix} \overline{\mathcal{L}}_1[k] & \overline{\mathbb{B}}_u \end{bmatrix} \overline{\mathcal{Q}}\,\overline{\mathcal{O}}_\alpha$, $\overline{\mathcal{Q}}\,\overline{\mathcal{O}}_\alpha$ is decomposed into Φ_1 and Φ_2 as in

$$\overline{\mathcal{Q}}\,\overline{\mathcal{O}}_\alpha = \begin{bmatrix} \overline{\Phi}_1 \\ \overline{\Phi}_2 \end{bmatrix} \tag{8.23}$$

where $\overline{\Phi}_1 \in \mathbb{R}^{(n-N)\times\alpha(n+p)}$ and $\overline{\Phi}_2 \in \mathbb{R}^{N\times\alpha(n+p)}$. Similarly, $\overline{\mathcal{Q}}\,\overline{\mathcal{N}}_{n,\alpha}$ in (8.22) is decomposed to

$$\overline{\mathcal{Q}}\,\overline{\mathcal{N}}_{n,\alpha} = \begin{bmatrix} \overline{\Psi}_1 \\ \overline{\Psi}_2 \end{bmatrix} \tag{8.24}$$

where $\overline{\Psi}_1 \in \mathbb{R}^{((p-N)\times(n+p))}$ and $\overline{\Psi}_2 \in \mathbb{R}^{N\times(n+p)}$. Substituting (8.23) and (8.24) into (8.22) yields the following estimation error:

$$\overline{e}[k+1] = \left(\overline{\mathbb{A}} - \overline{\mathcal{L}}_1[k]\overline{\Phi}_1 - \overline{\mathbb{B}}_u\,\overline{\Phi}_2\right)\overline{e}[k] + \left(\overline{\mathcal{L}}_1[k]\overline{\Psi}_1 + \overline{\mathbb{B}}_u\,\overline{\Psi}_2 - \mathbb{P}_n\right) n[k] \tag{8.25}$$

The error's covariance matrix, $E\left\{\overline{e}[k+1]\,\overline{e}[k+1]^T\right\}$, can be obtained using (8.25), and

is given by

$$\overline{\Sigma}\left[k+1\right]=\overline{\mathcal{L}}_1\left[k\right]\left(\overline{\Phi}_1\overline{\Sigma}\left[k\right]\overline{\Phi}_1^T+\overline{\Psi}_1\overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)\overline{\mathcal{L}}_1\left[k\right]^T+\overline{\Upsilon}\ \overline{\Pi}\left[k\right]\overline{\Upsilon}^T+\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Lambda}^T-$$

$$\overline{\mathcal{L}}_1\left[k\right]\left(\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Upsilon\Pi}\left[k\right]\overline{\Psi}_1^T\right)^T-\left(\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Upsilon}\ \overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)\overline{\mathcal{L}}_1\left[k\right]^T \tag{8.26}$$

where

$$\overline{\Lambda}=\overline{\mathbb{A}}-\overline{\mathbb{B}}_u\Phi_2 \tag{8.27a}$$

$$\overline{\Upsilon}=\overline{\mathbb{B}}_u\Psi_2-\mathbb{P}_n \tag{8.27b}$$

$$\overline{\Pi}\left[k\right]=E\left\{n\left[k\right]\times n\left[k\right]^T\right\}=\begin{bmatrix}\mathbb{Q}\left[k+\alpha-1\right] & 0\\ 0 & \mathbb{R}\left[k+\alpha\right]\end{bmatrix} \tag{8.27c}$$

In (8.27c), $\mathbb{Q}$ and $\mathbb{R}$ are the process and measurement noise covariance matrices introduced in Chapter 6. To find the optimal $\overline{\mathcal{L}}_1\left[k\right]$ that minimizes the trace of the error's covariance matrix $\overline{\Sigma}\left[k+1\right]$, the gradient of (8.26) with respect to $\overline{\mathcal{L}}_1\left[k\right]$ is obtained and equated with zero [126]. This procedures results in the following $\overline{\mathcal{L}}_1\left[k\right]$:

$$\overline{\mathcal{L}}_1\left[k\right]=\left(\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Upsilon}\ \overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)\left(\overline{\Phi}_1\overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Psi}_1\overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)^{-1} \tag{8.28}$$

Substituting $\overline{\mathcal{L}}_1\left[k\right]$ from (8.28) into (8.26) results in the minimum error's covariance matrix, which is as follows:

$$\overline{\Sigma}\left[k+1\right]=\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Lambda}^T+\overline{\Upsilon\Pi}\left[k\right]\overline{\Upsilon}^T-\left(\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Upsilon}\ \overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)\times$$

$$\left(\overline{\Phi}_1\overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Psi}_1\overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)^{-1}\times\left(\overline{\Lambda}\ \overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Upsilon}\ \overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)^T \tag{8.29}$$

As seen in (8.28) and (8.29), $\vartheta=\left(\overline{\Phi}_1\overline{\Sigma}\left[k\right]\overline{\Phi}_1^T-\overline{\Psi}_1\overline{\Pi}\left[k\right]\overline{\Psi}_1^T\right)$ must be inverted in order to find the optimal $\overline{\mathcal{L}}_1\left[k\right]$ and the minimum error's covariance matrix. Since $\overline{\Sigma}\left[k\right]$ in ϑ is dependent on noise, ϑ is a random matrix whose distribution depends on noise parameters. Thus, it can be shown that the probability of singularity for a random matrix is practically zero, because the Lebesgue measure for the zero set of its determinant polynomial is zero. Therefore, ϑ is practically invertible. However, for the practically unlikely scenario of

singularity for ϑ, pseudo-inverse can be used instead of inverse [83].

In conclusion, condition (ii) in Section 8.1 was met by developing the ALFCS from the LFC. Then, $\overline{\mathcal{L}}[k]$ was designed according to (8.20) to satisfy conditions (i) and (iii). Condition (i) was addressed by choosing $\overline{\mathcal{L}}_2[k] = \overline{\mathbb{B}}_u$ and designing $\overline{\mathcal{Q}}$ using (8.21). Condition (iii) was also held by finding the optimal $\overline{\mathcal{L}}_1[k]$ according to (8.28). After designing the SUIE for ALFCS, the outputs of this system at time steps k to $k+\alpha$ and its states at time step $k-1$ must be substituted in (8.15) to obtain the ALFCS's states at time step k. The flowchart of this procedure is illustrated in Fig. 8.1. By considering that (i) the number of states, i.e., n, is greater than or equal to N, m, and p, and (ii) all the steps in Fig. 8.1 involve only simple matrix summation, multiplication, and inversion, the computational complexity for each on-line step in the flowchart is calculated using Big O notation [130], and is shown beside it. Therefore, using the obtained complexity for each step, the overall computational complexity of the algorithm is bounded by $O(n^3)$.

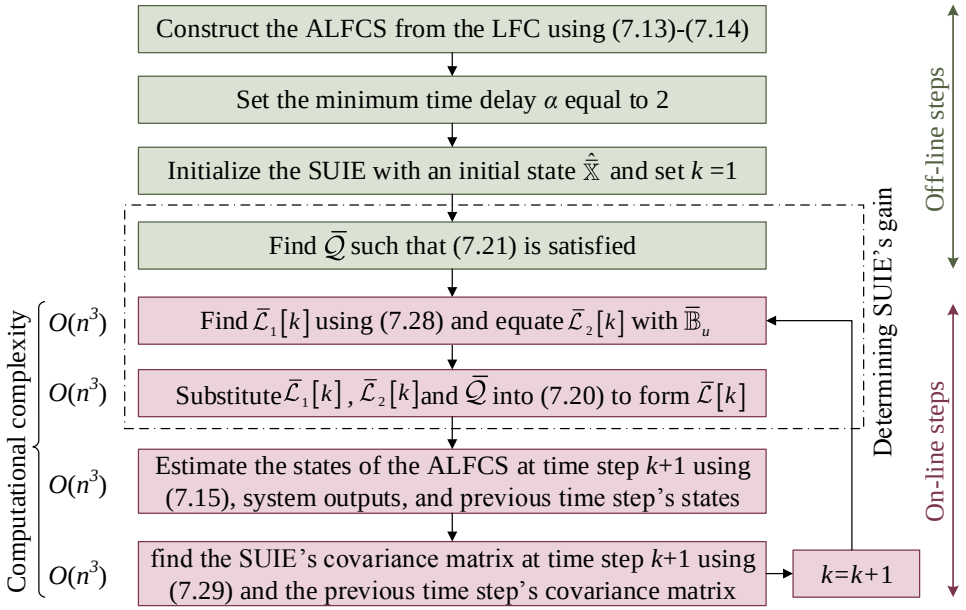


Figure 8.1: Flowchart of state estimation for the ALFCS using a SUIE.

8.1.2 Relation Between ALFCS and OLFCS

The following explains how to find the states, estimation error, and covariance matrix of the LFC system from those of the ALFCS. As shown in (8.14a), the first n states of the ALFCS equal all of the states of the LFC; thus, using (8.14a), the states of the LFC system are obtained from

$$\hat{\mathbb{X}}[k] = \begin{bmatrix} I_{n\times n} & O_{n\times(\alpha(n+p)-n)} \end{bmatrix} \hat{\overline{\mathbb{X}}}[k] \tag{8.30}$$

Similarly, the estimation error for the LFC system is

$$e[k] = \begin{bmatrix} I_{n\times n} & O_{n\times(\alpha(n+p)-n)} \end{bmatrix} \overline{e}[k] \tag{8.31}$$

where $\overline{e}[k]$ is given in (8.25). Additionally, using $\overline{\Sigma}[k+1]$ in (8.29), the error covariance matrix of the LFC system is calculated by

$$\Sigma[k+1] = \begin{bmatrix} I_{n\times n} & O_{n\times(\alpha(n+p)-n)} \end{bmatrix} \overline{\Sigma}[k+1] \begin{bmatrix} I_{n\times n} \\ O_{(\alpha(n+p)-n)\times n} \end{bmatrix} \tag{8.32}$$

8.2 FDIA Diagnosis Using SUIE

This section presents a technique for detecting and identifying FDIAs targeting an AGC system.

8.2.1 FDIA Detection

As explained in Section 6.4.2, when an FDIA is in progress, a new component, i.e., $\mathbb{B}_h \times \mathbb{H}[k]$, is added to the system model in (6.33), and modifies it to (6.41). This new component also modifies (8.16) to:

$$\tilde{\mathcal{Y}}[k:k+\alpha] = \mathcal{Y}[k:k+\alpha] + \mathcal{M}_\alpha \mathcal{H}[k:k+\alpha] \tag{8.33}$$

where $\tilde{Y}[k:k+\alpha]$ is the ALFCS's output during an FDIA, and $\mathcal{M}_\alpha$ and $\mathcal{H}[k:k+\alpha]$ are

$$\mathcal{M}_\alpha = \begin{bmatrix} O_{p\times z} & O_{p\times z} & \cdots & O_{p\times z} & O_{p\times z} \\ \mathbb{C}\mathbb{B}_h & O_{p\times z} & \cdots & O_{p\times z} & O_{p\times z} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_h & \mathbb{C}\mathbb{A}^{\alpha-3}\mathbb{B}_h & \cdots & O_{p\times z} & O_{p\times z} \\ \mathbb{C}\mathbb{A}^{\alpha-1}\mathbb{B}_h & \mathbb{C}\mathbb{A}^{\alpha-2}\mathbb{B}_h & \cdots & \mathbb{C}\mathbb{B}_h & O_{p\times z} \end{bmatrix} \tag{8.34a}$$

$$\mathcal{H}[k:k+\alpha] = \begin{bmatrix} \mathbb{H}[k]^T & \mathbb{H}[k+1]^T & \cdots & \mathbb{H}[k+\alpha]^T \end{bmatrix}^T \tag{8.34b}$$

When the system is not under an FDIA, all elements of $\mathcal{H}[k:k+\alpha]$ are zero, and thus $\mathcal{Y}[k:k+\alpha]$ equals $\tilde{\mathcal{Y}}[k:k+\alpha]$. However, during an FDIA, $\tilde{\mathcal{Y}}[k:k+\alpha]$ differs from $\mathcal{Y}[k:k+\alpha]$, resulting in the following estimation error:

$$\tilde{e}[k+1] = \overline{e}[k+1] + \overline{\mathcal{L}}[k]\,\mathcal{M}_\alpha \mathcal{H}[k:k+\alpha] - \overline{\mathbb{B}}_h \mathbb{H}[k] \tag{8.35}$$

where $\overline{e}[k+1]$ is the SUIE's error during attack-free operation of the AGC, and is given in (8.25). Additionally, $\overline{\mathbb{B}}_h$ is developed using the same procedure as for (8.14c), and is

$$\overline{\mathbb{B}}_h = \left[\begin{array}{ccccc|ccccc} \mathbb{B}_h^T & O_{z\times n} & \cdots & O_{z\times n} & O_{z\times n} & O_{z\times p} & O_{z\times p} & \cdots & O_{z\times p} & O_{z\times p} \end{array}\right]^T \tag{8.36}$$

where z is the possible number of attacks can target the system. It is shown in Appendix E that during an FDIA, the probability of amplification of the estimation error in (8.35) after one time step is practically 1. In other words, for an FDIA, the probability of remaining undetectable after one time step is zero. This issue leads to erroneous state estimation during FDIAs, and is exploited to detect such attacks by using

$$r[k] = \mathbb{Y}[k] - \mathbb{C}\hat{\mathbb{X}}[k] \tag{8.37}$$

where $\mathbb{Y}[k]$ is given in (6.41b). By substituting the estimated states given by (8.30) into (8.37), $r[k]$ during attack-free operation equals $C \times e[k] + \mathbb{V}[k]$, whose expected value is

zero. During an FDIA, however, $r[k]$ becomes

$$\tilde{r}[k] = \mathbb{C}\left(e[k] + \begin{bmatrix} I_{n\times n} & O_{n\times(\alpha(n+p)-n)} \end{bmatrix}\left(\overline{\mathcal{L}}[k]\,\mathcal{M}_\alpha\mathcal{H}[k:k+\alpha] - \overline{\mathbb{B}}_h\mathbb{H}[k]\right)\right) + \mathbb{V}[k] \tag{8.38}$$

Thus, an FDIA can be detected when the Euclidean norm of $r[k]$ increases above a certain threshold. Meanwhile, as suggested by the χ^2–testing method, the weighted vector norm of this function—instead of its Euclidean norm—can be used to decrease the rate of false alarms [131]. As a result, the RF for detecting FDIAs can be as

$$g[k] = r[k]^T\Omega[k]^{-1}r[k] \tag{8.39}$$

where $\Omega[k]$ is the covariance matrix of $r[k]$, i.e., $E\left\{r[k]\times r[k]^T\right\}$, and can be obtained using

$$\Omega[k] = \mathbb{C}\Sigma[k]\mathbb{C}^T + \mathbb{R}[k] \tag{8.40}$$

In fact, $\Omega[k]$ indicates how accurately the elements of $r[k]$ are estimated; smaller values on the trace of $\Omega[k]$ signify more accurate estimation of their corresponding states [131]. Therefore, by taking the inverse of $\Omega[k]$ and using it as a weighting factor in (8.40) for adding up the square of the components of $r[k]$, the elements that are estimated more (less) accurately have larger (smaller) weighting factors. FDIAs targeting an AGC system can be detected by comparing the Euclidean norm of $g[k]$ with a threshold, denoted by tr^*. In other words, an FDIA is detected if

$$\|g[k]\| > tr^* \tag{8.41}$$

Since $\|g[k]\|$ has no unit, tr^* is also a unit-less number that must be chosen such that all FDIAs are detected, while false alarms are avoided. This threshold can be set either by monitoring the SUIE's RF during attack-free conditions and selecting its highest value, or by using hypothesis testing and the χ^2–testing method's tables [131]. Using the first method, tr^* is determined numerically in Section 8.3. In the rest of this chapter, the SUIE used for FDIA detection based on (8.37)-(8.41) is termed the *Main SUIE*.

8.2.2 FDIA Type Identification

The method presented in Section 8.2.1 can detect FDIAs, but it is not able to identify their types. Identification helps to mitigate FDIAs more quickly by indicating which sensor measurements have been targeted. To identify FDIAs, a number of AISUIEs must be designed. To this aim, as explained in Section 6.4.2, the system model during FDIAs, given by (6.41), and the number of attack inputs ($h_{f,i}$ and $h_{T_1,i}$ to $h_{T_N,i}$) should be found for each area. Then, for designing each AISUIE, a certain combination of attack inputs are modeled as unknown inputs, and other attack inputs and their impacts on the system states are ignored in the AISUIE state-space model. Additionally, instead of the sum of all tie-lines' power deviation, each tie-line's power deviation must be individually considered as a system state. Given that the number of possible attack inputs in Area i of Fig. 6.7 is z_i, $2^{z_i}-1$ separate AISUIEs, each associated with a combination of Area i's attack inputs, should be designed. For example, there are three attack inputs for Area 1 of the three-area power system mentioned in Chapter 6. Thus, seven AISUIEs should be designed for this area, as denoted in Table 8.1 by AISUIE A to G. In this table, $h_{T_2,1}$, $h_{T_3,1}$, and $h_{f,1}$ are attack inputs that represent FDIAs targeting $\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$, and Δf_1, respectively. The state-space equation of each AISUIE models the attack inputs shown in column 2, as well as their impacts on the system states. Hence, each AISUIE's model in Table 8.1 includes a combination of FDIAs that can target the parameters presented in column 3. The unknown inputs of each AISUIE are the attack inputs associated with that AISUIE as well as the system unknown input vector $\mathbb{U}_u[.]$. Thus, the state-space equation used for designing each AISUIE, e.g. AISUIE A, is

$$\begin{cases} \mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + [\mathbb{B}_u \;\; \mathbb{B}_h^A] \begin{bmatrix} \mathbb{U}_u[k] \\ \mathbb{H}^A[k] \end{bmatrix} + \mathbb{B}_n\mathbb{U}_n[k] + \mathbb{W}[k] \\ \mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k]\,\mathbb{V}[k] \end{cases} \tag{8.42}$$

where $\mathbb{H}^A[k]$ is the attack input vector of AISUIE A, which contains attack input $h_{T_2,1}$, and $\mathbb{B}_h^A$ is a matrix that includes only the column(s) of $\mathbb{B}_h$ that is(are) associated with the attack input(s) of $\mathbb{H}^A[k]$. The output equation of all AISUIEs are the same as the system output equation, shown in (6.41b). As a result of this formulation, when Area 1 is targeted, the RF of AISUIE A does not increase for its respective attacks, since its state-

Table 8.1: AISUIEs for Area 1 of The Three-Area Power System

AISUIE	Considered attack input(s)	Unconsidered attack input(s)	Parameter(s) whose attack(s) is(are) modeled	Parameter(s) whose attack(s) is(are) not modeled	Unknown input(s)
A	$h_{T_2,1}$	$h_{T_3,1}$, $h_{f,1}$	$\Delta P_{tie_{1,2}}$	$\Delta P_{tie_{1,3}}$, Δf_1	$h_{T_2,1}$, $\mathbb{U}_u$
B	$h_{T_3,1}$	$h_{T_2,1}$, $h_{f,1}$	$\Delta P_{tie_{1,3}}$	$\Delta P_{tie_{1,2}}$, Δf_1	$h_{T_3,1}$, $\mathbb{U}_u$
C	$h_{f,1}$	$h_{T_2,1}$, $h_{T_3,1}$	Δf_1	$\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$	$h_{f,1}$, $\mathbb{U}_u$
D	$h_{T_2,1}$, $h_{T_3,1}$	$h_{f,1}$	$\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$	Δf_1	$h_{T_2,1}$, $h_{T_3,1}$, $\mathbb{U}_u$
E	$h_{T_2,1}$, $h_{f,1}$	$h_{T_3,1}$	$\Delta P_{tie_{1,2}}$, Δf_1	$\Delta P_{tie_{1,3}}$	$h_{T_2,1}$, $h_{f,1}$, $\mathbb{U}_u$
F	$h_{T_3,1}$, $h_{f,1}$	$h_{T_2,1}$	$\Delta P_{tie_{1,3}}$, Δf_1	$\Delta P_{tie_{1,2}}$	$h_{T_3,1}$, $h_{f,1}$, $\mathbb{U}_u$
G	$h_{T_2,1}$, $h_{T_3,1}$, $h_{f,1}$	–	$\Delta P_{tie_{1,2}}$, $\Delta P_{tie_{1,3}}$, Δf_1	–	$h_{T_2,1}$, $h_{T_3,1}$, $h_{f,1}$, $\mathbb{U}_u$

space equation includes those attacks in its model as unknown inputs. In other words, if any attack that is not associated with AISUIE A happens in Area 1, the RF of AISUIE A increases. As a result, if the main SUIE's RF increases over its threshold and AISUIE A's RF does not, it signifies that only some/all of the attacks associated with AISUIE A are active, as shown in the following equation:

$$\|g\,[k]\| > tr^* \qquad \text{and} \qquad \|g_A\,[k]\| < tr_A^* \tag{8.43}$$

where $\|g_A\,[k]\|$ is the Euclidean norm of AISUIE A's RF, and tr_A is this AISUIE's threshold.

Using the AISUIEs designed in Table 8.1, attacks are identified according the RF-increase for the AISUIEs, as indicated in Table 8.2. For example, in Table 8.2 an increase in the RFs of AISUIEs B, C, and F, accompanied by less-than-threshold RFs for the rest of the AISUIEs, indicates that $h_{T_2,1}$ is targeted. Similarly, a simultaneous increase in the RFs of AISUIEs A to F indicates that all three parameters—i.e., $h_{T_2,1}$, $h_{T_3,1}$, and $h_{f,1}$—are targeted. Additionally, as shown in Table 8.2, AISUIE G's RF does not increase during any attack, since its state-space model includes all possible attacks inputs as unknown inputs. Based on this design, the RF of AISUIE G does not increase during normal conditions or the modeled FDIAs. Therefore, since all possible attacks are modeled in AISUIE G, any increase in the RF of this AISUIE signifies other abnormal non-attack events, such as a fault.

Table 8.2: Identification Logic for Area 1 of The Three-Area Test System

Targeted parameter(s)	RF increase for AISUIEs						
	A	*B*	*C*	*D*	*E*	*F*	*G*
$h_{T_2,1}$	-	✓	✓	-	-	✓	-
$h_{T_3,1}$	✓	-	✓	-	✓	-	-
$h_{f,1}$	✓	✓	-	✓	-	-	-
$h_{T_2,1}$, $h_{T_3,1}$	✓	✓	✓	-	✓	✓	-
$h_{T_2,1}$, $h_{f,1}$	✓	✓	✓	✓	-	✓	-
$h_{T_3,1}$, $h_{f,1}$	✓	✓	✓	✓	✓	-	-
$h_{T_2,1}$, $h_{T_3,1}$, $h_{f,1}$	✓	✓	✓	✓	✓	✓	-
Other events, such as faults	✓	✓	✓	✓	✓	✓	✓

The designed AISUIEs in Table 8.1 identify FDIAs targeting Area 1 when only this area is under attack. However, if any other area is targeted at the same time, the RFs of all AISUIEs increase, since the out-of-area attacks have not been modeled in the AISUIEs of Table 8.1. This issue can be easily addressed by modeling the attack inputs of all other areas as unknown inputs for the AISUIEs of each area. For example, if the attack inputs $h_{f,2}$, $h_{T_1,2}$, $h_{T_3,2}$, $h_{f,3}$, $h_{T_1,3}$, and $h_{T_2,3}$—which represent intrusions against $\Delta\omega_2$, $\Delta P_{tie_{2,1}}$, $\Delta P_{tie_{2,3}}$, $\Delta\omega_3$, $\Delta P_{tie_{3,1}}$, and $\Delta P_{tie_{3,2}}$ of Areas 2 and 3, respectively—are also modeled as unknown inputs for the AISUIEs of Area 1 in Table 8.1, the RFs of these AISUIEs do not increase for attacks targeting Areas 2 and 3. As a result of this modeling, the RF of each AISUIE in Table 8.1 increases only if the respective parameter(s) for Area 1 is (are) targeted.

8.3 Performance Evaluation

8.3.1 Off-line Simulation

Using MATLAB/Simulink, this section assesses the performance of the proposed FDIA-detection and -identification technique for the three-area power system introduced in Appendix C. The state-space equation of this test system was presented in Section 6.4.2.

However, in this section, each tie-line's power is modeled separately. The estimation delay for the Main SUIE and all AISUIEs is $\alpha = 2$ time-steps. The process noise ($\mathbb{W}$ and $\mathbb{V}$) added to each area's state-space equations in (6.41) is zero-mean Gaussian noise with the time-invariant covariance matrix of $0.03 \times diag\begin{bmatrix} 1 & 1 & 0.03 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ [125]. The elements of this covariance matrix are related to and in the same order as those in (6.23a), e.g., the variances of the process noise corresponding to the frequency is 0.0009, and other states' noise variances are 0.03. The output equation of each area includes the power being delivered by each tie-line, $\Delta\omega_i$, and $\Delta P_{c_{g,i}}$ for the generator(s) that is(are) controlled by the AGC. The measurement noise in the output equation is also Gaussian, zero-mean, and with the time-invariant covariance matrix of $0.03 \times diag\begin{bmatrix} 1 & 1 & 0.03 & 1 \end{bmatrix}$. Moreover, as explained in Section 6.4.2, each area's AGC can be targeted by three attacks. Thus, seven AISUIEs, shown in Table 8.1, should be designed for each area.

To determine the thresholds for the Main SUIE and AISUIEs, the SUIEs' RFs are monitored during attack-free conditions, and the thresholds are determined such that no FDIA is detected. Not only does this method take into account the effect of noise on RFs, it also considers other unknown sources of error or known ones (such as parameter uncertainties, which are modeled by a percentage error that is normally distributed around zero, with 5% standard deviation). To obtain the above-mentioned thresholds, the Main SUIE's and the designed AISUIEs' RFs were recorded for 1000 seconds in the presence of noise and parameter uncertainties during normal condition. The largest recorded RF for each SUIE plus a 20% security margin was assigned to the threshold of that SUIE. Afterwards, to verify the obtained thresholds, the above-mentioned procedure was repeated two more rounds, each for 1000 seconds. If the obtained thresholds in the test rounds are greater than the initial ones, the initial thresholds are replaced by the larger recorded ones. This procedure was continued until the test rounds verified the obtained thresholds. As an example, Fig. 8.2 illustrates the Main SUIE's RF for 1000 seconds: the maximum of $g[k]$ is 0.15. Thus, the FDIA-detection threshold for the Main SUIE can be selected as 0.15 plus 20% security margin, and so tr^* is set to 0.18. Similar results are also obtained for the AISUIEs.

Next, six scenarios involving FDIAs against Area 1's measurements are investigated. For each scenario, the RF of the Main SUIE and AISUIEs A, B, and C in Table 8.1 are

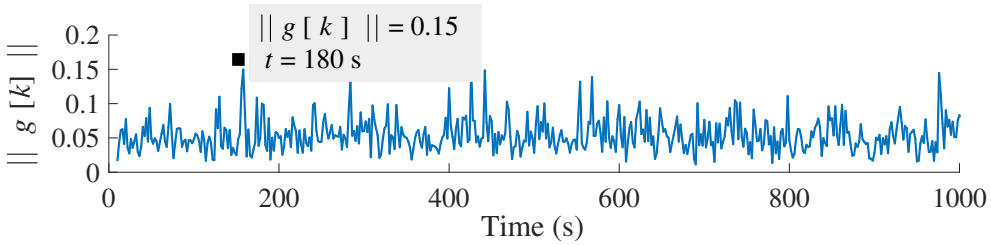


Figure 8.2: Main SUIE's RF considering noise and parameter uncertainties.

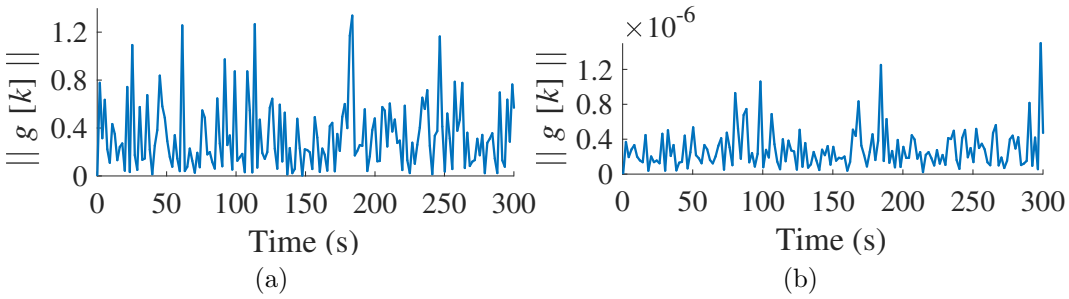


Figure 8.3: Main SUIE's RF, (a) Scenario 1, (b) Scenario 2.

presented.

• Scenario 1: In this scenario, no attack targets the AGC, and the system operates normally in the presence of noise. However, the Main SUIE does not take into account the effects of noise in the state-space model, i.e., the noise means and variances are considered to be zero. This scenario and the next one show how the designed SIUE reduces the impact of noise on its estimated outputs and RFs. Fig. 8.3a displays the Main SUIE's RF during Scenario 1: when the noise is not considered in designing the Main SUIE, its RF is in the order of 1 at all times, which is greater than $tr = 0.18$. Thus, noise can increase the false alarm rate in the system if it is not properly dealt with.

• Scenario 2: This scenario is similar to Scenario 1, but the noise and its effects are included in the Main SUIE's equations to show how accurately the Main SUIE works in the presence of noise. Fig. 8.3b shows the Main SUIE's RF: the RF is in the order of 10^{-6}. This reduction in the Main SUIE's RF with respect to Scenario 1 indicates the effectiveness of the designed SUIE in eliminating the noise impact on estimated states.

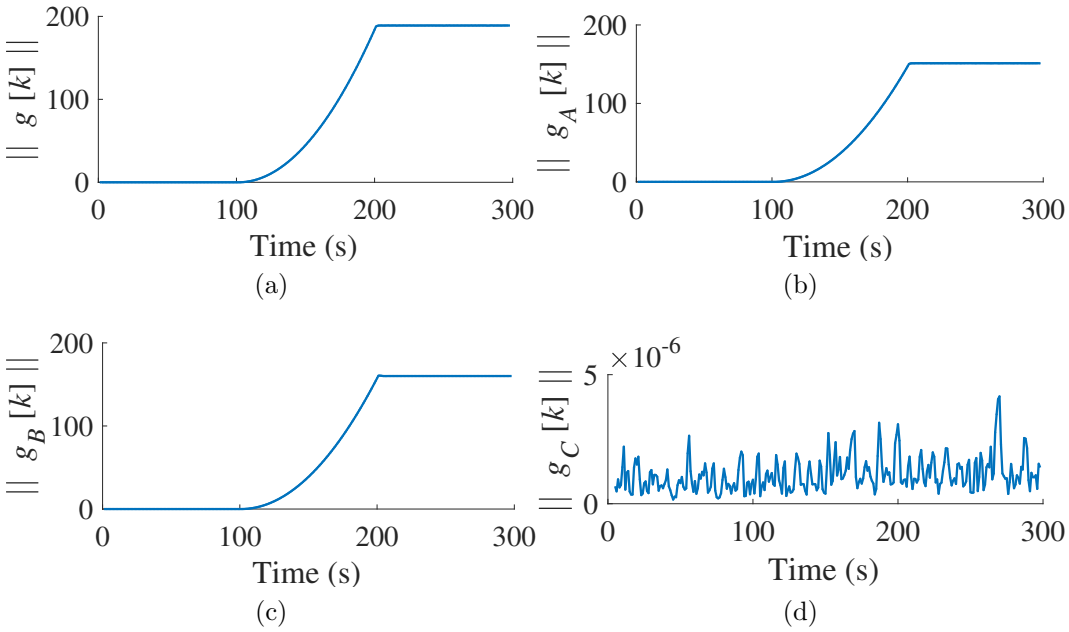


Figure 8.4: Scenario 3 RFs, (a) Main SUIE, (b) AISUIE A, (c) AISUIE B, (d) AISUIE C.

• Scenario 3: In this scenario, an FDIA uses attack input $h_{f,1}$ to decreases the frequency measurements gradually by 0.12 Hz. The FDIA starts at $t = 100$ s. As Fig. 8.4 shows, the RFs of the Main SUIE and the AISUIEs increase one time step, i.e., 2 s, after the FDIA starts, as explained in Appendix E. As $h_{f,1}$ is the only non-zero attack input in this scenario, the RFs of AISUIEs A, B, and D increase. The RFs of other AISUIEs remain very small, since they include $h_{f,1}$ in their model as an unknown input (Table 8.1 and Fig. 8.4d).

• Scenario 4: The FDIA in this scenario increases the power measurements of the tie-line that connects Areas 1 and 2 by 5%. The attack starts at $t = 50$ s and ends at $t = 150$ s. Fig. 8.5 shows the Main SUIE's and the AISUIEs' RFs: the RFs of the Main SUIE and AISUIEs B and C grow large. The RF of AISUIE A does not rise, since this AISUIE's model involves the FDIAs that target power measurements of the tie-line between Areas 1 and 2 (Table 8.1). Therefore, an increase in the Main SUIE's RF without rising AISUIE A's RF signifies that $h_{T_2,1}$ is targeted.

• Scenario 5: This scenario involves an FDIA that utilizes attack inputs $h_{f,1}$, $h_{T_2,1}$, $h_{T_3,1}$

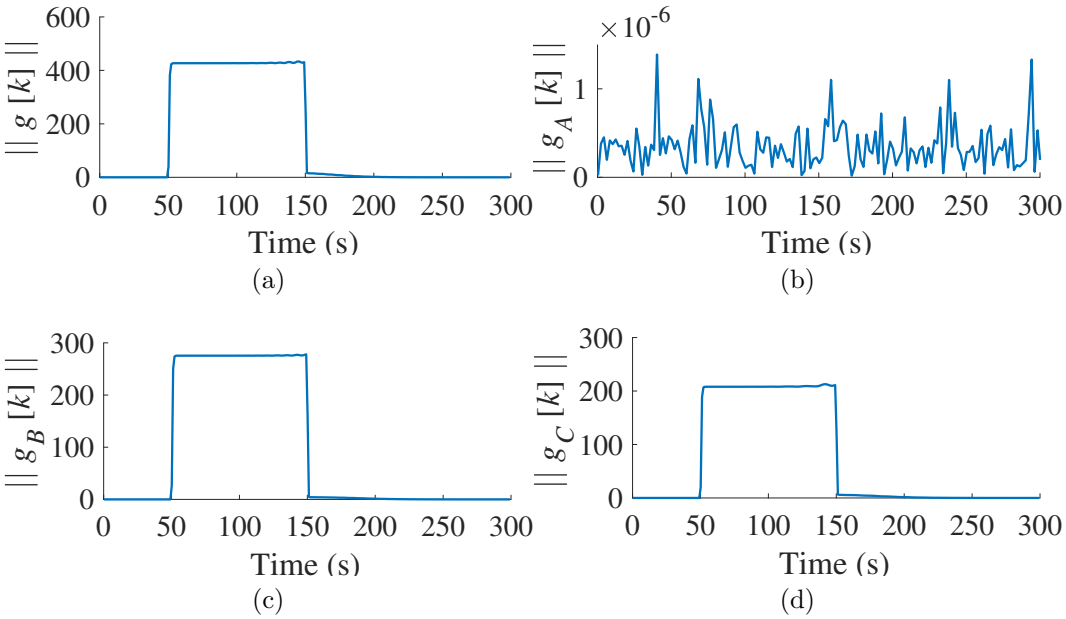


Figure 8.5: Scenario 4 RFs, (a) Main SUIE, (b) AISUIE A, (c) AISUIE B, (d) AISUIE C.

to manipulate all of the measurements. The FDIA starts at $t = 30$ s and ends at $t = 150$ s. The measurements are manipulated gradually until the deviations of the tie-line power and frequency measurements from their nominal values reach 5% and 0.12 Hz, respectively. The increase in the RFs of the Main SUIE and three sample AISUIEs has been depicted in Fig. 8.6. The RFs of these AISUIEs increase, since two of the non-zero attack inputs are absent in these AISUIEs' unknown inputs (Table 8.1), e.g., AISUIE C's model lacks the attacks against tie-line power measurements. Similarly, the RFs of AISUIEs D, E, and F increase since their models lack one of the non-zero attack inputs. Therefore, this scenario's FDIA cannot be identified by AISUIEs A to F. However, because AISUIE G's model includes all non-zero attack inputs, the RF of this AISUIE does not increase, as shown in Fig. 8.7, meaning that all measurements have been targeted simultaneously. Additionally, as the injections increase gradually, the RFs also change with a similar pattern. The abrupt end of the FDIA also makes the RFs drop suddenly.

• Scenario 6: This scenario shows the performance of the proposed method for multiple simultaneous attacks on different areas and parameters of the system. In this scenario, the

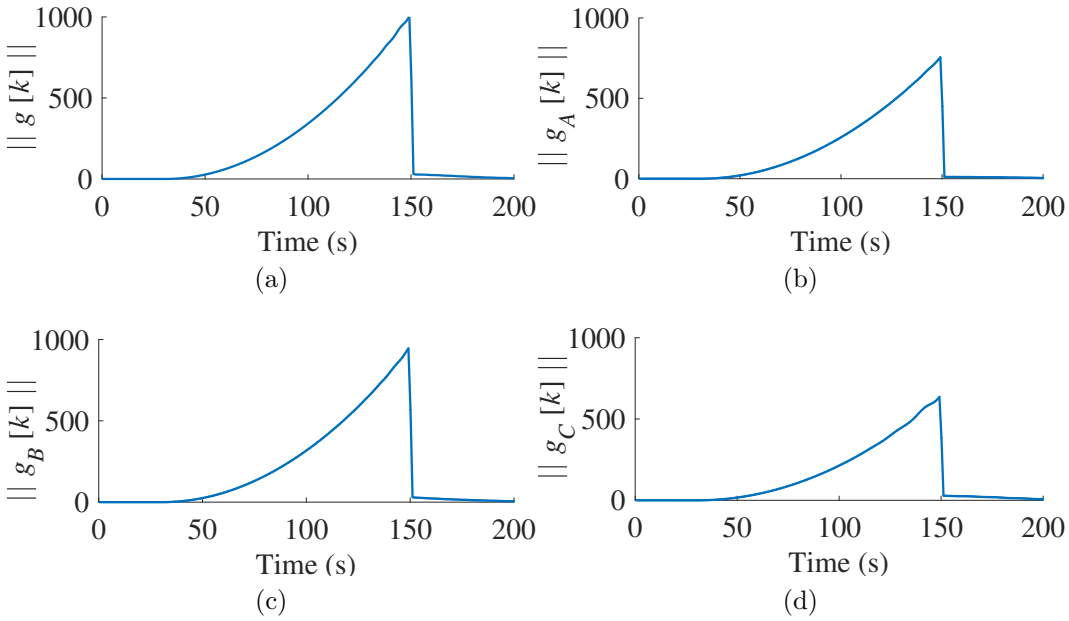


Figure 8.6: Scenario 5 RFs, (a) Main SUIE, (b) AISUIE A, (c) AISUIE B, (d) AISUIE C.

FDIA discussed in Scenario 3 targets the frequencies of Areas 1 and 2 at the same time; i.e., the targeted parameters are $h_{f,1}$ and $h_{f,2}$. In addition to the unknown inputs mentioned in Table 8.1, the attack inputs of Areas 2 and 3 are modeled as unknown inputs as well, resulting in the development of AISUIEs that are robust against out-of-area attacks. Fig. 8.8 illustrates the RFs of AISUIEs A, B, C, and G for Area 1. The RF of AISUIE C—which is associated with $h_{f,1}$ (Tables 8.1 and 8.2)—remains around zero, indicating that only $h_{f,1}$ is under attack in Area 1. The RF of AISUIE G also remains around zero, because both the nonzero attack inputs, i.e., $h_{f,1}$ and $h_{f,2}$, are modeled as unknown inputs for this AISUIE. However, AISUIEs A and B detect the attack, because the respective state-space equations do not model the attacks on $h_{f,1}$. Area 2's AISUIEs also give the same results, because the same parameter ($h_{f,2}$) is under attack in that area.

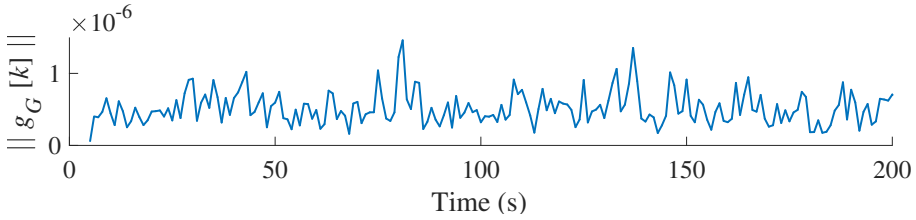


Figure 8.7: RF of AISUIE G during Scenario 5.

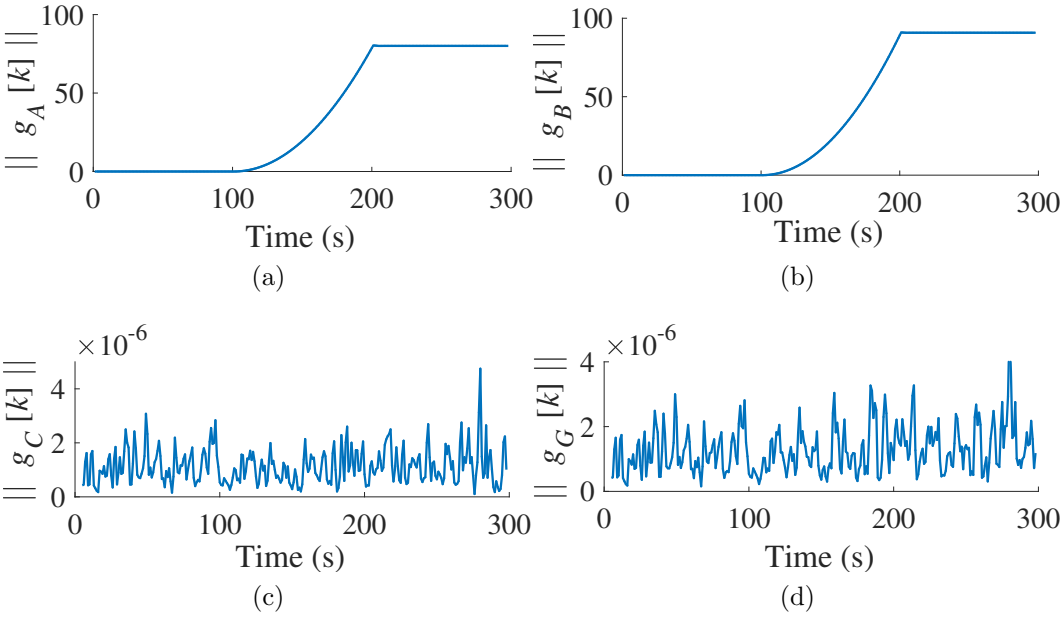


Figure 8.8: Scenario 6 RFs, (a) AISUIE A, (b) AISUIE B, (c) AISUIE C, (d) AISUIE G.

8.3.2 Real-Time Simulation

This section investigates the performance of the proposed method using an OPAL RTS. As explained in Section 4.3.2, utilizing an RTS for testing power system control/protection methods is a well-established practice [132, 133, 134, 135]. This approach integrates a physical control/protection platform within a software-based real-time digital simulator and constitutes an HIL verification environment. In an HIL setup (Fig. 8.9), a physical controller emulates the proposed method by using simulation signals obtained in real time.

In the developed HIL setup, the processor that emulates the proposed attack-detection

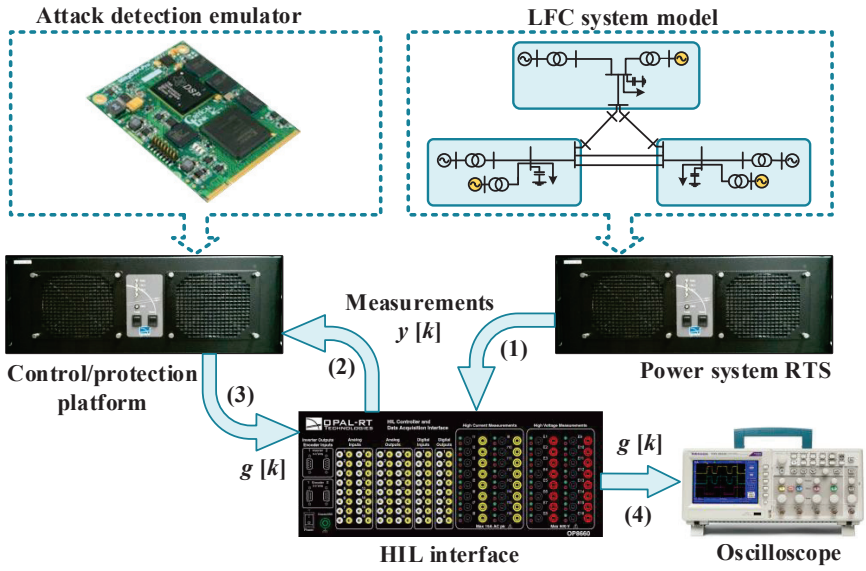


Figure 8.9: HIL setup.

technique uses 16 GB of RAM, and its speed is 3.33 GHz. Using this processor, the minimum simulation step size that allows running the proposed FDIA-detection algorithm in real-time for the three-area test system is 4 ms. Since the AGC system time step (2 s) is substantially larger than 4 ms, the proposed method can be implemented in real-time for this system. Additionally, since the RFs of the Main SUIE and all AISUIEs must be converted to a voltage in order to be shown by the oscilloscope and as the voltages of the I/O ports are limited to 15 V, the RFs are scaled down by a factor of 1/100. In this subsection two scenarios are investigated:

• The attack defined in Scenario 4 of the previous subsection targets the system for 110 s. When the power measurements of the tie-line that connects Areas 1 and 2 are increased by 5% in Scenario 4, the RFs of the Main SUIE and AISUIEs B and C increase, as shown in Fig. 8.10. The time and voltage divisions for all sub-figures in Fig. 8.10 are set to 25 s and 1 V, respectively. The increases in the RFs of the Main SUIE and AISUIEs B and C are about 5.2, 1.75, and 1.75 V, respectively, one time step after the attack starts. Thus, the RFs exceed their thresholds, signifying that $h_{T_2,1}$ is targeted, as previously indicated.

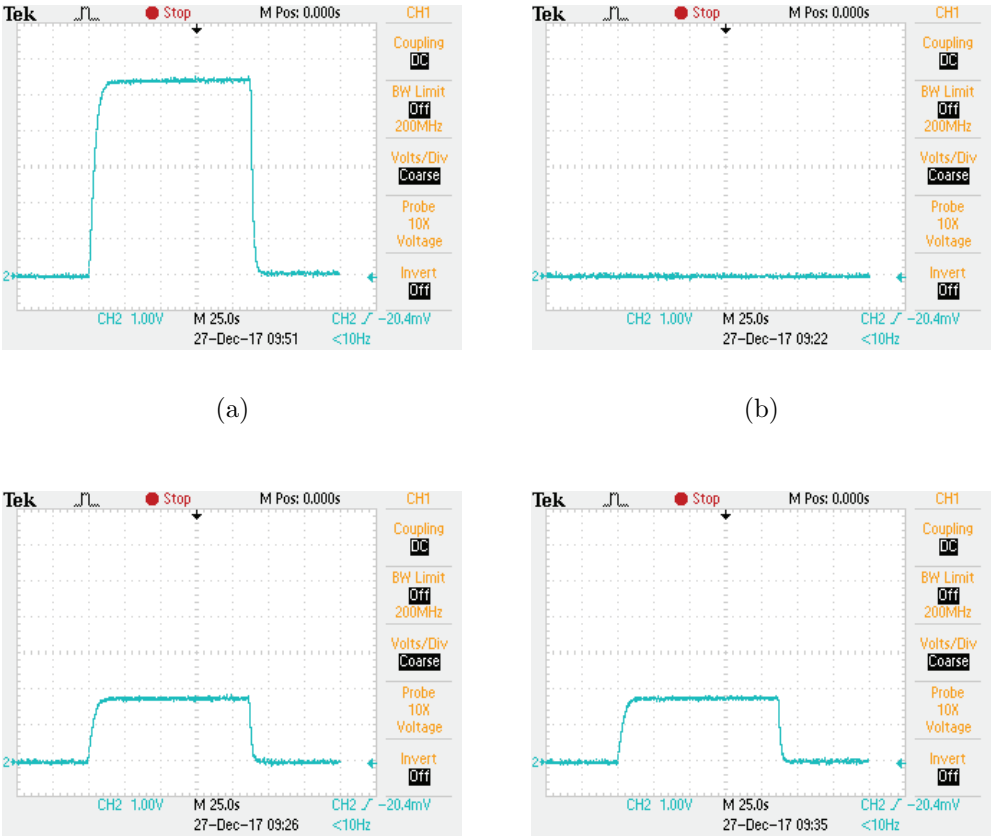


Figure 8.10: Scenario 4 RFs obtained by RTS, (a) Main SUIE, (b) AISUIE *A*, (c) AISUIE *B*, (d) AISUIE *C*.

• Scenario 7: This scenario starts an FDIA by increasing the power measurements of the tie-line connecting Areas 1 and 3 by 5%, i.e., $h_{T_3,1} = 5\%$; after 35 s, this tie-line's measurements are increased by 10% instead of 5%; after 40 s, $h_{T_3,1}$ is changed to 15%; and finally, the attack ends 110 s after its inception. The results of this scenario are shown in Fig. 8.11. In all sub-figures of 8.11, the time division is set to 25 s, while the voltage division is set to 5 V for Fig. 8.11a and to 1 V for Figs. 8.11b-8.11d. The Main SUIE's RF reaches 3.5 V in Fig. 8.11a after the first step of the attack is carried out, demonstrating that an attack has been initiated. The RF of the Main SUIE increases in three steps up to

about 15 V, indicating the three stages of this FDIA. On the other hand, as shown in Table 8.1, FDIAs against this tie-line's power measurements have not been modeled in AISUIEs A, C and E. Therefore, in addition to the Main SUIE's RF, the RFs of AISUIEs A and C rise in Figs. 8.11b and 8.11d. However, the RF of AISUIE B does not grow, since attack input $h_{T_3,1}$ is modeled in AISUIE B as an unknown input.

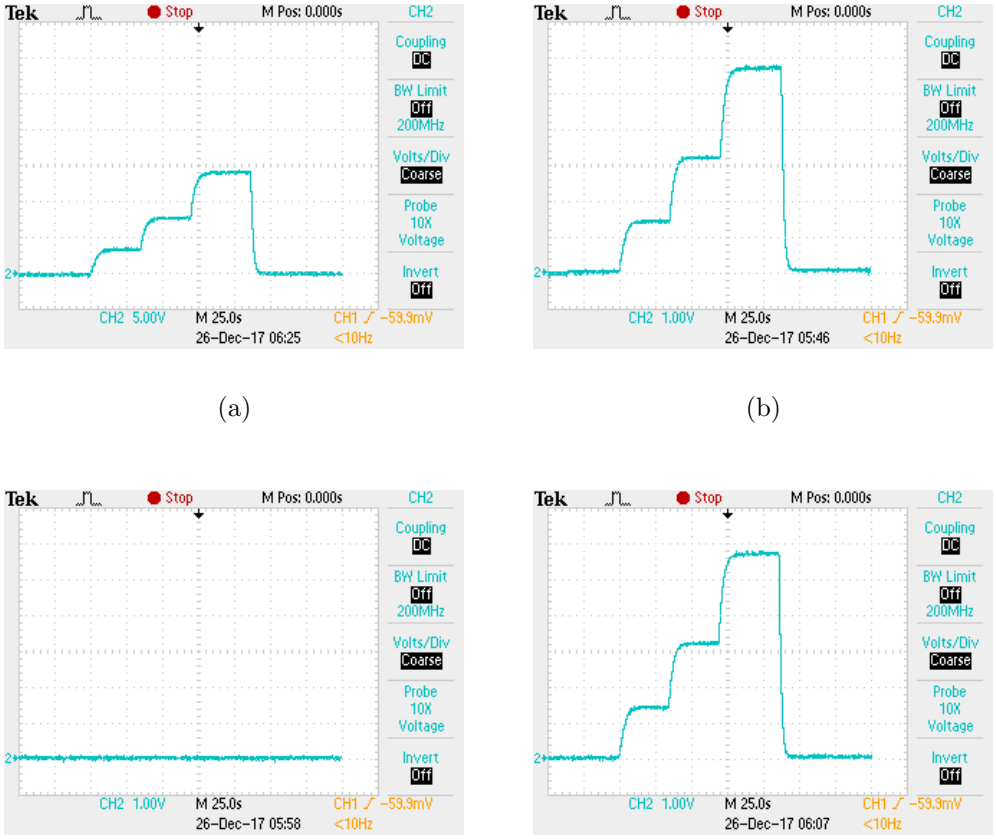


Figure 8.11: Scenario 7 RFs obtained by RTS, (a) Main SUIE, (b) AISUIE A, (c) AISUIE B, (d) AISUIE C.

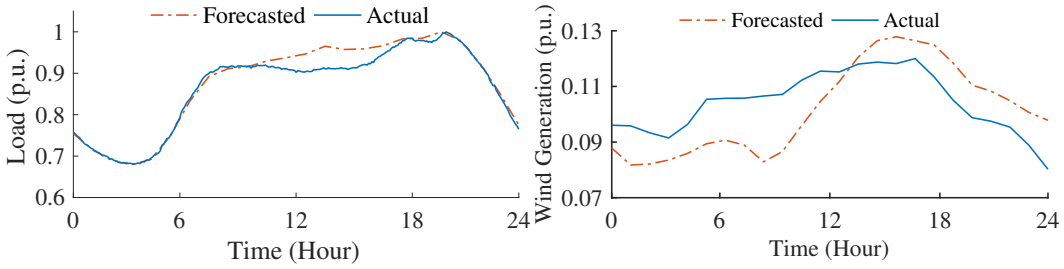


Figure 8.12: Load and wind generation profiles used for comparative analysis (a) Load, (b) Wind generation.

8.3.3 Comparative Analysis

As explained in Section 8.1, one of the main advantages of the proposed method is its independence from load changes in the network. Therefore, unlike other techniques, e.g., in [2, 38], the proposed method does not require forecasted data for the system load and the generation of intermittent renewable energy sources, such as wind and solar, for detecting FDIAs. Therefore, the performance of the proposed method is not affected by forecasting-techniques' error. Considering uncertainties in load and wind generation forecasts, the following scenarios compare the performance of the proposed method with the anomaly detection engine in [2] from the perspective of false alarms:

• Scenario 8: In this scenario, the actual and forecasted load and wind-generation profiles (Fig. 8.12) for each area of the three-area test system have been extracted from the New England ISO website [136]. These profiles are related to September 1st, 2017, and are normalized based on the peak-load of the day. In this scenario, the scheduled tie-line powers are considered to be 300, 60, and 240 MW for tie-lines 1-2, 1-3, and 2-3, respectively. To compare the proposed method with that in [2], the anomaly-detection engine presented in this reference is simulated. Using the forecasted load and wind-generation profiles in Fig. 8.12, parameters ACE_{max}, ACE_{min}, and δ_2 for each hour are obtained such that false alarms are minimized (Fig. 8.13). Using the obtained values, the anomaly-detection engine generates three false positive alarms at hours 8, 13, and 14 when the load and wind generation changes with the actual profiles in Fig. 8.12. These alarms are generated due

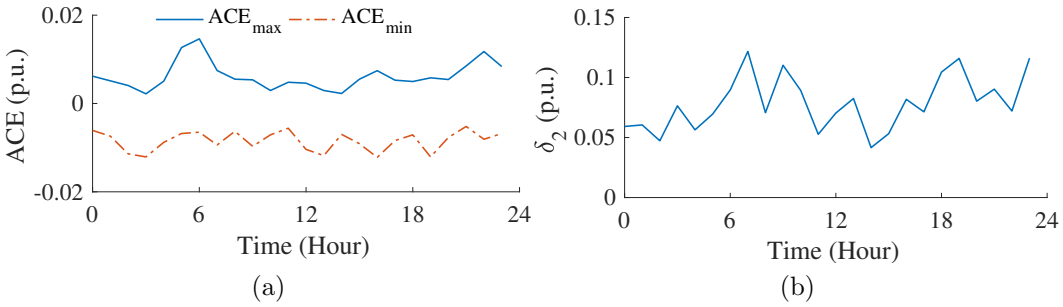


Figure 8.13: Parameters of the method proposed by [2] obtained for Scenario 7, (a) ACE_{max} and ACE_{min}, (b) δ_2.

to the large error between the forecasted and actual load and wind generation at these hours. On the other hand, the RF of the Main SUIE during this scenario is shown in Fig. 8.14. Due to the independence of the proposed method from load changes in the system, the RF is less than the defined threshold at all times, and thus it does not generate any false positive during this period.

- Scenario 9: This scenario shows that the independence from load changes in the system is a critical feature, since raising false positive alarms due to load changes can potentially lead to system instability. To illustrate this issue, over-frequency elements of the protective relays are set based on the guidelines for Western Interconnection, USA [137]. According to this setting, the over-frequency elements of generators trip if the frequency (i) exceeds 60.6 Hz and does not fall below this threshold within 180 s, (ii) exceeds 61.6 Hz and does not recover within 30 s, or (iii) surpasses 61.7 Hz. In this scenario, the forecasted load and wind generation are considered to be perfectly matched with the actual ones. However, at $t = 100$ s, a short-circuit fault happens in Area 2 of the three-area system. The fault removal protective relays lead to 20% load loss in this area. Since faults are generally unpredictable, their effects on the forecasted ACE cannot be considered. Thus, the anomaly-detection engine generates a false positive alarm, due to the large ACE signal created after the short-circuit fault. As the alarm is raised, the actual ACE values are replaced by forecasted values, and are sent to the AGC system of Area 2 once every 5 minutes. However, because the AGC system in Area 2 does not contribute properly to frequency regulation due to its erroneous inputs, this area's frequency exceeds 60.6 Hz,

as shown in Fig. 8.15. Therefore, the relays detect an over-frequency. After 3 minutes, the relays pick up based on their settings, tripping the generators. This issue renders the system unstable.

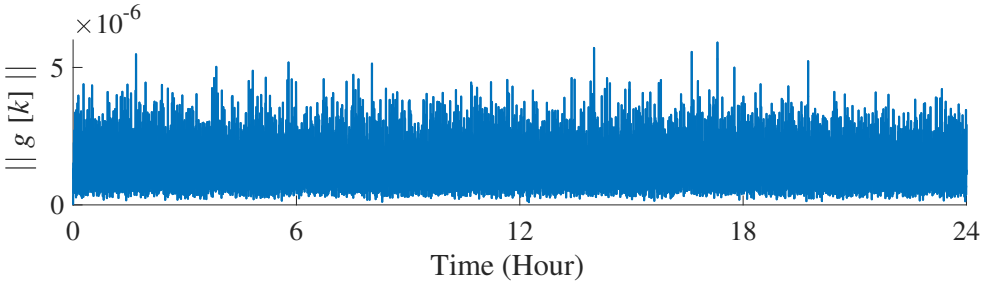


Figure 8.14: Main SUIE's RF during Scenario 7.

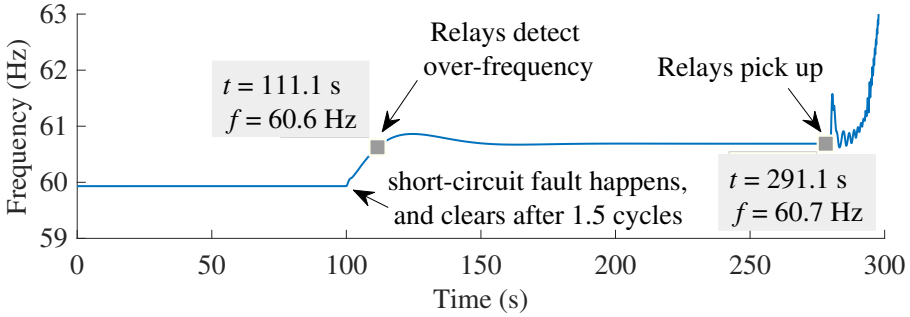


Figure 8.15: System frequency during Scenario 8.

8.4 Conclusion

This chapter proposed a method for detecting and identifying FDIAs against AGC systems in the presence of measurement and process noise. This method uses a SUIE that estimates the LFC system's states without requiring the real-time load changes in the grid. FDIAs are detected by comparing the SUIE's RF with a predefined threshold. To identify FDIAs, a number of AISUIEs were developed. A certain combination of attack inputs is among the unknown inputs of each AISUIE. Thus, if an FDIA happens, the RFs of all AISUIEs that

lack the respective attack input in their model increase. Implementing the proposed method for a three-area system using MATLAB/Simulink showed that this method properly detects and identifies FDIAs in the presence of noise, without requiring information about load changes in the grid. Additionally, the proposed method was tested using the OPAL RTS, and was compared with another method in the literature.

Chapter 9

Conclusions

9.1 Summary

The main objectives of this dissertation were divided into two main groups: (i) to introduce LCDRs as vulnerable protective elements in AC and DC power systems, in terms of cyber-attacks, and to address this issue by proposing methods that detect intrusions in a timely fashion, and (ii) to present AGC systems as susceptible controllers in power networks, and to propose application-based measures to make this controller robust against cyber-attacks. On this basis, the dissertation was divided into two parts. In the first part, the vulnerabilities of LCDRs to cyber-attacks were discussed and illustrated first. The destructiveness of cyber-attacks against LCDRs in both AC and DC systems was then demonstrated through three case studies. Afterwards, two methods were proposed to address the cyber-security problem of AC LCDRs, and one technique was presented to make DC LCDRs cyber-resilient. The first method for AC LCDRs was proposed for SV-based ones, and the second method can be employed in both SV-based and phasor-based relays. Both methods are initiated after LCDRs' pickup to confirm the occurrence of faults and to differentiate them from cyber-attacks.

The second part of the dissertation, on the other hand, focused on the other group of objectives. To this aim, first the vulnerabilities of AGC systems were discussed, and the LFC system model under FDIAs was obtained. Afterwards, to prove the potentials and

destructiveness of cyber-attacks against AGC systems, an SHA was proposed to disrupts the normal operation of this controller quickly and undetectably. Finally, two methods were proposed to detect and identify intrusions against AGC systems, and to make this controller robust against attacks. Both methods work without requiring load data in the system, in contrast to other methods presented in the literature. Additionally, the second proposed method takes into account the process and measurement noise and minimizes the noise effect on attack-detection accuracy.

The contents of each chapter can be summarized as follows:

• Chapter 2 unveiled the vulnerabilities of AC and DC LCDRs to cyber-attacks, and elaborated on how intrusions can target this relay type in both types of systems. The mathematical formulation of cyber-attacks against both AC and DC LCDRs and the criteria that must be met in order to trip the lines protected by each relay type were discussed next. In particular, a number of attack strategies were simulated for AC LCDRs to illustrate how cyber-attacks can move the operating point of this relay type into the trip zone. Finally, three case studies were presented to demonstrate the destructiveness of coordinated attacks against AC and DC LCDRs. It was shown that coordinated attacks can result in a kind of instability, depending on the attack strategy, and potentially lead to a system collapse.

• To detect attacks and differentiate them from faults, Chapter 3 proposed an attack-detection method for SV-based AC LCDRs. This method is initiated immediately after LCDRs pick up. In the proposed method, an SV-based AC LCDR detects attacks by comparing its terminal's estimated and locally-measured voltages in each sequence. To estimate the local voltage for each sequence, an LCDR uses a UIOs, the local and remote measurements, and the state-space model of the faulty line, all associated with that sequence. The difference between measured and estimated local voltages in each sequence is small during internal faults, since in such situations the proposed method's state-space model, based on which the UIO operates, and the actual system model are the same. Nonetheless, these two models differ during FDIAs, resulting in a large difference between the estimated and measured voltages. As a result, monitoring the the above-mentioned difference in both sequences can be used to confirm faults.

• Similar to Chapter 3, Chapter 4 presented a method for detecting attacks targeting AC

LCDRs, yet for both SV-based and phasor-based types. In the proposed method, when an LCDR pick up, its PS and NS submodules calculate and measure the superimposed voltages at the relay's local terminal. Attacks are then detected if the difference between the calculated and measured superimposed voltages in any sequence exceeds the defined threshold for that sequence.

• Chapter 5 presented an attack-detection method by which DC LCDRs can differentiate between cyber-attacks and faults using local measurements. The proposed method installs a POC, which includes an inductor and a capacitor in parallel, at each converter's terminal. A POC thus resonates and generates a damped sinusoidal component with a specific frequency during faults. However, this specific frequency component is not generated by POCs during cyber-attacks, load-changes, and other non-fault events in the system, and thus it can be regarded as a fault signature. On this basis, the proposed attack-detection submodule incorporated in LCDRs verify the occurrence of faults by applying FFT to the voltage across POCs in real-time and capturing the magnitude of the component oscillating with this specific frequency. Detecting this specific frequency thus validates an LCDR's tripping decision. Accordingly, a cyber-attack is flagged if an LCDR picks up without detecting the specific frequency.

• Chapter 6 began by explaining an AGC system's operating principal and alarms, its vulnerabilities to cyber-attacks, and the potential destructiveness of attacks targeting this controller. Afterwards, a number of basic attacks were introduced against AGC systems, and their impacts on power system operation were studied. An SHA was formulated and optimized next to disrupt the normal operation of AGC systems quickly. The SHA was designed such that no AGC alarm is raised, so the attack remains undetectable. Additionally, this chapter introduced the LFC system state-space model in under attack.

• Chapter 7 proposed a method to detect and identify intrusions against an AGC system. In contrast to other techniques in the literature, this method works independently from load data in the system. The proposed method detects attacks by estimating the LFC system's states using a UIO, and calculating the UIO's RF. An increase in the UIO's RF over a predefined threshold signifies an attack, since in normal conditions, the estimated and measured values for LFC states are ideally the same. This method also identifies attacks by designing a number of identification UIOs.

• Analogous to Chapter 7, Chapter 8 proposed a method for detecting and identifying FDIAs against AGC systems. However, the method proposed in Chapter 8 takes into account measurement and process noise as well. Therefore, instead of a UIO, a SUIE was used to estimate the states of LFC systems and calculate the RF. Attacks were then detected by comparing the SUIE's RF with a predefined threshold. Additionally, the proposed method identifies FDIAs by utilizing a number of AISUIEs.

9.2 Contributions

The research presented in this dissertation made the following main contributions:

- Introduced LCDRs as vulnerable protection relays and proposed a novel intrusion-detection method for unveiling attacks targeting SV-based AC LCDRs.
- Developed another attack-detection technique for AC LCDRs, that can be employed in both LCDR types.
- Proposed an attack detection method for DC LCDRs, that can differentiate between attacks and faults in a few microseconds.
- Developed basic attacks against AGC systems and investigated their impacts on power system operation. Additionally, it formulated an SHA to disrupt the normal operation of AGC systems quickly and undetectably.
- Presented a new model for describing LFC systems under attack. This model can be used for identification purposes and for analyzing the system during FDIAs.
- Presented an anomaly-based intrusion-detection method for discovering FDIAs targeting AGC systems. The method works without requiring load data in the system. Additionally, it identifies the parameters that are targeted and differentiates attacks from other abnormal non-attack events, such as faults.
- Presented another intrusion-detection and -identification method for AGC systems. This method utilizes a SUIE for detecting attacks, and it works independently from

load data in the system. Additionally, by optimally designing the SUIE's gain, the proposed method minimized the effect of noise on detection accuracy. Therefore, unlike with existing methods in the literature, with the proposed method, load forecast errors do not affect detection accuracy, and noise impact is minimized.

9.3 Directions for Future Work

Further research on the cyber-security of protection and control systems in general, and LCDRs and AGC systems in particular, may include the topics listed below:

1. Utilizing machine learning techniques for detecting attacks and differentiating them from faults.
2. investigating the performance of multi-terminal high-voltage DC networks under cyber-attacks targeting voltage regulation system.
3. Investigating the effect of cyber-attacks against AGC systems on electricity markets, and proposing attack scenarios accordingly.

References

[1] *L90 Line Differential Relay – UR Series Instruction Manual*, GE Multilin, Markham, ON, Canada, 2006, version 4.9x. [Online]. Available: https://www.gegridsolutions.com/products/manuals/l90/l90man-m2.pdf

[2] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, March 2014.

[3] (2016) Duke energy CEO: Cyber-threats grow; EPA lawsuit clarifying. [Online]. Available: https://www.newsobserver.com/news/business/article63393057.html

[4] R. S. Ross, S. W. Katzke, and L. A. Johnson, "Minimum security requirements for federal information and information systems," Tech. Rep., 2006.

[5] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," in *The State of the Art in Intrusion Prevention and Detection*. Auerbach Publications, 2014, pp. 139–154.

[6] J. C. Das, *Power System Protective Relaying*, 1st ed., ser. Power Systems Handbook Volume 3. CRC Press, 2018.

[7] "Ukraine power cut was cyber-attack," 2017. [Online]. Available: http://www.bbc.com/news/technology-38573074

[8] (2016) Hackers are hitting israel's energy sector with a severe cyber attack. [Online]. Available: https://www.businessinsider.com/israel-electric-cyberattack-2016-1

[9] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 23–36, March 2017.

[10] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[11] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," Schweitzer Engineering Laboratories Inc., Pullman, WA, USA, Tech. Rep., 2017.

[12] V. Gurevich, *Cyber and Electromagnetic Threats in Modern Relay Protection.* ch. 4, CRC Press, 2014.

[13] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436–447, Apr. 2017.

[14] H. Miller, J. Burger, N. Fischer, and B. Kasztenny, "Modern line current differential protection solutions," in *63rd Annual Conference for Protective Relay Engineers*, Mar. 2010, pp. 1–25.

[15] S. D. A. Fletcher, P. J. Norman, S. J. Galloway, P. Crolla, and G. M. Burt, "Optimizing the roles of unit and non-unit protection methods within DC microgrids," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 2079–2087, Dec 2012.

[16] M. Monadi, C. Gavriluta, A. Luna, J. I. Candela, and P. Rodriguez, "Centralized protection strategy for medium voltage DC microgrids," *IEEE Trans. Power Del.*, vol. 32, no. 1, pp. 430–440, Feb 2017.

[17] C. Yuan, M. A. Haj-ahmed, and M. S. Illindala, "Protection strategies for medium-voltage direct-current microgrid at a remote area mine site," *IEEE Trans. Ind. Electron.*, vol. 51, no. 4, pp. 2846–2853, July 2015.

[18] S. Dhar and P. K. Dash, "Differential current-based fault protection with adaptive threshold for multiple PV-based DC microgrid," vol. 11, no. 6, pp. 778–790, May 2017.

[19] S. Dhar, R. K. Patnaik, and P. K. Dash, "Fault detection and location of photovoltaic based DC microgrid using differential protection strategy," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4303–4312, Sept 2018.

[20] S. H. Horowitz and A. G. Phadke, *Power system relaying*. John Wiley & Sons, ch. 5-6, 2008.

[21] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[22] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, March 2017.

[23] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, Accepted for publication, 2018.

[24] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. Smart Grid*, Accepted for publication, 2018.

[25] J. Hong, R. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, Accepted for publication, 2018.

[26] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1477–1481, July 2007.

[27] J. Hong and C. C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, , accepted for publication, 2017.

[28] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[29] Y. Yang *et al.*, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1092–1102, Jun. 2014.

[30] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly detection based on zone partition for security protection of industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4257–4267, May 2018.

[31] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, July 2017.

[32] L. Chen, X. Lin, Z. Li, F. Wei, N. Jin, R. Lyu, and C. Liu, "Remedial pilot main protection scheme for transmission line independent of data synchronism," *IEEE Trans. Smart Grid*, , accepted for publication, 2017.

[33] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2442–2451, June 2018.

[34] J. T. Hagen and B. E. Mullins, "TCP veto: A novel network attack and its application to SCADA protocols," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2013, pp. 1–6.

[35] Y. Yang, H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, and S. Sezer, "Cybersecurity test-bed for IEC 61850 based smart substations," in *2015 IEEE Power Energy Society General Meeting*, July 2015, pp. 1–5.

[36] P. Kundur, *Power System Stability and Control*. New York: McGraw-hill, Chs. 11 and 12, 1994.

[37] M. Govindarasu, A. Hann, and P. Sauer, "Cyber-physical systems security for smart grid," *Future Grid Initiative White Paper*, PSERC, 2012.

[38] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[39] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 223–232, Jan 2015.

[40] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, Mar. 2016.

[41] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, accepted for publication, 2017.

[42] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *49th IEEE Conference on Decision and Control (CDC)*, Dec. 2010, pp. 5973–5978.

[43] R. Tan, H. H. Nguyen, E. Y. S. Foo, X. Dong, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Optimal false data injection attack against automatic generation control in power grids," in *ACM/IEEE 7th International Conference on Cyber-Physical Systems*, 2016, pp. 1–10.

[44] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed," in *2015 IEEE Power Energy Society General Meeting*, July 2015, pp. 1–5.

[45] T. S. Ustun and R. H. Khan, "Multiterminal hybrid protection of microgrids over wireless communications network," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2493–2500, Sep. 2015.

[46] B. Kasztenny, N. Fischer, K. Fodero, and A. Zvarych, "Communications and data synchronization for line current differential schemes," in *proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA*, 2011.

[47] *SEL-387L Relay – Line Current Differential Instruction Manual*, Schweitzer Engineering Laboratories, Pullman, Washington, USA, Jan. 2016. [Online]. Available: https://selinc.com/products/387L

[48] S. Ward *et al.*, "Cyber security issues for protective relays; c1 working group members of power system relaying committee," in *IEEE Power Engineering Society General Meeting*, June 2007, pp. 1–8.

[49] *SIPROTEC 7SD61–Differential protection relay for two line ends*, Nuremberg, Germany, Jul. 2013. [Online]. Available: http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/protection/line-differential/pages/7sd61.aspx

[50] J. Holbach, N. Schsuter, and A. Struecker, "Secure data communication for line differential relays," in *2009 Power Systems Conference*, March 2009, pp. 1–6.

[51] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of pmu data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, , accepted for publication, 2017.

[52] "Ieee guide for application of digital line current differential relays using digital communication," *IEEE Std C37.243-2015*, pp. 1–72, Aug 2015.

[53] "Protection systems using telecommunications," CIGRE, CE/SC 34 34/35.11, Ref. No. 192, Tech. Rep., 2001.

[54] D. M. E. Ingram, P. Schaub, D. A. Campbell, and R. R. Taylor, "Quantitative assessment of fault tolerant precision timing for electricity substations," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 10, pp. 2694–2703, Oct 2013.

[55] M. Kabir-Querrec, S. Mocanu, J. M. Thiriet, and E. Savary, "A test bed dedicated to the study of vulnerabilities in IEC 61850 power utility automation networks,"

in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2016, pp. 1–4.

[56] C. Jiwen and L. Shanmei, "Cyber security vulnerability assessment for smart substations," in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Oct. 2016, pp. 1368–1373.

[57] *IEC 61850: Communication networks and systems for power utility automation*, editiond 2, 2013.

[58] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, accepted for publication, 2016.

[59] Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based scada networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, April 2017.

[60] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[61] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, Mar. 2016.

[62] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC applications to time synchronization spoofing," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4601–4612, Sept 2018.

[63] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sept. 2016.

[64] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[65] P. Kaplunovich and K. Turitsyn, "Fast and reliable screening of N-2 contingencies," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4243–4252, Nov 2016.

[66] *SEL-411L Advanced Line Differential Protection, Automation, and Control System*, SEL, Pullman, WA, USA, Jun. 2013. [Online]. Available: https://www.selinc.com/SEL-411L

[67] A. J. Conejo, F. D. Galiana, and I. Kockar, "Z-bus loss allocation," *IEEE Trans. Power Syst.*, vol. 16, no. 1, pp. 105–110, Feb 2001.

[68] T. Yong and R. Lasseter, "Optimal power flow formulation in market of retail wheeling," in *IEEE Power Engineering Society. 1999 Winter Meeting*, vol. 1, Jan 1999, pp. 394–398.

[69] P. M. Anderson, *Power system control and stability*, 1st ed. Iowa State University Press, 1980.

[70] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *International Conference on Information Security and Cryptology*. Springer, 2005, pp. 186–198.

[71] N. Mithulananthan, C. A. Canizares, J. Reeve, and G. J. Rogers, "Comparison of PSS, SVC, and STATCOM controllers for damping power system oscillations," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 786–792, May 2003.

[72] T. Athay, R. Podmore, and S. Virmani, "A practical method for the direct analysis of transient stability," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 2, pp. 573–584, March 1979.

[73] N. Chaudhuri, B. Chaudhuri, R. Majumder, and A. Yazdani, *Multi-terminal direct-current grids: Modeling, analysis, and control*. John Wiley & Sons, chapter 6, 2014.

[74] "IEEE guide for protective relay applications to distribution lines," *IEEE Std C37.230-2007*, pp. 1–100, 2008.

[75] L. Xu and D. Chen, "Control and operation of a DC microgrid with variable generation and energy storage," *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2513–2522, Oct 2011.

[76] A. S. Dobakhshari and A. M. Ranjbar, "A novel method for fault location of transmission lines by wide-area voltage measurements considering measurement errors," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 874–884, Mar. 2015.

[77] J. Izykowski, E. Rosolowski, M. M. Saha, M. Fulczyk, and P. Balcerek, "A fault-location method for application with current differential relays of three-terminal lines," *IEEE Trans. Power Del.*, vol. 22, no. 4, pp. 2099–2107, Oct 2007.

[78] R. P. Medeiros, F. B. Costa, and K. M. Silva, "Power transformer differential protection using the boundary discrete wavelet transform," *IEEE Trans. Power Del.*, vol. 31, no. 5, pp. 2083–2095, Oct 2016.

[79] K. Ogata, *Discrete-Time Control Systems*. Prentice-Hall International, ch. 5, 1995.

[80] L. Silverman, "Inversion of multivariable linear systems," *IEEE Trans. Autom. Control*, vol. 14, no. 3, pp. 270–276, Jun 1969.

[81] S. Sundaram and C. N. Hadjicostis, "Delayed observers for linear systems with unknown inputs," *IEEE Trans. Autom. Control*, vol. 52, no. 2, pp. 334–339, Feb 2007.

[82] A. Saberi, A. A. Stoorvogel, and P. Sannuti, "Exact, almost and optimal input decoupled (delayed) observers," vol. 73, no. 7, pp. 552–581, Jan 2000.

[83] J. S. Golan, *Foundations of Linear Algebra*. Springer Science & Business Media, 2013, vol. 11, ch. 14, pp. 198-203.

[84] C.-T. Chen, *Linear system theory and design*. Oxford University Press, Inc., Ch. 8, p. 250, 1995.

[85] S. Sundaram and C. N. Hadjicostis, "On delayed observers for linear systems with unknown inputs," in *Proceedings of the 44th IEEE Conference on Decision and Control*, Dec 2005, pp. 7210–7215.

[86] R. L. Williams and D. A. Lawrence, *Linear State-space Control Systems*. John Wiley & Sons, 2007.

[87] M. Sain and J. Massey, "Invertibility of linear time-invariant dynamical systems," *IEEE Transactions on Automatic Control*, vol. 14, no. 2, pp. 141–149, April 1969.

[88] J. Kautsky, N. Nichols, and P. Van Dooren, "Robust pole assignment in linear state feedback," vol. 41, no. 5, pp. 1129–1155, 1985.

[89] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*. New York: Clarendon Press, ch. 2, p 86, 1988.

[90] A. Hooshyar and R. Iravani, "A new directional element for microgrid protection," *IEEE Trans. Smart Grid*, accepted for publication, 2017.

[91] A. Hooshyar and M. Sanaye-Pasand, "CT saturation detection based on waveform analysis using a variable-length window," *IEEE Trans. Power Del.*, vol. 26, no. 3, pp. 2040–2050, July 2011.

[92] J. R. Marti, L. R. Linares, and H. W. Dommel, "Current transformers and coupling-capacitor voltage transformers in real-time simulations," *IEEE Trans. Power Del.*, vol. 12, no. 1, pp. 164–168, Jan 1997.

[93] M. M. Haji and W. Xu, "Online determination of external network models using synchronized phasor data," *IEEE Trans. Power Syst.*, accepted for publication, 2016.

[94] W. Xu, I. R. Pordanjani, Y. Wang, and E. Vaahedi, "A network decoupling transform for phasor data based voltage stability analysis and monitoring," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 261–270, Mar. 2012.

[95] A. Rahmati, M. A. Dimassi, R. Adhami, and D. Bumblauskas, "An overcurrent protection relay based on local measurements," *IEEE Trans. Ind. Appl.*, vol. 51, no. 3, pp. 2081–2085, May 2015.

[96] K. Vu, M. M. Begovic, D. Novosel, and M. M. Saha, "Use of local measurements to estimate voltage-stability margin," in *Proceedings of the 20th International Conference on Power Industry Computer Applications*, May 1997, pp. 318–323.

[97] P. M. Anderson, *Analysis of Faulted Power Systems*. Wiley-IEEE Press, Ch. 4, 1995, pp. 71–151.

[98] S. M. Abdelkader and D. J. Morrow, "Online thevenin equivalent determination considering system side changes and measurement errors," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2716–2725, Sept 2015.

[99] A. T. Johns and S. K. Salman, *Digital protection for power systems*. IET, Ch. 2, 1997.

[100] J. Das, *Power system analysis: short-circuit load flow and harmonics*. CRC press, ch. 3, 2016.

[101] H. Saadat, *Power system analysis*. WCB/McGraw-Hill, Chs. 6, 9, and 10, 1999.

[102] *Line differential protection RED670 Application manual*, ABB, Vasteras, Sweden, June 2010. [Online]. Available: https://library.e.abb.com/public/9922d42ef60039dec12578570041dd47/1MRK505186-UEN_D_en_Application_manual__Line_Differential_Protection_IED_RED_670_1.1.pdf

[103] J. Yang, J. E. Fletcher, and J. O'Reilly, "Short-circuit and ground fault analyses and location in vsc-based DC network cables," *IEEE Trans. Ind. Electron.*, vol. 59, no. 10, pp. 3827–3837, Oct 2012.

[104] E. S. K. C. A. Desoer, *Basic circuit theory*. Chs. 5 and 14, Tata McGraw-Hill Education, 1969.

[105] S. R. Pulikanti, G. Konstantinou, and V. G. Agelidis, "DC-link voltage ripple compensation for multilevel active-neutral-point-clamped converters operated with SHE-PWM," *IEEE Trans. Power Del.*, vol. 27, no. 4, pp. 2176–2184, Oct 2012.

[106] H. J. Sira-Ramirez and R. Silva-Ortigoza, *Control design techniques in power electronics devices*. Springer Science & Business Media, 2006.

[107] J. Duenas, "Isolated, shunt-based current sensing reference design," Texas Instruments, Tech. Rep., 2014. [Online]. Available: http://www.ti.com/lit/ug/tidu384a/tidu384a.pdf

[108] M. J. Thompson, "Percentage restrained differential, percentage of what?" in *2011 64th Annual Conference for Protective Relay Engineers*, April 2011, pp. 278–289.

[109] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. John Wiley & Sons, ch. 10, pp. 485-497, 2012.

[110] "Frequency event detection methodology," The North American Electric Reliability Corporation (NERC), Oct. 2012. [Online]. Available: http://www.nerc.com/comm/oc/rslandingpagedl/candidatefrequencyevents/frequency_event_detection_methodology_october_2012.pdf

[111] N. R. Panel, "Frequency operating standards determination," *National Electricity Code Administrator Limited, Australia*, 2001.

[112] G. R. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, Ch. 4, 2004.

[113] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP3 protocol," *Critical Infrastructure Protection III*, pp. 67–81, 2009.

[114] "National SCADA testbed (NSTB) assessments summary report: Common industrial control system cyber security weaknesses," *Idaho National Laboratory (INL)*, May 2010.

[115] I. Darwish, O. Igbe, O. Celebi, T. Saadawi, and J. Soryal, "Smart grid DNP3 vulnerability analysis and experimentation," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, Nov 2015, pp. 141–147.

[116] I. A. Siddavatam and F. Kazi, "Security assessment framework for cyber physical systems: A case-study of DNP3 protocol," in *2015 IEEE Bombay Section Symposium (IBSS)*, Sept 2015, pp. 1–6.

[117] *700G series – generator protection technical manual*, Selnic. [Online]. Available: https://selinc.com/products/700G/

[118] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright, "Distributed MPC strategies with application to power system automatic generation control," *IEEE Trans. Control Syst. Technol.*, vol. 16, no. 6, pp. 1192–1206, Nov 2008.

[119] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Grid*. Springer, 2015, pp. 303–328.

[120] S. Liu, P. X. Liu, and A. E. Saddik, "Modeling and stability analysis of automatic generation control over cognitive radio networks in smart grids," *IEEE Trans. Syst., Man, Cybern.*, vol. 45, no. 2, pp. 223–234, Feb 2015.

[121] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr 2013.

[122] P. Jovanovic and S. Neves, *Practical Cryptanalysis of the Open Smart Grid Protocol*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 297–316.

[123] K. Kursawe and C. Peters, "Structural weaknesses in the open smart grid protocol," in *2015 10th International Conference on Availability, Reliability and Security*, Aug 2015, pp. 1–10.

[124] D. Ichalal and S. Mammar, "On unknown input observers for LPV systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 9, pp. 5870–5880, Sept 2015.

[125] S. Stankovic, "Stochastic inclusion principle applied to decentralized automatic generation control," vol. 72, no. 3, pp. 276–288, 1999.

[126] S. Sundaram and C. N. Hadjicostis, "Optimal state estimators for linear systems with unknown inputs," in *Proceedings of the 45th IEEE Conference on Decision and Control*, Dec. 2006, pp. 4763–4768.

[127] C. K. Chui and G. Chen, *Kalman Filtering: with Real-Time Applications*. Springer Berlin Heidelberg, ch. 5, 1991.

[128] P. Grigolini, "The projection approach to the problem of colored noise," *Physics Letters A*, vol. 119, no. 4, pp. 157–162, 1986.

[129] R. Singh, B. C. Pal, and R. A. Jabr, "Distribution system state estimation through gaussian mixture model of the load as pseudo-measurement," vol. 4, no. 1, pp. 50–59, Jan. 2010.

[130] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. MIT Press, Cambridge MA, ch. 3, 1990.

[131] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[132] M. Matar and R. Iravani, "FPGA implementation of the power electronic converter model for real-time simulation of electromagnetic transients," *IEEE Trans. Power Del.*, vol. 25, no. 2, pp. 852–860, Apr. 2010.

[133] B. Lu, X. Wu, H. Figueroa, and A. Monti, "A low-cost real-time hardware-in-the-loop testing approach of power electronics controls," *IEEE Trans. Ind. Electron.*, vol. 54, no. 2, pp. 919–931, Apr. 2007.

[134] M. A. Azzouz and E. F. El-Saadany, "Multivariable grid admittance identification for impedance stabilization of active distribution networks," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1116–1128, May 2017.

[135] J.-N. Paquin, C. Dufour, and J. Bélanger, "A hardware-in-the-loop simulation platform for prototyping and testing of wind generator controllers," in *CIGRÉ Canada Conference on Power Systems Winnipeg*, 2008.

[136] [Online]. Available: https://www.iso-ne.com

[137] "Standard PRC-024-2 – generator frequency and voltage protective relay settings," The North American Electric Reliability Corporation (NERC), Jan. 2015. [Online]. Available: http://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-024-2.pdf

[138] *Compact Load-Shedding relay PML630 series – Technical Manual*, ABB, Aug. 2016. [Online]. Available: https://library.e.abb.com/public/e6307807487d48c4a485da9dd4e6b385/PML630_oper_757183_ENe.pdf

[139] W. Li, A. Monti, and F. Ponci, "Fault detection and classification in medium voltage DC shipboard power systems with wavelets and artificial neural networks," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 11, pp. 2651–2665, Nov 2014.

APPENDICES

Appendix A

Description of the 39-bus new England Test System in Chapters 2, 3, 4, and 7

The details of the 39-bus New England power system [72] shown in Figures 2.2 and 7.6 are presented in this section. This test system includes 3 areas as illustrated in Fig. 7.6. The base power is 100 MW, and the generated voltages and powers of generators are shown in Table A.1. For each area, governor and turbine time constants as well as droop and damping coefficients have been considered similar to those of the three-area test system in C (Table C.2). The system consists of 34 lines and 19 loads, whose data is provided in Tables A.2 and A.3.

In this test system, Lines are protected by distance and overcurrent relays. Additionally, Lines 6-11, 4-14, 2-3, and 3-18 are critical and protected by LCDRs, which are set based on the default settings of [1]. The frequency relays utilized in this test system are Over Frequency Relays (OFRs) and Under Frequency Relays (UFRs), which are used for Under Frequency Load Shedding (UFLS), as well as for over- and under-frequency generator rejection schemes [138], [117]. The UFLS scheme sheds 10%, 15%, and 20% of the load when the frequency drops below 59.2 Hz, 58.8 Hz, and 58 Hz, respectively [36], and trips the generator if the frequency reaches 57.8 Hz [137]. The OFRs trip generators if the

frequency (i) exceeds 60.5 Hz and does not fall below this threshold within $10^{(90.93-1.45f)}$ s, or (ii) surpasses 61.8 Hz [137].

Table A.1: Generators' voltage and power in 39-bus New England system

Bus	V [kV]	P [pu]	Q [pu]
31	225.860	5.713	3.639
30	240.925	2.500	0.832
32	226.113	6.500	0.015
33	229.356	6.320	0.697
34	232.829	5.080	1.488
35	241.339	6.500	1.670
36	244.605	5.600	0.754
37	236.394	5.400	-0.353
38	236.095	8.300	-0.005
39	236.900	10.00	-0.365

Table A.2: Transmission line characteristics of 39-bus New England system

Line		R [pu]	X [pu]	B [pu]
From Bus	To Bus			
1	2	0.1522	1.7872	30.3821
1	39	0.0265	0.6613	19.8375
2	3	0.0208	0.2412	4.1090
2	25	0.0637	0.0782	1.3284
3	4	0.0293	0.4800	4.9893
3	18	0.0155	0.1871	3.0085
4	5	0.0108	0.1733	1.8174
4	14	0.0109	0.1761	1.8862
5	6	0.0006	0.0072	0.1194
5	8	0.0095	0.1327	1.7490
6	7	0.0058	0.0895	1.0999
6	11	0.0061	0.0711	1.2050
7	8	0.0019	0.0224	0.3796
8	9	0.0883	1.3941	14.6094
9	39	0.0265	0.6613	31.7400
10	11	0.0018	0.0196	0.3317
10	13	0.0018	0.0196	0.3317
13	14	0.0096	0.1079	1.8412
14	15	0.0413	0.4982	8.4028
15	16	0.0090	0.0935	1.7006
16	17	0.0066	0.0838	1.2637
16	19	0.0330	0.4023	6.2718
16	21	0.0114	0.1928	3.6393
16	24	0.0019	0.0368	0.4245
17	18	0.0061	0.0711	1.1443
17	27	0.0238	0.3166	5.8864
21	22	0.0118	0.2074	3.7993
22	23	0.0061	0.0975	1.8749
23	24	0.0815	1.2961	13.3678
25	26	0.1094	1.1038	17.5310
26	27	0.0218	0.2286	3.7264
26	28	0.2156	2.3771	39.1264
26	29	0.3769	4.1328	68.0426
28	29	0.0224	0.2412	0.3978

Table A.3: Load characteristics of 39-bus New England system

Bus	P [pu]	Q [pu]
3	3.220	0.024
4	5.000	1.840
7	2.338	0.840
8	5.220	1.760
12	0.075	0.880
15	3.200	1.530
16	3.294	0.323
18	1.580	0.300
20	6.800	1.030
21	2.740	1.150
23	2.475	0.846
24	3.086	-0.922
25	2.240	0.472
26	1.390	0.170
27	2.810	0.755
28	2.060	0.276
29	2.835	0.269
31	0.092	0.046
39	11.04	2.500

Appendix B

Description of the DC Test System in Chapters 2 and 5

The details of the 7-bus medium-voltage DC test system shown in Fig. 2.22 is presented in this section, [67]. The system voltage level is 5 kV, which is typical for DC networks [139]. This test system consists of eight lines with the resistance and inductance of 0.017 Ω/km and 2 mH/km, respectively, and has seven converter terminals. The AC/DC two-level converter connected to Bus 1 interfaces the DC grid to an AC system. Converters #2, #4 and #7 are of boost type and connect distributed energy sources to the DC grid. Each individual converter, consisting of a 200 μH inductor and a 10 mF capacitor, controls the DC system voltage through V-I droop control, where the voltage is linearly reduced when the converter's output current is increased. Simultaneously, these converters ensure power balance in the system. On the other hand, each buck converter, #3, #5, and # 6, includes a 200 μH inductor and a 10 mF capacitor, connects DC loads to the grid, and adopts constant power control.

Considering the action of the droop control loop, the current reference provided by the voltage control loop is given by

$$I_{i,inner,ref} = \underbrace{(V_{DC,i,ref} - V_{DC,i} - I_i * k_{droop,i})}_{\text{error}} \times G_{PI}(s) \tag{B.1}$$

where $I_{i,inner,ref}$ and I_i are the inductor's reference and output measured currents of the i-th converter, respectively; $V_{DC,i,ref}$ and V_i are the reference and measured terminal voltages of the i-th converter, respectively; $k_{droop,i}$ is the droop gain of the i-th converter; and $G_{PI}(s)$ denotes the PI controller.

Appendix C

Description of the Three-Area Test System in Chapters 6, 7, and 8

The three-area test system is shown in Fig. 6.2 [36]. The original system in [36] is a real two-area power network, but it is small for LFC studies. Thus, a third area is added to the two-area system in this study to make it appropriate for LFC studies. Each area consists of two 20 kV, 900 MVA generation units with the parameters shown in Table C.1. One generator in each area is equipped with an AGC system. The parameters related to the LFC and AGC systems are shown in Table C.2.

The per unit length susceptance and series impedance of all of the tie-lines are $B = 3.308$ $\mu\mho$/km and $z = 0.053 + j0.53$ Ω/km. Additionally, the rating voltage and power of transformers are 20/230 kV and 900 MVA, and their leakage reactance is 15%. Capacitor banks installed in Areas 1 to 3 are 200, 315, and 330 MVAr, respectively. The generated power and loads for each area also are shown in Table C.3.

The utilized protective relays include UFRs, which are used for UFLS scheme, Rate-of-Change-of-Frequency (ROCOF) relays, and OFRs [138], [117]. The UFLS scheme sheds 10%, 15%, and 20% of the total load if the frequency drops bellow 59.2 Hz, 58.8 Hz, and 58 Hz, respectively [36]. Furthermore, for frequencies below 59.4 Hz, 10%, 15%, 20%, and 25% of the total load are shed if the rate provided by the ROCOF elements of the relays exceeds -0.4 Hz/s, -1 Hz/s, -2 Hz/s, and -4 Hz/s, respectively [36]. OFRs trip generators if

the frequency (i) exceeds 60.5 Hz and does not fall below this threshold within $10^{90.93-1.45f}$ s, or (ii) surpasses 61.8 Hz [137].

Table C.1: Generator Specifications for the Three-Area Test System

Parameter	Value (p.u.)	Parameter	Value (p.u.)	Parameter	Value (p.u.)	Parameter	Value (p.u.)
X_d	1.8	X'_q	0.55	T'_{do}	0.8	A_{Sat}	0.015
X_q	1.7	X''_d	0.25	T'_{qo}	0.4	B_{Sat}	9.6
X_l	0.2	X''_q	0.25	T''_{do}	0.03	ψ_{T1}	0.9
X'_d	0.3	R_a	0.0025	T''_{qo}	0.05	K_D	0

Table C.2: LFC System Parameters in Each Area of the Three-Area Test System

Parameter	Value		
	Area 1	Area 2	Area 3
H: Generators inertia constant (s)	6.5	6.175	6.175
T_g: Governor time constant (s)	0.08	0.3	0.3
T_{ch}: Turbine time constant (s)	0.4	0.36	0.36
R: Speed droop coefficient (Hz/MW)	2.4	2.4	2.4
D: Damping coefficient (MW/Hz)	0.014	0.008	0.008

Table C.3: Generated and Consumed Powers in the Three-Area Test System

Area	Generated power (MW or MVAr)				Load (MW or MVAr)	
1	$P_{G_1} = 730$	$Q_{G_1} = 213$	$P_{G_2} = 803$	$Q_{G_2} = 115$	$P_{L_1} = 967$	$Q_{L_1} = 90$
2	$P_{G_3} = 802$	$Q_{G_3} = 122$	$P_{G_4} = 780$	$Q_{G_4} = 133$	$P_{L_2} = 1590$	$Q_{L_2} = 90$
3	$P_{G_5} = 677$	$Q_{G_5} = 78$	$P_{G_6} = 742$	$Q_{G_6} = 98$	$P_{L_3} = 1698$	$Q_{L_3} = 95$

Appendix D

Proof of Theorem 5

To prove Theorem 5, the following theorem should be used:

Theorem 9. *Consider the following discrete system*

$$\langle S\rangle: \quad \begin{cases} \mathbb{X}[k+1] = \mathbb{A}\mathbb{X}[k] + \mathbb{B}_u\mathbb{U}_u[k] \\ \mathbb{Y}[k] = \mathbb{C}\mathbb{X}[k] \end{cases} \tag{D.1}$$

which is associated with the following continuous system

$$(S): \quad \begin{cases} \dot{\mathbb{X}}(t) = \mathbb{A}_c\mathbb{X}(t) + \mathbb{B}_{c,u}\mathbb{U}_u(t) \\ \mathbb{Y}(t) = \mathbb{C}\mathbb{X}(t) \end{cases} \tag{D.2}$$

and $\mathbb{X} \in \mathbb{R}^n$, $\mathbb{U}_u \in \mathbb{R}^N$, and $\mathbb{Y} \in \mathbb{R}^p$. Condition (7.5) holds for $\langle S\rangle$—or equivalently $\langle S\rangle$ is invertible/observable—if and only if it holds for (S) [87]. □

In the following, it is proved that $\alpha = 2$ satisfies (7.5) for continuous LFC systems in multi-area power networks. This proof can be done in four steps as follows:

• *Step 1*: *Determining the general state vector $\mathbb{X}_i$ and matrices $\mathbb{A}_{ii}$, $\mathbb{A}_{ij}$, $\mathbb{B}_{u,i}$, and $\mathbb{C}_i$ for each area:* For Area i, the total number of generators and the number of generators equipped with an AGC system are denoted by G_i and ψ_i, respectively. This area is connected to Areas $j \in \delta_i$, where δ_i denotes the set of all areas that are connected to Area i. As explained in Section 6.4.1, $\mathbb{X}_i$ and $\mathbb{A}_{i,i}$ for Area i are defined as:

$$\mathbb{X}_i = \left[\begin{array}{c|c|ccccccc|ccccccc|ccc} \Delta P_{tie_i} & \Delta\omega_i & \Delta P_{m_{1,i}} & \cdots & \Delta P_{m_{\psi_i,i}} & \Delta P_{m_{\psi_i+1,i}} & \cdots & \Delta P_{m_{G_i,i}} & \Delta P_{v_{1,i}} & \cdots & \Delta P_{v_{\psi_i,i}} & \Delta P_{v_{\psi_i+1,i}} & \cdots & \Delta P_{v_{G_i,i}} & \Delta P_{c_{1,i}} & \cdots & \Delta P_{c_{\psi_i,i}} \end{array} \right]^T \tag{C.3}$$

$$\mathbb{A}_{ii} = \left[\begin{array}{c|c|ccccccc|ccccccc|ccc} 0 & \sum_{j\in\delta_i} T_{ij} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline \frac{-1}{2H_i} & \frac{-D_{e_i}}{2H_i} & \frac{1}{2H_i} & \cdots & \frac{1}{2H_i} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \frac{-1}{T_{ch_{1,i}}} & \cdots & 0 & 0 & \cdots & 0 & \frac{1}{T_{ch_{1,i}}} & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{-1}{T_{ch_{\psi_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & \frac{1}{T_{ch_{\psi_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & \frac{-1}{T_{ch_{\psi_i+1,i}}} & \cdots & 0 & 0 & \cdots & 0 & \frac{1}{T_{ch_{\psi_i+1,i}}} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & \frac{-1}{T_{ch_{G_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & \frac{1}{T_{ch_{G_i,i}}} & 0 & \cdots & 0 \\ \hline 0 & \frac{-1}{R_{1,i}T_{g_{1,i}}} & 0 & \cdots & 0 & 0 & \cdots & 0 & \frac{-1}{T_{g_{1,i}}} & \cdots & 0 & 0 & \cdots & 0 & \frac{1}{T_{g_{1,i}}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{-1}{R_{\psi_i,i}T_{g_{\psi_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & \frac{-1}{T_{g_{\psi_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & \frac{1}{T_{g_{\psi_i,i}}} \\ 0 & \frac{-1}{R_{\psi_i+1,i}T_{g_{\psi_i+1,i}}} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \frac{-1}{T_{g_{\psi_i+1,i}}} & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{-1}{R_{G_i,i}T_{g_{G_i,i}}} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & \frac{-1}{T_{g_{G_i,i}}} & 0 & \cdots & 0 \\ \hline -k_{1,i} & -k_{1,i}\beta_i & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ -k_{\psi_i,i} & -k_{\psi_i,i}\beta_i & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array} \right] \tag{C.4}$$

where the number of states in $\mathbb{X}_i$ is $2G_i + \psi_i + 2$. For Area $j \in \delta_i$, $\mathbb{A}_{ij}$ is a matrix with all elements equal to zero, except the elements located on row 1 and column 2, which are equal to $-T_{i,j}$. For all other areas, $\mathbb{A}_{ij} \in \mathbb{R}^{(2G_i+\psi_i+2)\times(2G_i+\psi_i+2)}$ is a zero matrix. The unknown input and output matrices $\mathbb{B}_{u,i} \in \mathbb{R}^{(2G_i+\psi_i+2)\times 1}$ and $\mathbb{C}_i \in \mathbb{R}^{(\psi_i+2)\times(2G_i+\psi_i+2)}$ are defined as follows:

$$\mathbb{B}_{u,i} = \left[\begin{array}{c|c|ccc|ccc|ccc|ccc} 0 & \frac{-1}{2H_i} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]^T \tag{D.5}$$

$$\mathbb{C}_i = \left[\begin{array}{c|c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{array}\right] \tag{D.6}$$

• *Step 2*: *Determining the state-space matrices of the whole N-Area system using the obtained matrices for individual areas:* Using (6.29), the state matrix $\mathbb{A}_c \in \mathbb{R}^n$, unknown input matrix $\mathbb{B}_{c,u} \in \mathbb{R}^N$, and output matrix $\mathbb{C} \in \mathbb{R}^p$ for an N-area power system are obtained as:

$$\mathbb{A}_c = \begin{bmatrix} \mathbb{A}_{1,1} & \mathbb{A}_{1,2} & \cdots & \mathbb{A}_{1,N} \\ \mathbb{A}_{2,1} & \mathbb{A}_{2,2} & \cdots & \mathbb{A}_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{A}_{N,1} & \mathbb{A}_{2,2} & \cdots & \mathbb{A}_{N,N} \end{bmatrix} \tag{D.7}$$

$$\mathbb{B}_{c,u} = diag\begin{bmatrix} \mathbb{B}_{u,1} & \mathbb{B}_{u,2} & \cdots & \mathbb{B}_{u,N} \end{bmatrix} \tag{D.8}$$

$$\mathbb{C} = diag\begin{bmatrix} \mathbb{C}_1 & \mathbb{C}_2 & \cdots & \mathbb{C}_N \end{bmatrix} \tag{D.9}$$

• *Step 3*: *Forming matrices* $\mathcal{J}_{u,\alpha}$ *and* $\mathcal{J}_{u,\alpha-1}$: Using (7.2c), (7.6), (D.7)-(D.9), and by selecting $\alpha = 2$, $\mathcal{J}_{u,2}$ and $\mathcal{J}_{u,1}$ are as follows:

$$\mathcal{J}_{u,2} = \begin{bmatrix} O_{p\times n} & O_{p\times n} & O_{p\times n} \\ \mathbb{C}\mathbb{B}_{c,u} & O_{p\times n} & O_{p\times n} \\ \mathbb{C}\mathbb{A}_c\mathbb{B}_{c,u} & \mathbb{C}\mathbb{B}_{c,u} & O_{p\times n} \end{bmatrix} \tag{D.10}$$

$$\mathcal{J}_{u,1} = \begin{bmatrix} O_{p\times n} & O_{p\times n} \\ \mathbb{CB}_{c,u} & O_{p\times n} \end{bmatrix} \tag{D.11}$$

in which,

$$\mathbb{CB}_{c,u} = \begin{bmatrix} \mathbb{C}_1\mathbb{B}_{u,1} & 0 & \cdots & 0 \\ 0 & \mathbb{C}_2\mathbb{B}_{u,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbb{C}_N\mathbb{B}_{u,N} \end{bmatrix} = \left[\begin{array}{c|c|c|c} 0 & 0 & \cdots & 0 \\ \frac{-1}{2H_1} & 0 & \cdots & 0 \\ O_{\psi_1\times 1} & O_{\psi_1\times 1} & \cdots & O_{\psi_1\times 1} \\ \hline 0 & 0 & \cdots & 0 \\ 0 & \frac{-1}{2H_2} & \cdots & 0 \\ O_{\psi_2\times 1} & O_{\psi_2\times 1} & \cdots & O_{\psi_2\times 1} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \frac{-1}{2H_N} \\ O_{\psi_N\times 1} & O_{\psi_N\times 1} & \cdots & O_{\psi_N\times 1} \end{array}\right] \tag{D.12}$$

$$\mathbb{CA}_c\mathbb{B}_{c,u} = \begin{bmatrix} \mathbb{C}_1\mathbb{A}_{11}\mathbb{B}_{u,1} & \mathbb{C}_1\mathbb{A}_{12}\mathbb{B}_{u,2} & \cdots & \mathbb{C}_1\mathbb{A}_{1N}\mathbb{B}_{u,N} \\ \mathbb{C}_2\mathbb{A}_{21}\mathbb{B}_{u,1} & \mathbb{C}_2\mathbb{A}_{22}\mathbb{B}_{u,2} & \cdots & \mathbb{C}_2\mathbb{A}_{2N}\mathbb{B}_{u,N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{C}_N\mathbb{A}_{N1}\mathbb{B}_{u,1} & \mathbb{C}_N\mathbb{A}_{N2}\mathbb{B}_{u,2} & \cdots & \mathbb{C}_N\mathbb{A}_{NN}\mathbb{B}_{u,N} \end{bmatrix} =$$

$$\left[\begin{array}{c|c|c|c} \frac{-\sum_{j\in\delta_1} T_{1j}}{2H_1} & \frac{T_{12}}{2H_2} & \cdots & \frac{T_{1N}}{2H_N} \\ \frac{D_1}{4H_1^2} & 0 & \cdots & 0 \\ \Psi^1_{\psi_1\times 1} & O_{\psi_1\times 1} & \cdots & O_{\psi_1\times 1} \\ \hline \frac{T_{21}}{2H_1} & \frac{-\sum_{j\in\delta 2} T_{2j}}{2H_2} & \cdots & \frac{T_{2N}}{2H_N} \\ 0 & \frac{D_2}{4H_2^2} & \cdots & 0 \\ O_{\psi_2\times 1} & \Psi^2_{\psi_2\times 1} & \cdots & O_{\psi_2\times 1} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \frac{T_{N1}}{2H_1} & \frac{T_{N2}}{2H_2} & \cdots & \frac{-\sum_{j\in\delta_N} T_{Nj}}{2H_N} \\ 0 & 0 & \cdots & \frac{D_N}{4H_N^2} \\ O_{\psi_N\times 1} & O_{\psi_N\times 1} & \cdots & \Psi^N_{\psi_N\times 1} \end{array}\right] \tag{D.13}$$

In (D.12) and (D.13), $\Psi^i_{\psi_i\times 1}$ is defined as:

$$\Psi^i_{\psi_i\times 1} = \left[\begin{array}{ccc} \frac{k_{1,i}\beta_i}{2H_i} & \cdots & \frac{k_{\psi_i,i}\beta_i}{2H_i} \end{array}\right]^T \tag{D.14}$$

• *Step 4*: *Determining the rank of $\mathcal{J}_{u,2}$ and $\mathcal{J}_{u,1}$:* Since all elements of $\mathcal{J}_{u,1}$ except $\mathbb{CB}_{c,u}$ are zero in (D.11), the rank of $\mathcal{J}_{u,1}$ is equal to the rank of $\mathbb{CB}_{c,u}$. As shown in (D.12), the rank of $\mathbb{CB}_{c,u}$ is N, because all N non-zero elements of $\mathbb{CB}_{c,u}$ are located on different rows and columns. On the other hand,

$$rank\left(\mathcal{J}_{u,2}\right) = rank\left(\left[\begin{array}{ccc} O_{p\times n} & O_{p\times n} & O_{p\times n} \\ \mathbb{CB}_{c,u} & O_{p\times n} & O_{p\times n} \\ \mathbb{CA}_c\mathbb{B}_{c,u} & \mathbb{CB}_{c,u} & O_{p\times n} \end{array}\right]\right) = rank\left(\left[\begin{array}{cc} \mathbb{CB}_{c,u} & O_{p\times n} \\ \mathbb{CA}_c\mathbb{B}_{c,u} & \mathbb{CB}_{c,u} \end{array}\right]\right) \tag{D.15}$$

where, $\Upsilon = \left[\begin{array}{cc} \mathbb{CB}_{c,u} & 0 \\ \mathbb{CA}_c\mathbb{B}_{c,u} & \mathbb{CB}_{c,u} \end{array}\right]$ is as follows:

Column $\rightarrow$	1	2	$\cdots$	N	$N+1$	$N+2$	$\cdots$	N
Row $\downarrow$								
1	0	0	$\cdots$	0	0	0	$\cdots$	0
2	$\frac{-1}{2H_1}$	0	$\cdots$	0	0	0	$\cdots$	0
	$O_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$\cdots$	$O_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$\cdots$	$O_{\psi_1\times 1}$
	0	0	$\cdots$	0	0	0	$\cdots$	0
	0	$\frac{-1}{2H_2}$	$\cdots$	0	0	0	$\cdots$	0
	$O_{\psi_2\times 1}$	$O_{\psi_2\times 1}$	$\cdots$	$O_{\psi_2\times 1}$	$O_{\psi_2\times 1}$	$O_{\psi_2\times 1}$	$\cdots$	$O_{\psi_2\times 1}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
	0	0	$\cdots$	0	0	0	$\cdots$	0
	0	0	$\cdots$	$\frac{-1}{2H_N}$	0	0	$\cdots$	0
	$O_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$\cdots$	$O_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$\cdots$	$O_{\psi_N\times 1}$
$\Re_1$	$\frac{\sum_{j\in\delta_1} T_{1j}}{2H_1}$	$\frac{T_{12}}{2H_2}$	$\cdots$	$\frac{T_{1N}}{2H_N}$	0	0	$\cdots$	0
$\Re_2$	$\frac{D_1}{4H_1^2}$	0	$\cdots$	0	$\frac{-1}{2H_1}$	0	$\cdots$	0
$\Re_3 - \Re_{\psi_1+2}$	$\Psi^1_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$\cdots$	$O_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$O_{\psi_1\times 1}$	$\cdots$	$O_{\psi_1\times 1}$
$\Re_{\psi_1+3}$	$\frac{T_{21}}{2H_1}$	$\frac{\sum_{j\in\delta_2} T_{2j}}{2H_2}$	$\cdots$	$\frac{T_{2N}}{2H_N}$	0	0	$\cdots$	0
$\Re_{\psi_1+4}$	0	$\frac{D_2}{4H_2^2}$	$\cdots$	0	0	$\frac{-1}{2H_2}$	$\cdots$	0
$\Re_{\psi_1+5} - \Re_{\psi_1+\psi_2+4}$	$O_{\psi_2\times 1}$	$\Psi^2_{\psi_2\times 1}$	$\cdots$	$O_{\psi_2\times 1}$	$O_{\psi_2\times 1}$	$O_{\psi_2\times 1}$	$\cdots$	$O_{\psi_2\times 1}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\Re_{p-2}$	$\frac{T_{N1}}{2H_1}$	$\frac{T_{N2}}{2H_2}$	$\cdots$	$\frac{\sum_{j\in\delta_N} T_{Nj}}{2H_N}$	0	0	$\cdots$	0
$\Re_{p-1}$	0	0	$\cdots$	$\frac{D_N}{4H_N^2}$	0	0	$\cdots$	$\frac{-1}{2H_N}$
$\Re_p$	$O_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$\cdots$	$\Psi^N_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$O_{\psi_N\times 1}$	$\cdots$	$O_{\psi_N\times 1}$

(C.16)

To find rank(Υ), one should start by adding the rows of $[\mathbb{C}\mathbb{A}_c\mathbb{B}_{c,u} \;\; \mathbb{C}\mathbb{B}_{c,u}]$, called $\{\Re_1 \cdots \Re_p\}$, to $[\mathbb{C}\mathbb{B}_{c,u} \;\; 0]$, which has N independent rows. Addition of $\{\Re_2, \Re_{\psi_1+4}, \Re_{\psi_1+\psi_2+6}, \cdots, \Re_{p-1}\}$ increases the rank by N, since these rows are independent from each other, and they cannot be built by linearly combining the rows of $[\mathbb{C}\mathbb{B}_{c,u} \;\; 0]$. This is because the non-zero elements of $\mathbb{C}\mathbb{B}_{c,u}$ are located in columns $N+1$ to $2N$. However, other remaining rows are in the subspace spanned by the non-zero rows of $[\mathbb{C}\mathbb{B}_{c,u} \;\; 0]$, and thus these remaining rows do not affect the rank of Υ. As a result, the rank of $\mathcal{J}_{u,2}$ is $2N$, which yields

$$rank\left(\mathcal{J}_{u,2}\right) - rank\left(\mathcal{J}_{u,1}\right) = 2N - N = N \tag{D.17}$$

Therefore, the continuous state-space equation of an LFC system represented by (D.3)-(D.9) satisfies the invertibility/observability condition of (7.5), regardless of the number of generators that are controlled by the AGC system in each area. Therefore, according to Theorem 9, so does the discretized LFC system.

Appendix E

Feasibility of Stealthy FDIAs Against AGC Systems

This appendix investigates the feasibility of stealthy FDIAs against AGC system when the proposed method in Chapter 8 is utilized.

For an attack to remain stealthy at each time step, the last two terms of (8.35) must cancel out each other, i.e.,

$$\overline{\mathcal{L}}\,[k]\,\mathcal{M}_{\alpha}\mathcal{H}\,[k:k+\alpha]-\overline{\mathbb{B}}_{h}\mathbb{H}\,[k]=0 \tag{E.1}$$

This equation can be rewritten as

$$\underbrace{\left(\overline{\mathcal{L}}\,[k]\,\mathcal{M}_{\alpha}-\left[\overline{\mathbb{B}}_{h}\;\;O_{\alpha(n+p)\times z}\;\;\cdots\;\;O_{\alpha(n+p)\times z}\right]\right)}_{\theta[k]}\mathcal{H}\,[k:k+\alpha]=0 \tag{E.2}$$

In (E.2), the last z columns of $\theta[k]$ are zero, since the last z columns of $\mathcal{M}_{\alpha}$ in (8.34a) and $[\overline{B}_{h}\;O_{\alpha(n+p)\times z}\;\cdots\;O_{\alpha(n+p)\times z}]$ are zero. Therefore, $\theta[k]$ can be written as

$$\theta\,[k]=\left[\begin{array}{cccc}\theta_{1}[k] & \cdots & \theta_{\alpha}[k] & O_{\alpha(n+p)\times z}\end{array}\right] \tag{E.3}$$

where $\theta_{1}[k]$ to $\theta_{\alpha}[k]$ are sub-matrices of $\theta[k]$, each containing z columns. On the other

hand, as shown in (8.20), $\theta_1[k]$ to $\theta_\alpha[k]$ depend on $\overline{\mathcal{L}}_1[k]$, which is a sub-matrix of $\overline{\mathcal{L}}[k]$. $\overline{\mathcal{L}}_1[k]$ is not a constant matrix and should be specifically determined for each time step in real time using the estimation covariance matrix, as shown in (8.28). Therefore, due to the time-varying nature of $\overline{\Sigma}[k]$ in (8.29) and $\overline{\mathcal{L}}_1[k]$ in (8.28), an attacker does not access these matrices for any time step beforehand. Consequently, $\theta_1[k]$ to $\theta_\alpha[k]$ cannot be predicted before time step k.

Assume that an attacker initiates an LCDR against an AGC system at time step k. At this time step, the SIUE is estimating the states of the system at time step $k-\alpha$, since the SUIE is delayed for α time steps. Therefore, for a stealthy LCDR, $\mathbb{H}[k]$ must be designed such that (E.4) is met.

$$\begin{bmatrix} \theta_1[k-\alpha] & \cdots & \theta_\alpha[k-\alpha] & O_{\alpha(n+p)\times z} \end{bmatrix} \begin{bmatrix} O_{z\times 1} \\ \vdots \\ O_{z\times 1} \\ \mathbb{H}[k] \end{bmatrix} = 0 \tag{E.4}$$

In the first time step, any $\mathbb{H}[k]$ satisfies (E.4). The injected attack vector at time step k is denoted by $\mathbb{H}^*[k]$.

In the next time step, i.e., $k+1$, $\mathbb{H}[k+1]$ must be determined such that (E.5) holds:

$$\begin{bmatrix} \theta_1[k-\alpha+1] & \cdots & \theta_\alpha[k-\alpha+1] & O_{\alpha(n+p)\times z} \end{bmatrix} \begin{bmatrix} O_{z\times 1} \\ \vdots \\ O_{z\times 1} \\ \mathbb{H}^*[k] \\ \mathbb{H}[k+1] \end{bmatrix} = 0 \tag{E.5}$$

To satisfy (E.5), $\theta_\alpha[k-\alpha+1]\mathbb{H}^*[k]$ must be zero. As $\mathbb{H}^*[k]$ was determined in the previous time step without using $\theta_\alpha[k-\alpha+1]$, since $\theta_1[k-\alpha+1]$ to $\theta_\alpha[k-\alpha+1]$ were unknown in the previous time step when $\mathbb{H}^*[k]$ was formed, the probability of $\mathbb{H}^*[k]$ being in the null-space of $\theta_\alpha[k-\alpha+1]$ is practically zero. Accordingly, the probability of (E.5) being satisfied is zero.

Similarly, if the injected attack vector at time step $k+1$ is denoted by $\mathbb{H}^*[k+1]$, $\mathbb{H}[k+2]$

must be chosen such that

$$\begin{bmatrix} \theta_1[k-\alpha+2]^T \\ \vdots \\ \theta_{\alpha-2}[k-\alpha+2]^T \\ \theta_{\alpha-1}[k-\alpha+2]^T \\ \theta_{\alpha}[k-\alpha+2]^T \\ O_{z\times\alpha(n+p)} \end{bmatrix}^T \begin{bmatrix} O_{z\times1} \\ \vdots \\ O_{z\times1} \\ \mathbb{H}^*[k] \\ \mathbb{H}^*[k+1] \\ \mathbb{H}[k+2] \end{bmatrix} = 0 \tag{E.6}$$

In (E.6), if $\theta_{\alpha}[k-\alpha+2]\mathbb{H}^*[k+1] + \theta_{\alpha-1}[k-\alpha+2]\mathbb{H}^*[k]$ is equal to zero, this equation is satisfied. However, with the same rationale, the probability of (E.6) being satisfied is practically zero. This trend continues until the end of the attack. As a result, the probability of carrying out a stealthy attack is practically zero, and FDIAs will be detected one time step after their initiation.

Appendix F

List of Publications

The following is a list of publications by the author during doctoral studies.

F.1 Peer-Reviewed Journal Articles

[1] **A. Ameli**, A. Hooshyar, E. El-Saadany, and A. M. Youssef,"An Intrusion Detection Method for Line Current Differential Relays", *IEEE Transactions on Information Forensics and Security*, Apr., 2019.

[2] **A. Ameli**, A. Hooshyar, and E. El-Saadany, "Development of a Cyber-Resilient Line Current Differential Relay", *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 305 - 318, Jan. 2019.

[3] **A. Ameli**, A. Hooshyar, E. El-Saadany, and A. M. Youssef, "Attack Detection and Identification for Automatic Generation Control Systems", *IEEE Transactions on Power Systems*, vol. 13, no. 10, pp. 2575 - 2590, Oct. 2018.

[4] **A. Ameli**, A. Hooshyar, A. H. Yazdavar, E. El-Saadany, and A. M. Youssef, "Attack Detection for Load Frequency Control Systems Using Stochastic Unknown Input Estimators", *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575 - 2590, Oct. 2018.

F.2 Submitted Journal Articles

[1] **A. Ameli**, K. H. Saleh, A. Kirakosyan, and E. El-Saadany, "Developing a Cyber-Resilient Line Current Differential Relay for DC Microgrids", submitted to *IEEE Transactions on Power Delivery*, Apr. 2019.

F.3 Under-Preparation Journal Articles

[1] **A. Ameli**, A. Ayad, A. Hooshyar, and E. El-Saadany, "Intrusion Detection for Line Current Differential Relays Using Machine-Learning Techniques".

F.4 Conference Proceedings

[1] **A. Ameli**, A. Kirakosyan, K. A. Saleh, and E. El-Saadany, "Vulnerabilities of Line Current Differential Relays to Cyber-Attacks", *2018 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington DC, USA, Feb. 17 - 20, 2019.