Louisiana Tech University
Louisiana Tech Digital Commons

Doctoral Dissertations | Graduate School

Summer 2014

A knowledge discovery approach for the detection of power grid state variable attacks

Nathan Wallace
Louisiana Tech University

Follow this and additional works at: https://digitalcommons.latech.edu/dissertations

Part of the Electrical and Computer Engineering Commons, and the Other Computer Sciences Commons

Recommended Citation
Wallace, Nathan, "" (2014). *Dissertation*. 252.
https://digitalcommons.latech.edu/dissertations/252

This Dissertation is brought to you for free and open access by the Graduate School at Louisiana Tech Digital Commons. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of Louisiana Tech Digital Commons. For more information, please contact digitalcommons@latech.edu.

A KNOWLEDGE DISCOVERY APPROACH FOR THE DETECTION OF POWER GRID STATE VARIABLE ATTACKS

by

Nathan Wallace, B.S., B.S., M.S.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

COLLEGE OF ENGINEERING AND SCIENCE
LOUISIANA TECH UNIVERSITY

August 2014

UMI Number: 3662465

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI®
Dissertation Publishing

UMI 3662465
Published by ProQuest LLC 2015. Copyright in the Dissertation held by the Author.
Microform Edition © ProQuest LLC.
All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code.

ProQuest®

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

30th June 2014
Date

We hereby recommend that the dissertation prepared under our supervision by Nathan Wallace

entitled A Knowledge Discovery Approach for the Detection of Power Grid State Variable Attacks

be accepted in partial fulfillment of the requirements for the Degree of Doctor of Philosophy

Supervisor of Dissertation Research

Head of Department

Engineering
Department

Recommendation concurred in:

Advisory Committee

SIGNED BY TRAVIS ATKISON

Approved:

Director of Graduate Studies

Dean of the College

Approved:

Dean of the Graduate School

GS Form 13a
(6/07)

ABSTRACT

As the level of sophistication in power system technologies increases, the amount of system state parameters being recorded also increases. This data not only provides an opportunity for monitoring and diagnostics of a power system, but it also creates an environment wherein security can be maintained. Being able to extract relevant information from this pool of data is one of the key challenges still yet to be obtained in the smart grid. The potential exists for the creation of innovative power grid cybersecurity applications, which harness the information gained from advanced analytics. Such analytics can be based on the extraction of key features from statistical measures of reported and contingency power system state parameters. These applications, once perfected, will be able to alert upon potential cyber intrusions providing a framework for the creation of power system intrusion detection schemes derived from the cyber-physical perspective. With the power grid having a growing cyber dependency, these systems are becoming increasingly the target of attacks. The current power grid is undergoing a state of transition where new monitoring and control devices are being constantly added. These newly connected devices, by means of the cyber infrastructure, are capable of executing remote control decisions along with reporting sensor data back to a centralized location.

This dissertation is an examination of advanced data mining and data analytic techniques for the development of a framework for detecting malicious cyber activity in

the power grid based solely on reported power system state parameters. Through this examination, results indicate the successful development of a cyber-event detection framework capable of detecting and localizing 92% of the simulated cyber-events. In focusing on specific types of intrusions, this work describes the utilization of machine learning techniques to examine key features of multiple power systems for the detection of said intrusions. System analysis is preformed using the Newton-Raphson method to solve the nonlinear power system partial differential power flow equations for a 5-Bus and 14-Bus power system. This examination offers the theory and simulated implementation examples behind a context specific detection approach for securing the current and next generation's critical infrastructure power grid.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Thesis. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Thesis. Further, any portions of the Thesis used in books, papers, and other works must be appropriately referenced to this Thesis.

Finally, the author of this Thesis reserves the right to publish freely, in the literature, at any time, any or all portions of this Thesis.

Author Nate Walker

Date 24th July 2014

GS Form 14
(5/03)

DEDICATION

The work described in this dissertation is dedicated to my wonderful and supporting family whose efforts made this dissertation possible. To my father and mother, I am extremely grateful for all your love and support. To my amazing grandmother, Elaine, this dissertation is a testament to your work ethic as I have tried to mirror that mentality. I would also like to dedicate this work to my niece and nephew. Please always follow your dreams and never allow perceived limitations to dictate your destiny. Lastly, this work is dedicated to all the teachers and mentors that helped me over the years.

TABLE OF CONTENTS

ABSTRACT iii

DEDICATION vi

LIST OF TABLES xiv

LIST OF FIGURES xviii

ACKNOWLEDGMENTS xxiv

CHAPTER 1 INTRODUCTION 1

1.1 Motivation 3

1.1.1 Vulnerabilities 5

1.1.2 Data the Grid Offers 5

1.1.3 Why a Context Specific Approach 8

1.2 Statement of Hypothesis 9

1.3 Contributions 9

1.4 Organization 10

CHAPTER 2 BACKGROUND 12

2.1 Overview of Power Systems 12

2.1.1 Power Flow 13

2.1.2 State Estimation 16

2.2 Multivariate Analysis 17

2.3 Knowledge Discovery 20

2.3.1 Learning Techniques 22

2.3.2 Detection via Classification 23

2.3.3 Validation 23

CHAPTER 3 RELATED RESEARCH 26

3.1 Introduction 26

3.2 Bad Data Detection via State Estimation 27

3.3 Data Mining for Power Grid Security 28

3.4 Cyber-Event Detection via an IT Perspective 29

3.4.1 Proof of Concept ICS Attack 29

3.5 Cyber-Event Detection via a Physical Perspective 33

3.6 Conclusions 34

CHAPTER 4 DETECTION VIA STATE VARIABLES 36

4.1 Implementation 38

4.2 Approach Overview 39

4.3 Convergence Classification 40

4.3.1 Convergence Feature 41

4.3.2 Discriminant Classification 43

4.4 Instance Classification 46

4.4.1 Feature Extraction via Transformation 47

4.4.2 Classification 50

4.5 Localization 53

4.5.1 Grubbs Test 53

4.6 Conclusions 55

CHAPTER 5 SIMULATION MODELS 57

5.1 Introduction 57

5.2 Modeling Power Systems 57

5.2.1 5-Bus 58

5.2.2 IEEE 14-Bus 59

5.3 Monte Carlo Simulations 59

5.4 Cyber-Event Attack Models 60

5.4.1 Single Variate Attack of Type I 62

5.4.2 Multivariate Attack of Type I 62

5.4.3 Single Variate Attack of Type II 63

5.4.4 Multivariate Attack of Type II 64

5.5 Conclusions 64

CHAPTER 6 FEATURE EXTRACTION RESULTS 65

6.1 Introduction 65

6.2 Convergence Feature 66

6.2.1 5-Bus 66

6.2.2 IEEE 14-Bus 68

6.3 Dimensional Transformation 69

6.3.1 State Variables Retained for Transformation 70

6.3.2 Transformation Results 72

6.4 Univariate Statistics 79

6.4.1 5-Bus 79

6.4.2 IEEE 14-Bus 81

6.5 Conclusions 84

CHAPTER 7 SELECTION OF CLASSIFIER PARAMETERS 85

7.1 Introduction 85

7.2 Convergence Classifier 86

7.2.1 5-Bus 86

7.2.2 IEEE 14-Bus 88

7.2.3 Classifier Parameters Selected 89

7.3 Instance Classifier 90

7.4 Conclusions 91

CHAPTER 8 CYBER-EVENT IDENTIFICATION RESULTS 92

8.1 Introduction 92

8.2 False Positive Analysis 95

8.3 5-Bus Identification 97

8.3.1 True Positive Analysis 98

8.3.2 Convergence Classification 100

8.3.3 Instance Classification 102

8.3.4 False Negative Analysis 104

8.4 IEEE 14-Bus Identification 106

8.4.1 True Positive Analysis 106

8.4.2 Convergence Classification 108

8.4.3 Instance Classification 110

8.4.4 False Negative 113

8.5 Conclusions 114

CHAPTER 9 CYBER-EVENT SOURCE LOCALIZATION RESULTS 116

9.1 Introduction 116

9.2 False Positive Analysis 118

9.3 True Positive Analysis 119

9.4 5-Bus Localization Results 120

9.5 IEEE 14-Bus Localization Results 123

9.6 Conclusions 126

CHAPTER 10 STEALTHY ATTACKS 127

10.1 Introduction 127

10.2 5-Bus 128

10.3 IEEE 14-Bus 130

10.4 Conclusions 132

CHAPTER 11 CONCLUSIONS AND RECOMMENDATIONS 134

11.1 Introduction 134

11.2 Framework Classifiers and Parameters 135

11.3 Computational Constraints 136

11.4 Framework Performance 137

11.5 Conclusions 139

CHAPTER 12 FUTURE WORK 140

12.1 Introduction 140

12.2 Modifying Classifiers 141

12.2.1 Convergence Classifier 141

12.2.2 Instance Classifier 142

12.2.3 Localization 142

12.3 Examining Forensics Implementation 142

12.4 Increase Power System Features 143

12.5 Integration Into a Cyber-Physical Detection Scheme 144

12.6 Conclusions 148

APPENDIX A 5-BUS POWER SYSTEM 149

A.1 System Details 150

A.2 Power Flow Simulation Snapshots 151

A.3 State Parameter Variances from Monte Carlo Simulations 152

APPENDIX B 14-BUS POWER SYSTEM 155

B.1 System Details 156

B.2 Power Flow Simulation Snapshots 157

APPENDIX C PRINCIPAL COMPONENT ANALYSIS DIMENSIONAL TRANSFORMATIONS 165

C.1 5-Bus Transformation 166

C.1.1 Without Line Flows 166

C.1.2 With Line Flows 168

C.2 IEEE 14-Bus Transformation 170

C.2.1 Without Line Flows 170

C.2.2 With Line Flows 172

APPENDIX D CYBER-EVENT IDENTIFICATION PLOTS AND TABLES 174

D.1 5-Bus Identification 175

D.1.1 Without Line Flows 175

D.1.2 With Line Flows 179

D.2 IEEE 14-Bus Identification 183

D.2.1 Without Line Flows 183

D.2.2 With Line Flows 187

APPENDIX E CYBER-EVENT LOCALIZATION PLOTS AND TABLES 191

E.1 5-Bus Localization 192

E.1.1 Without Line Flows 192

E.1.2 With Line Flows 198

E.2 IEEE 14-Bus Localization 204

E.2.1 Without Line Flows 204

E.2.2 With Line Flows 210

BIBLIOGRAPHY 218

VITA 226

LIST OF TABLES

Table 1.1: Cybersecurity Statistics Concerning Power Systems 4

Table 1.2: Example of power data based on estimated average smart grid enabled utility readings per day. 7

Table 2.1: Calculations for the elements of the Jacobian matrix [1]. 15

Table 4.1: 5-Bus Data Matrix Features 50

Table 5.1: Attack Type Notation 62

Table 6.1: 5-Bus Convergence Parameters 67

Table 6.2: 14-Bus Convergence Parameters 68

Table 6.3: 5-Bus State Parameters Without Line Flows 70

Table 6.4: 5-Bus Power Line Flow Variables 71

Table 6.5: IEEE 14-Bus State Parameters Without Line Flows 71

Table 6.6: IEEE 14-Bus Power Line Flow Variables 72

Table 6.7: Data Matrix Sizes for Each of the Four Considered Cases 73

Table 6.8: Hotelling T^2 Statistics for Each of the Four Considered Cases 78

Table 6.9: 5-Bus Grubbs Test Parameters 80

Table 6.10: IEEE 14-Bus Grubbs Test Parameters for Variables 1-68 82

Table 6.11: IEEE 14-Bus Grubbs Test Parameters for Variables 69-136 83

Table 7.1: Selected Convergence Classifier Parameters for Each Topology 90

Table 7.2: Selected Instance Classifier Hotelling T2 91

Table 8.1: 5-Bus Without Line Flows SI Classification Results 95

Table 8.2: Detection Scheme False Positive Results 96

Table 8.3: Detection Scheme True Positive Results 99

Table 8.4: Detection Scheme False Positive Results 106

Table 8.5: IEEE 14-Bus Converging State Variable Physical Representation.....110

Table 11.1: Detection Scheme Computational Time (s) 137

Table A.1: 5-Bus Transmission Line Impedances [2] 150

Table A.2: 5-Bus Input Snapshot 151

Table A.3: 5-Bus Output (**Bold**) Snapshot 151

Table B.1: 14-Bus Transmission Line Impedances.....157

Table B.2: 14-Bus Input Snapshot 157

Table B.3: 14-Bus Output (**Bold**) Snapshot 158

Table D.1: 5-Bus Without Line Flows SI Classification Results.....175

Table D.2: 5-Bus Without Line Flows SII Classification Results 176

Table D.3: 5-Bus Without Line Flows MI Classification Results 177

Table D.4: 5-Bus Without Line Flows MII Classification Results.....178

Table D.5: 5-Bus With Line Flows SI Classification Results.....179

Table D.6: 5-Bus With Line Flows SII Classification Results 180

Table D.7: 5-Bus With Line Flows MI Classification Results.....181

Table D.8: 5-Bus With Line Flows MII Classification Results 182

Table D.9: IEEE 14-Bus Without Line Flows SI Classification Results 183

Table D.10: IEEE 14-Bus Without Line Flows SII Classification Results.....184

Table D.11: IEEE 14-Bus Without Line Flows MI Classification Results.....185

Table D.12: IEEE 14-Bus Without Line Flows MII Classification Results 186

Table D.13: IEEE 14-Bus With Line Flows SI Classification Results 187

Table D.14: IEEE 14-Bus With Line Flows SII Classification Results.....188

Table D.15: IEEE 14-Bus With Line Flows MI Classification Results.....189

Table D.16: IEEE 14-Bus With Line Flows MII Classification Results.....190

Table E.1: 5-Bus Without Line Flows SI Localization Results 192

Table E.2: 5-Bus Without Line Flows SII Localization Results.....194

Table E.3: 5-Bus Without Line Flows MI Localization Results.....195

Table E.4: 5-Bus Without Line Flows MII Localization Results.....197

Table E.5: 5-Bus With Line Flows SI Localization Results.....198

Table E.6: 5-Bus With Line Flows SII Localization Results 200

Table E.7: 5-Bus With Line Flows MI Localization Results 201

Table E.8: 5-Bus With Line Flows MII Localization Results.....203

Table E.9: IEEE 14-Bus Without Line Flows SI Localization Results.....204

Table E.10: IEEE 14-Bus Without Line Flows SII Localization Results 206

Table E.11: IEEE 14-Bus Without Line Flows MI Localization Results 207

Table E.12: IEEE 14-Bus Without Line Flows MII Localization Results.....209

Table E.13: IEEE 14-Bus With Line Flows SI Localization Results.....210

Table E.14: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x1-x68.....212

Table E.15: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x69-x136 213

Table E.16: IEEE 14-Bus With Line Flows MI Localization Results.....214

Table E.17: IEEE 14-Bus Without Line Flows MII Localization Results for State Variables x1-x68 216

Table E.18: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x69-x136 217

LIST OF FIGURES

Figure 1.1: Basic Power System Application Feedback Model 2

Figure 2.1: General Knowledge Discovery Process 21

Figure 2.2: Classification Matrix 24

Figure 3.1: IT Based Detection Experimental Network Topology 30

Figure 3.2: Engineer's Control Packet Timestamps 32

Figure 3.3: Attacker's Control Packet Timestamps 32

Figure 4.1: Detection Via State Variables Approach 37

Figure 4.2: Approach Flow Chart 40

Figure 4.3: Building Classification Dataset 42

Figure 5.1: Power System Notation 58

Figure 6.1: 5-Bus Convergence Map for Controlled Voltage Parameters 67

Figure 6.2: 14-Bus Convergence Map for Controlled Voltages Bus 1 and 2 69

Figure 6.3: PCA Scree Plot for 5-Bus System With Lines 73

Figure 6.4: Percent Variances Accounted for by the First 10 Components of Each Transformation 74

Figure 6.5: Scores and Feature Vectors Transformed 5-Bus Without Line Flows. 75

Figure 6.6: Hotelling T^2 of 500 5-Bus Instances Without Line Flows 77

Figure 6.7: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows 77

Figure 6.8: 5-Bus Average Voltages for Grubbs Test 'n' Selection 80

Figure 6.9: IEEE 14-Bus Average Voltages for Grubbs Test 'n' Selection 81

Figure 7.1: 5-Bus Convergence Discriminant Classifier Comparison 87

Figure 7.2: 5-Bus Convergence Discriminant Classifier Misclassification Rate..... 87

Figure 7.3: IEEE 14-Bus Convergence Discriminant Classifier Comparison 88

Figure 7.4: IEEE 14-Bus Convergence Discriminant Classifier Misclassification Rate 89

Figure 8.1: Cyber-Event Identification Approach 93

Figure 8.2: 5-Bus Without Line Flows SI Classification Results..... 95

Figure 8.3: False Positive Classification 96

Figure 8.4: 5-Bus Overall True Positive Results for Each Attack Type..... 98

Figure 8.5: 5-Bus Overall True Positive Convergence Classifier Results 101

Figure 8.6: 5-Bus Overall True Positive Instance Classifier Results.....102

Figure 8.7: 5-Bus Overall True Positive Instance Classifier Results, Without Injected Powers 103

Figure 8.8: 5-Bus Overall True Positive Instance Classifier Results, With Injected Powers 104

Figure 8.9: 5-Bus Overall False Negative Instance Classifier Results.....105

Figure 8.10: IEEE 14-Bus Overall True Positive Results for Each Attack Type 107

Figure 8.11: IEEE 14-Bus Overall True Positive Convergence Classifier Results ...109

Figure 8.12: 14-Bus Overall True Positive Instance Classifier Results.....111

Figure 8.13: IEEE 14-Bus Overall True Positive Instance Classifier Results, Without Injected Powers 112

Figure 8.14: IEEE 14-Bus Overall True Positive Instance Classifier Results, With Injected Powers 113

Figure 8.15: IEE 14-Bus Overall False Negative Instance Classifier Results.....114

Figure 9.1: 5-Bus Without Line Flows SII Localization Results 117

Figure 9.2: Overall False Positive Localization Results 118

Figure 9.3: Overall True Positive Localization Results 119

Figure 9.4: 5-Bus True Positive Localization Results, Without Injected Powers .. 121

Figure 9.5: 5-Bus True Positive Localization Results, With Injected Powers 122

Figure 9.6: IEEE 14-Bus True Positive Localization, Without Injected Powers ... 124

Figure 9.7: IEEE 14-Bus True Positive Localization, With Injected Powers 125

Figure 10.1: 5-Bus False Negative, Without Injected Powers 128

Figure 10.2: 5-Bus False Negative, With Injected Powers 129

Figure 10.3: IEEE 14-Bus False Negative, Without Injected Powers 130

Figure 10.4: IEEE 14-Bus False Negative, With Injected Powers 131

Figure 12.1: Suggested Future Approach for High Confident Intrusion Detection .. 145

Figure A.1: 5-Bus One-line Diagram 150

Figure A.2: Boxplot 5-Bus Voltages, 500 Instances 152

Figure A.3: Boxplot 5-Bus Angles, 500 Instances 152

Figure A.4: Boxplot 5-Bus Real and Reactive Powers Generated, 500 Instances .. 153

Figure A.5: Boxplot 5-Bus Real and Reactive Powers Consumed, 500 Instances .. 153

Figure A.6: Boxplot 5-Bus Real Powers Injected, 500 Instances 154

Figure A.7: Boxplot 5-Bus Reactive Powers Injected, 500 Instances 154

Figure B.1: 14-Bus One-line Diagram 156

Figure B.7: 14-Bus Real Powers Injected, 500 Instances 158

Figure B.2: Boxplot 14-Bus Voltages, 500 Instances 159

Figure B.3: Boxplot 14-Bus Angles, 500 Instances 159

Figure B.4: Boxplot 14-Bus Real and Reactive Powers Generated, 500 Instances.160

Figure B.5: Boxplot 14-Bus Real Power Consumed, 500 Instances 160

Figure B.6: Boxplot 14-Bus Reactive Powers Consumed, 500 Instances.....161

Figure B.8: 14-Bus Real Powers Injected, 500 Instances 161

Figure B.9: 14-Bus Real Powers Injected, 500 Instances 162

Figure B.10: 14-Bus Real Powers Injected, 500 Instances 162

Figure B.11: 14-Bus Reactive Powers Injected, 500 Instances.....163

Figure B.12: 14-Bus Reactive Powers Injected, 500 Instances.....163

Figure B.13: 14-Bus Reactive Powers Injected, 500 Instances.....164

Figure B.14: 14-Bus Reactive Powers Injected, 500 Instances.....164

Figure C.1: PCA Scree Plot of 500 5-Bus Instances Without Line Flows 166

Figure C.2: 500 5-Bus Scores and Feature Vectors Transformed 166

Figure C.3: Hotelling T^2 of 500 5-Bus Instances Without Line Flows.....167

Figure C.4: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows 167

Figure C.5: PCA Scree Plot 168

Figure C.6: Scores and Feature Vectors Transformed 168

Figure C.7: Hotelling T^2 of 500 5-Bus Instances With Line Flows.....169

Figure C.8: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances With Line Flows.....169

Figure C.9: PCA Scree Plot of 500 14-Bus Instances Without Line Flows 170

Figure C.10: 500 14-Bus Scores and Feature Vectors Transformed 170

Figure C.11: Hotelling T^2 of 500 14-Bus Instances Without Line Flows.....171

Figure C.12: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows 171

Figure C.13: PCA Scree Plot of 500 14-Bus Instances With Line Flows 172

Figure C.14: 500 14-Bus Scores and Feature Vectors Transformed 172

Figure C.15: Hotelling T^2 of 500 14-Bus Instances With Line Flows 173

Figure C.16: Histogram and Rayleigh Curve Fit of T^2 values for 500 IEEE 14-Bus Instances With Line Flows 173

Figure D.1: 5-Bus Without Line Flows SI Classification Results 175

Figure D.2: 5-Bus Without Line Flows SII Classification Results 176

Figure D.3: 5-Bus Without Line Flows MI Classification Results 177

Figure D.4: 5-Bus Without Line Flows MII Classification Results 178

Figure D.5: 5-Bus With Line Flows SI Classification Results 179

Figure D.6: 5-Bus With Line Flows SII Classification Results 180

Figure D.7: 5-Bus With Line Flows MI Classification Results 181

Figure D.8: 5-Bus With Line Flows MII Classification Results 182

Figure D.9: IEEE 14-Bus Without Line Flows SI Classification Results 183

Figure D.10: IEEE 14-Bus Without Line Flows SII Classification Results 184

Figure D.11: IEEE 14-Bus Without Line Flows MI Classification Results 185

Figure D.12: IEEE 14-Bus Without Line Flows MII Classification Results 186

Figure D.13: IEEE 14-Bus With Line Flows SI Classification Results 187

Figure D.14: IEEE 14-Bus With Line Flows SII Classification Results 188

Figure D.15: IEEE 14-Bus With Line Flows MI Classification Results 189

Figure D.16: IEEE 14-Bus With Line Flows MII Classification Results 190

Figure E.1: 5-Bus Without Line Flows SI Localization Results 192

Figure E.2: 5-Bus Without Line Flows SII Localization Results 193

Figure E.3: 5-Bus Without Line Flows MI Localization Results 195

Figure E.4: 5-Bus Without Line Flows MII Localization Results.....196

Figure E.5: 5-Bus With Line Flows SI Localization Results.....198

Figure E.6: 5-Bus With Line Flows SII Localization Results 199

Figure E.7: 5-Bus With Line Flows MI Localization Results 201

Figure E.8: 5-Bus With Line Flows MII Localization Results.....202

Figure E.9: IEEE 14-Bus Without Line Flows SI Localization Results.....204

Figure E.10: IEEE 14-Bus Without Line Flows SII Localization Results 205

Figure E.11: IEEE 14-Bus Without Line Flows MI Localization Results 207

Figure E.12: IEEE 14-Bus Without Line Flows MII Localization Results.....208

Figure E.13: IEEE 14-Bus With Line Flows SI Localization Results.....210

Figure E.14: IEEE 14-Bus With Line Flows SII Localization Results.....211

Figure E.15: IEEE 14-Bus With Line Flows MI Localization Results.....214

Figure E.16: IEEE 14-Bus With Line Flows MII Localization Results 215

ACKNOWLEDGMENTS

Though my name is on the cover of this dissertation, I cannot take full credit for the completion of the work enclosed. This work has been supported and aided by many individuals and all of which will forever have my respect and gratitude. First and foremost I would like to acknowledge the love and caring support offered by my beautiful fiancée, Karri Jenkins. Her endless and selfless support throughout this endeavor made this possible.

Also, I would like to thank my advisor Dr. Travis Atkison for his immeasurable support and guidance over the years. His experiences and guidance offered valuable insight into the many aspects of my graduate studies. In addition, I would like to acknowledge the committee members: Dr. Galen Turner, Dr. Jean Gourd, Dr. Mickey Cox, and Dr. Rastko Selmic. Each exhibited flexibility and offered their unique perspectives towards this effort.

Last, but certainly not least, the support and guidance offered by the teachings of my Lord and Savior Jesus Christ along with the Saints allowed for a clear and dedicated mind even in the late hours.

"All wisdom comes from the Lord, and wisdom is with him for eternity."

— Sirach 1:1

CHAPTER 1

INTRODUCTION

Industrial control systems (ICS) are present across many industries ranging from transportation to utilities [3]. An ICS is comprised of multiple controllers, each functioning as logic engines using conditional processing. One of the most prevalent ICSs is the critical infrastructure power grid. This meshed network of geographically distributed control systems (DCS) has recently seen an influx of solid-state devices with Internet/intranet networking capabilities. Benefits of this influx include the command and control ability granted to the governing ICS. This governing ICS contains the supervisory control and data acquisition (SCADA) system. However, with this influx of smart network capable devices, the potential for various cyber threats arises [4] and therefore sophisticated cyber detection and localization methods must be developed and analyzed.

A basic model, derived from similar ones presented in [5, 6], of a power system application with state feedback is presented in Figure 1.1. The feedback model shown is governed by the energy management system (EMS) which, during an event, will instruct the SCADA system to send control commands to the power system application [7]. An event can consist of a fault, i.e. a downed power line, or a disturbance as modest as a customer turning on a lamp. Events change the operating conditions of

the application and if drastic enough will cause the EMS to take immediate action to protect the system from catastrophic failure. In instances where the event does not cause immediate harm to the power system, the EMS will remain idle or change control parameters to provide power to customers more economically. The purpose of this feedback interface is for the constant monitoring and control of the power system application in an effort to ensure the efficient delivery of power to the grid customers.

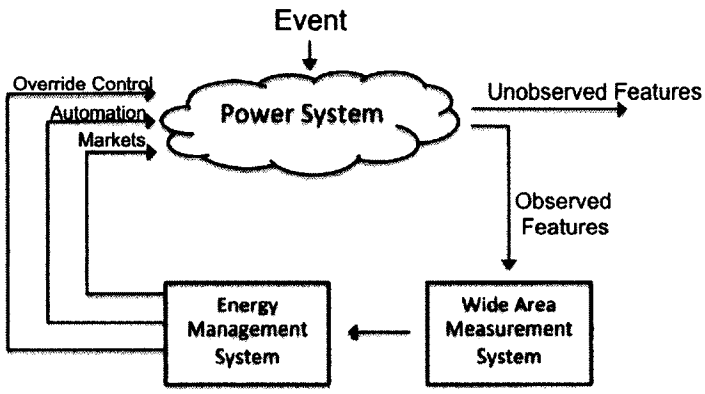

Figure 1.1: Basic Power System Application Feedback Model

The remote execution and control vulnerabilities inherent to ICS arises from the utilization of information technology (IT) systems. Such technology includes the communication and device infrastructure that is used in the current grid and the proposed schemes that are to be used in the future smart grid. Thus, the vulnerabilities found in the supporting IT infrastructure can be exploited to compromise an ICS [8]. Because an ICS requires 100% availability and equal reliability, implementing traditional IT security may provide an additional dimension of attack vectors that an attacker can use to breach an ICS. Using IT based security alone enables an attacker, through the use of zero-day attacks or non-patched systems attacks, the ability to

effectively infiltrate the control system's local area network (LAN), granting control from either inside or outside the network. A system that can recognize these intrusions and isolate them based on control level data and not just IT level data will effectively prevent most attacks from occurring or at the very least minimize damage caused by the intrusion.

To solve this problem, this work examines control system security, specifically power grid security, using a context specific approach. The work demonstrated here takes an inter-disciplinary approach using techniques from the machine learning community and applies them to the power flow dynamics of multiple power systems in an effort to detect and localize cyber intrusions. Based on the state variables of the power system, features are identified using techniques first introduced in the data mining community. These features then serve in the development of models used in the detection and localization of the system breaches.

1.1 Motivation

Enhancing the security posture of the critical infrastructure power grid is one of the biggest challenges in cyberspace. One of the goals of the Obama administration's *A Policy Framework for the 21st Century Grid* is a power infrastructure with improved grid security and resilience [9]. This resilience describes a need for a self-healing network that can prevent, detect, mitigate, and effectively avoid most cyber threats found in a control system environment. The integration of today's petabytes [10] and tomorrow's exobytes of state parameters and the ability to process it diligently using

revolutionary cyber incident detection models will make this goal among others a reality.

Originally, the control system local area network (LAN) was not connected to any Internet/Intranet connected devices. This created the so-called air-gap, physically securing the devices from other Internet connected devices. However, for an increase in efficiency and remote monitoring capabilities, the control system had to be integrated into corporate LANs. The recommended network architecture for a control system LAN is provided in [11]. This recommended controls system protection scheme combines the practices of IT security to the control system with the goal of an end-all secure environment. Furthermore, in a recent report [12], a total of 7,200 control devices have been found to be directly connected to the World Wide Web. This project known as SHINE was stared in Spring of 2012 and sought to raise awareness for controls system security with the initial finding reaching 500,000 Internet connected devices. In a recent report [13], it is stated that the energy sector is the fifth-most-targeted sector worldwide and is hit with nine highly sophisticated attacks per day. These and other statistics, shown in Table 1.1, reveal the immediate action needed to secure the control infrastructure that governs power systems.

Table 1.1: Cybersecurity Statistics Concerning Power Systems

Description	Source	Cite
Public Utility Compromised	ICS-CERT	[14]
Observed Energy Sector Attacks	Cisco	[15]
500,000 ICS Devices Openly Connected to WWW	ICS-CERT	[12]
9 sophisticated attacks per day	Symantec	[13]
Reported ICS attacks up 52% in 2012	Dept. Homeland Security	[16]
Cyber attack becoming primary threat against U.S.	FBI	[17]

1.1.1 Vulnerabilities

A vulnerability in terms of industrial control system is any weakness that can be exploited in such a way that will compromise the intended operation of the control system. In an article published by the Idaho National Laboratory [18], the common vulnerabilities of industrial control systems are outlined. Vulnerabilities include lack of input validation, weak communication protocols and authentication, and failure to the patch system's software.

Threats against the critical infrastructure power grid are inevitable and continue to happen every day. Some threats are the result of accidental circumstances while others are the direct result of aggressors. In the context of cyber, these aggressors include hackers, who may attack for various reasons including: intellectual challenge, curiosity, monetary gain, power, vengeance, or terrorism. In addition, breaches into critical infrastructures may be the result of a nation-state sponsored effort.

1.1.2 Data the Grid Offers

The source of the petabytes of data is a result of two new intelligent electronic devices (IEDs): the phasor measurement unit (PMU) and the smart meter. The smart meter is the base element of the advanced metering infrastructure (AMI). This is in part a result of the establishment of the Smart Grid Investment Grant (SGIG) program by the Energy Independence and Security Act of 2007 [19], Section 1306, and amended under the American Recovery and Reinvestment Act of 2009 [20]. In July of 2012, the Department of Energy (DOE) published a progress report of the SGIG program stating that PMUs offer the essential wide-area visibility needed in

the power grid due to its sampling rate of 30 to 120 times per second. The report then goes on to state that there are currently over 950 networked PMUs installed in North America funded by the SGIG program. The SGIG AMI projects support the installation of smart meters capable of transmitting data at 15-, 30-, or 60-minute intervals for customer billing information, interval load data, system voltage levels, and power quality. There are currently a total of 65 SGIG AMI projects, with an end goal of installing a total of 15.5 million smart meters [21]. As of April 30th 2014, the total number of AMI meter installations reported to the *SmartGrid Integrated Project Reporting Information System* (SIPRIS) [22] was found to be 16.2 million, well past the end goal [23].

An industry projection suggests that by 2015, there will be a total of 65 million smart meters installed nationwide. The RF meshed AMI network is operated predominately on the unlicensed Industrial, Scientific, and Medical (ISM) band between 902-928 MHz and is defined in Part 15 of the FCC regulations. A proprietary protocol that is optimized for AMI meshed network communication is described in [24]. When in initiation mode, each packet is 32 bytes in length with a header of 15 bytes that is capable of containing the packet's route. Metering nodes are capable of caching the previously established packet routes for future communication. The security of packet transmission can be based on key pairs [25]. However, this protocol and others have been found to have vulnerabilities as demonstrated by Brinkhaus *et al.* [26].

At the distribution level, the electrical loads are determined by the power consumption of the customers. This example of interdependence, among others, allows for a unique opportunity for the development of an analytical framework that in

the event of a cyber incident will detect a certain number of inconsistencies in the reported power system state variables. Table 1.2 shows an example of power level data based on the estimated average smart grid enabled utility readings per day. The data is categorized into three classes: 1) raw data 2) pre-processed data and 3) database or historical data. The raw data is aggregated by the SCADA system without any preprocessing done by the smart device controllers and is stored in databases in a Historian server. Database and historical data can be analyzed for its trending information and will contain information that can be used to detect high-level periodic malware similar to the Stuxnet worm. Stuxnet, a malicious program that autonomously targeted the control systems of an Iranian nuclear facility is believed to be installed on more than 60,000 computers [27]. The code of this revolutionary cyber-weapon is freely available online.

Table 1.2: Example of power data based on estimated average smart grid enabled utility readings per day.

Data	From	Class	Data Amt	Analysis
Circuit Breaker Position	Substation	2	10kb	Real Time
Over Current Alert	Substation and Line IED	2	10kb	Real Time
Protective Relay Status	Substation	2	10kb	Real Time
Device Voltage Meters	Substation and Line IED	1	100kb	Real Time
Device Current Meters	Substation and Line IED	1	100kb	Real Time
Feeder Switch	Substation	2	10kb	Real Time
Telemertered Readings	Substation	2	10kb	Real Time
Transformer Meters	Substation	1	100kb	Real Time
Line Voltage Meters	Power Line IEDs	1	100kb	Real Time
Line Current Meters	Power Line IEDs	1	100kb	Real Time
Power Flow	EMS	2	100Mb	Real Time
Fault Location Reporting	EMS	2	100kb	Offline
Historian	EMS	3	10Tb	Offline
Smart Meter Readings	AMI	2	1Tb	Real Time
Appliance Reporting	HAN Zigbee Devices	2	100Mb	Real Time
Micro Generation	Photovoltaic, Wind, etc	2	100kb	Real Time

1.1.3 Why a Context Specific Approach

The end goal of any ICS attack is to obtain control over the critical application. Therefore, the end objective of the attack is to change some parameter of the system being controlled. The approach developed by this dissertation takes advantage of this fact and uses the system parameters to detect the presence of a cyber intrusion. More classical detection schemes may not be able to detect an intrusion due to the level of sophistication of the intrusion. These classical detection schemes are based on detecting intrusions locally by monitoring firewall logs, network traffic, and system logs among others. Though a valuable source of information, these sources do not provide a full picture of the system that is trying to be secured.

For example, in Brinkhaus *et al.* [26] the goal of the attack demonstrated was to change the power consumed by the customer so they would not have to pay as much on their power bill. To perform this attack successfully, the aggressor has to spoof the information being reported from a meter to the collector. An IT intrusion detection system (IDS) may or may not be able to detect this type of intrusion. The ability to detect depends on the level of sophistication of the attack. For instance, if the spoofed packet has all the information correctly spoofed, the IT IDS would not be able to recognize the intrusion. This is because IT IDSs are signature based detection systems and any deviation from those signatures will trigger an alarm. Whereas in a distributed network such as the critical infrastructure power grid system, the parameters reported in one location are based off of what is happening at a different part of the system. Examples of this dependency includes the fact that the power being consumed by a customer depends on the power being supplied to the customer.

1.2 Statement of Hypothesis

Given the number of reporting intelligent electronic devices (IEDs) being added to the critical infrastructure power grid, a framework can be formulated that utilizes the historical system state variables for the detection and localization of malicious cyber activity based on prediction models that fully express key system features. Formulation of this framework is based on a detection scheme founded in knowledge discovery techniques including: discriminant analysis and principal component analysis.

1.3 Contributions

As this work is an inter-disciplinary approach to solving the problem of securing the critical infrastructure power grid, it provides not only to the area of power systems, but also to the areas of cybersecurity, data knowledge discovery, and other related fields. This work successfully demonstrates the usage of machine learning algorithms for both feature selection and classification applied in a context specific environment for the detection and localization of cyber intrusions. Specific contributions to the areas of power systems, knowledge discovery, and the study of cyberspace include the following:

- Extraction and demonstrated utilization of key power system features based on system state parameters via dimensional transformation and statistical measures.
- Development of a cyber-event detection framework based on power system state parameters through the training and utilization of classification techniques including discriminant analysis and principal component analysis.

- Provides a scalability analysis via the comparison of the detection scheme when applied to two different power systems.
- A method for determining stealthy attacks and includes an examination into what state parameters are susceptible to these attacks and for what values.
- Lastly, a detailed description of how the contributions described above can be expanded upon for the creation of a high confident detection scheme that merges the two cyber and physical perspectives for the detection of cyber incidents in critical infrastructure power grid in a manner that is both self verifying and complementary.

1.4 Organization

Building off the context creation and statement of the problem provided by Chapter 1, Chapter 2 provides the necessary background information for the developed detection scheme including a discussion on power flow analysis and a description of the knowledge discovery approach. Also, provided in Chapter 2 is a discussion on how the developed cyber-event detection scheme will be evaluated. Through a discussion of related works, Chapter 3 provides an initial starting point for the scheme along with outlining drawbacks of other approaches to the problem. This chapter also describes an experiment that was conducted at the early stages of the dissertation which addresses some of the key issues with an IT based intrusion detection system.

The details of the approach taken by this dissertation to detect cyber-event based on a physical perspective is described in Chapter 4. In addition to these details, this chapter also discusses how the scheme could be implemented in a live SCADA

environment. Chapter 5 describes the many simulation models used to develop and test the detection scheme. This includes which power system topologies are being used for the analysis along with a discussion of Monte-Carlo power flow simulations. Also provided in Chapter 5 is a detailed formalization of the four attack models used throughout the dissertation. Chapter 6 discusses the key features extracted for the purpose of identification. The next chapter, Chapter 7, determines the exact parameters required for the classifiers to perform optimally and are based on a training size and statistical constants of the trusted models. Classification results of the identification and localization classifiers are presented in Chapters 8 and 9.

Chapter 8 outlines the identification of the presence of cyber-events in a power system instance while Chapter 9 discusses the localization or determination of the source of the cyber-event. Based of these results, an analysis on stealthy attacks was performed and results of this analysis is presented in Chapter 10. Chapter 11, outlines the recommendations and conclusions of the developed detection approach. The future work, outlined in Chapter 12, proposes some further modifications that may increase the true positive classification rate of the developed detection scheme. Also, provided in this chapter are several additional aspects of the detection scheme that could be considered including the possibility of combining the developed physical detection scheme with more traditional IT based detection schemes.

CHAPTER 2

BACKGROUND

2.1 Overview of Power Systems

The critical infrastructure power grid is divided up into three main levels: distribution, transmission, and generation. Distribution consists of the customer domain and contains the actual delivery of electrical power via feeder circuits while stepping down the voltage from the transmission level. Transmission is the bulk transport of electrical power from the generating facilities to the distribution level via multiple high voltage substations. Lastly, generation focuses on the creation of electricity based on the demand as defined by the load at the distribution level.

The primary steady state algorithms that determine the stability and reliability of the critical infrastructure power grid are: 1) power flow, 2) optimal power flow, and 3) state estimation. The power system challenge is to try to solve the nonlinear power balance equations in near real time given a percent of system values. The system state uses Kirchhoff's Law at each power system bus throughout the system in question. Kirchhoff's Law states that the sum of the powers entering a bus must be zero. The active and reactive components of the power flow equations in polar representation

form from bus i to bus j can be determined by solving Eqs. (2.1) and (2.2).

$$0 = \Delta P_i = P_i^{injec} - V_i \sum_{i=1}^{n} V_j Y_{ij} cos(\theta_i - \theta_j - \varphi_{ij}) \tag{2.1}$$

$$0 = \Delta Q_i = Q_i^{injec} - V_i \sum_{i=1}^{n} V_j Y_{ij} sin(\theta_i - \theta_j - \varphi_{ij}) \tag{2.2}$$

where P_i^{injec} and Q_i^{injec} are the injected powers into each bus, V_i is the voltage on bus i and Y_{ij} is element ij of the admittance matrix. Optimal power flow is the result of finding the desired power system state variables based on one or multiple cost functions. Examples of cost functions include minimization on power losses and fuel costs of generation. State estimation described the process of estimating the state of the power system based on an incomplete picture of the system being observed. With state estimation, system parameters are measured using intelligent electronic devices (IEDs) and are reported back to the SCADA system.

2.1.1 Power Flow

The goal of the Newton-Raphson method when applied to power system analysis is to provide an iterative method for solving the nonlinear algebraic power flow equations, Eqs. (2.1) and (2.2) [1]. This method is known as being the most common approach for solving the power flow equations [28]. The Newton-Raphson method when applied to solve the power flow problem can be summed up into the following five steps. Steps two through five are repeated until convergence or until some iteration limit has been reached.

1. Initialize variables using a flat start.

2. Use Eqs. (2.1) and (2.2) to solve

$$\Delta \mathbf{y}_i(\mathbf{x}) = \begin{bmatrix} \Delta \mathbf{P}_i \\ \Delta \mathbf{Q}_i \end{bmatrix} = \begin{bmatrix} \mathbf{P}_i^{injec} - \Delta \mathbf{P}_i \\ \mathbf{Q}_i^{injec} - \Delta \mathbf{Q}_i \end{bmatrix} \tag{2.3}$$

3. Calculate the full Jacobian $\mathbf{J}$ as defined by Eq. (2.6).

4. Use LU factorization to solve for the bus voltages and angles.

$$\mathbf{J} \begin{bmatrix} \Delta \theta_i \\ \Delta V_i \end{bmatrix} = \begin{bmatrix} \Delta \mathbf{P}_i \\ \Delta \mathbf{Q}_i \end{bmatrix} \tag{2.4}$$

5. Compute the next iteration of angles and voltages using

$$\mathbf{x}_{i+1} = \begin{bmatrix} \theta_{i+1} \\ \mathbf{V}_{i+1} \end{bmatrix} = \begin{bmatrix} \theta_i \\ V_i \end{bmatrix} + \begin{bmatrix} \Delta \theta_i \\ \Delta \mathbf{V}_i \end{bmatrix} \tag{2.5}$$

6. Calculate error or deltas of the active and reactive powers. Error ε is the highest absolute value.

$$\mathbf{J} = \left[\begin{array}{c|c} \mathbf{J1} & \mathbf{J2} \\ \hline \mathbf{J3} & \mathbf{J4} \end{array}\right] = \begin{bmatrix} \frac{\partial P_2}{\partial \delta_2} & \cdots & \frac{\partial P_2}{\partial \delta_N} & \frac{\partial P_2}{\partial V_2} & \cdots & \frac{\partial P_2}{\partial V_N} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial P_N}{\partial \theta_2} & \cdots & \frac{\partial P_N}{\partial \delta_N} & \frac{\partial P_N}{\partial V_2} & \cdots & \frac{\partial P_N}{\partial V_N} \\ \frac{\partial Q_2}{\partial \delta_2} & \cdots & \frac{\partial Q_2}{\partial \delta_N} & \frac{\partial Q_2}{\partial V_2} & \cdots & \frac{\partial Q_2}{\partial V_N} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial Q_N}{\partial \delta_2} & \cdots & \frac{\partial Q_N}{\partial \delta_N} & \frac{\partial Q_N}{\partial V_2} & \cdots & \frac{\partial Q_N}{\partial V_N} \end{bmatrix} \tag{2.6}$$

Calculations for the elements of the Jacobian matrix $\mathbf{J}$, Eq. (2.6), are outlined in Table 2.1. The use of this method to calculate the Jacobian matrix is thoroughly outlined in [1]. For the voltage controlled buses, the voltage magnitudes V_k are already known and allowing for the omission of the associated functions in the derivation

of the Jacobian matrix [1]. This is utilized and noted in the simulation code and decreases the computational complexity of the simulation.

Table 2.1: Calculations for the elements of the Jacobian matrix [1].

$n \neq k$	
	$\mathbf{J1_{kn}} = \frac{\partial P_k}{\partial \delta_n} = \mathrm{V}_k \mathrm{Y}_{kn} \mathrm{V}_n sin(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J2_{kn}} = \frac{\partial P_k}{\partial V_n} = \mathrm{V}_k \mathrm{Y}_{kn} cos(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J3_{kn}} = \frac{\partial Q_k}{\partial \delta_n} = -\mathrm{V}_k \mathrm{Y}_{kn} \mathrm{V}_n cos(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J4_{kn}} = \frac{\partial Q_k}{\partial V_n} = \mathrm{V}_k \mathrm{Y}_{kn} sin(\delta_k - \delta_n - \theta_{kn})$
$n = k$	
	$\mathbf{J1_{kk}} = \frac{\partial P_k}{\partial \delta_k} = -\mathrm{V}_k \sum_{n=1, n\neq k}^{N} \mathrm{Y}_{kn} \mathrm{V}_n sin(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J2_{kk}} = \frac{\partial P_k}{\partial V_k} = \mathrm{V}_k \mathrm{Y}_{kk} cos(\theta_{kk}) + \sum_{n=1}^{N} \mathrm{Y}_{kn} \mathrm{V}_n cos(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J3_{kk}} = \frac{\partial Q_k}{\partial \delta_k} = \mathrm{V}_k \sum_{n=1, n\neq k}^{N} \mathrm{Y}_{kn} \mathrm{V}_n cos(\delta_k - \delta_n - \theta_{kn})$
	$\mathbf{J4_{kk}} = \frac{\partial Q_k}{\partial V_k} = -\mathrm{V}_k \mathrm{Y}_{kk} sin(\theta_{kk}) + \sum_{n=1}^{N} \mathrm{Y}_{kn} \mathrm{V}_n sin(\delta_k - \delta_n - \theta_{kn})$

Step six produces a vector of errors ε. The goal of the iterative method is to decrease the error to a certain point that is declared acceptable. Unless otherwise noted, the error stopping point utilized for simulating the power flow via the Newton-Raphson method is $\varepsilon_s = 0.01$. This means that the absolute values of both the active and reactive power mismatches all have to be below 0.01 to be considered a converging instance. Also, for this examination convergence had to occur within 15 iterations or the instance was declared a non-converging instance. On average, the 5-bus system converged within 4 iterations. The extreme of 15 iterations was selected as a stopping point given that if the system did not converge within 15 iterations it is likely for that given set of inputs the system can not exists. The fact of non-convergence corresponds to the likelihood that the power system being observed does not exist at that given set of inputs. A flat start means that, for simulation purposes, all non-voltage controlled busses are assumed to have a voltage of 1 per unit while all angles are assumed to

be zero. For a more detailed description of the iterative solutions to the power flow problem, the reader is encouraged to view the following referenced text [28, 1, 2].

2.1.2 State Estimation

State estimation is one of the primary steady state algorithms that help to determine the stability and reliability of a power system [28]. The process of estimating the state of the system plays a pivotal role in the development of the detection approach presented in this dissertation. In most installations of a power system, not all state parameters can be measured. This could be the cause of any number of reasons ranging from cost of instrumentation installation to device failure. Therefore, there is a need to be able to derive or estimate those state parameters via other observable parameters. It is noted that a good state estimation algorithm will be able to smooth out small errors in measurements, detect and identify large measurement errors, and compensate for missing data [28].

One main underlying assumption of the state estimation process is that the measurement error of variables being observed follow a normal (or Gausian) probability density function of zero mean described by

$$f(v) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{v^2}{2\sigma^2}}. \tag{2.7}$$

This assumption is generally accepted in the formulation of the power system state estimation problem [6]. Since it is possible that the observed state parameters are not exact, what is actually being observed or measured can be represented in vector form [29, 6, 30], as $\mathbf{z} = (z_1, z_2, \ldots, z_m)^T$ in

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{v}. \tag{2.8}$$

For Eq. (2.8), $\mathbf{v} = (v_1, v_2, \ldots, v_m)^T$ is the measurement error that contains the uncertainty in the measurement and $\mathbf{h}(\mathbf{x}) = (h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_m(\mathbf{x}))^T$ is the vector of the nonlinear functions relating each measurement to the state variables $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$. With the formalization of Eq. (2.8), it can be said that the goal of the state estimation problem is to find an estimate $\hat{\mathbf{x}}$ for $\mathbf{x}$ that is a best fit for the measurements $\mathbf{z}$. The error $\mathbf{e}$ is simply the difference between the true values measured and the estimated measured values. The search for such a $\hat{\mathbf{x}}$ that minimizes

$$min f = \sum_{i=1}^{m} \frac{1}{\sigma^2}[z_i - h_i(x)]^2 \tag{2.9}$$

can be determined using an iterative process such as the Newton-Raphson method. With each iteration represented as

$$\hat{\mathbf{x}}^{k+1} = \hat{\mathbf{x}}^k + (H(x^k)^T R^{-1} H(x^k))^{-1} H(x^k)^T R^{-1}(z - h(x^k)), \tag{2.10}$$

the result can be calculated using a Taylor series expansion on the functions $\mathbf{h}(\mathbf{x})$ around a point $\mathbf{x}^k$ [6]. In Eq. (2.10), $H(x) = \frac{\partial h}{\partial x}$ denotes a Jacobian matrix formed via the partials of the $h(x)$.

2.2 Multivariate Analysis

With today's computational capabilities, analytical techniques for multivariate analysis can be implemented with much less cost. Multivariate analysis (MA) describes the aggregate of techniques and algorithms used to analyze observations which contain multiple features. Such techniques are useful in that they help to untangle the redundant information to reveal the interesting and normally hidden information. This section provides the necessary background information regarding techniques

in multivariate analysis necessary for the development of the detection framework presented in this dissertation. Notation developed in this section will be consistently used throughout the dissertation when possible.

Letting $\vec{\mathbf{X}}$ be a vector consisting of m variables and representing a single observation, the ith observation can be fully denoted in vector format as

$$\vec{\mathbf{X}}_i = \begin{bmatrix} \mathbf{x}_{i,1} & \mathbf{x}_{i,2} & \cdots & \mathbf{x}_{i,j} & \cdots & \mathbf{x}_{i,m-1} & \mathbf{x}_{i,m} \end{bmatrix}. \tag{2.11}$$

A sample mean vector $\bar{\mathbf{x}}$ for the jth variable or feature consisting of n observations is determined by

$$\bar{\mathbf{x}}_j = \frac{1}{n}\sum_{i=1}^{n} \mathbf{x}_{i,j}. \tag{2.12}$$

Thus, it can be stated that $\bar{\mathbf{x}}_1$ is the mean vector of the first feature and $\bar{\mathbf{x}}_m$ is the mean vector of the last feature. By using this notation a data matrix $\mathbf{X}$ that encapsulates all n observations of m different features can be defined as

$$\mathbf{X} = \begin{bmatrix} \vec{\mathbf{X}}_1 \\ \vdots \\ \vec{\mathbf{X}}_i \\ \vdots \\ \vec{\mathbf{X}}_n \end{bmatrix} = \begin{bmatrix} \mathbf{x}_{1,1} & \cdots & \mathbf{x}_{1,j} & \cdots & \mathbf{x}_{1,m} \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ \mathbf{x}_{i,1} & \cdots & \mathbf{x}_{i,j} & \cdots & \mathbf{x}_{i,m} \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ \mathbf{x}_{n,1} & \cdots & \mathbf{x}_{n,j} & \cdots & \mathbf{x}_{n,m} \end{bmatrix}. \tag{2.13}$$

The population mean of the data matrix Eq. (2.13) can be calculated as

$$\boldsymbol{\mu} = \mathbf{E}[\mathbf{X}] = \begin{bmatrix} \bar{\mathbf{x}}_1 & \ldots & \bar{\mathbf{x}}_j & \ldots & \bar{\mathbf{x}}_m \end{bmatrix}^{\mathrm{T}}, \tag{2.14}$$

and is an extension of the sample mean vector Eq. (2.11). It is also often desired to know how the variables vary within themselves and vary with respect to other variables. A square dispersion matrix represents just this in the form of variances (the diagonal terms) and covariances (the off diagonal terms). This dispersion matrix or sample covariance matrix $\mathbf{S}$ can be expressed in terms of the population mean as shown in

$$\mathbf{S} = \frac{1}{n-1}\sum_{i=1}^{n}(\vec{\mathbf{X}}_i^{\mathrm{T}} - \boldsymbol{\mu})(\vec{\mathbf{X}}_i^{\mathrm{T}} - \boldsymbol{\mu})^{\mathrm{T}}. \tag{2.15}$$

In cases of a zero-mean data matrix, Eq. (2.15) reduces to

$$\mathbf{S} = \frac{1}{n-1}\mathbf{X}^{\mathrm{T}}\mathbf{X}. \tag{2.16}$$

The closer the off-diagonal terms of $\mathbf{S}$ are to zero the closer the features represented by the indices of $\mathbf{S}$ are to being completely uncorrelated. Conversely, the higher these off-diagonal terms are the more correlated the two features are. Also, the higher the off diagonal terms are the higher the redundancy is in the data matrix $\mathbf{X}$. Using the terms, $s_{i,j}$, of the covariance matrix $\mathbf{S}$, a correlation matrix $\mathbf{R}$ can be created that describes the dependency between features in

$$\mathbf{R} = \begin{bmatrix} 1 & r_{1,2} & \dots & r_{1,m-1} & r_{1,m} \\ r_{2,1} & 1 & \dots & r_{2,m-1} & r_{2,m} \\ \vdots & \dots & \ddots & \dots & \vdots \\ r_{m-1,1} & r_{m-1,2} & \dots & 1 & r_{m-1,m} \\ r_{m,1} & r_{m,2} & \dots & r_{m,m-1} & 1 \end{bmatrix}, \tag{2.17}$$

where

$$r_{i,j} = \frac{s_{i,j}}{\sqrt{s_{i,i}s_{j,j}}}.$$

A more direct and less computationally expensive approach to calculating $\mathbf{R}$ is to create a diagonal matrix $\mathbf{D}$ comprised of only the diagonal terms of $\mathbf{S}$, $(s_{11}, s_{22}, \ldots, s_{mm})$, as shown in

$$\mathbf{R} = \mathbf{D}^{-1}\mathbf{S}\mathbf{D}^{-1} = \begin{bmatrix} \sqrt{s_{11}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{s_{mm}} \end{bmatrix}^{-1} \mathbf{S} \begin{bmatrix} \sqrt{s_{11}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{s_{mm}} \end{bmatrix}^{-1}. \tag{2.18}$$

2.3 Knowledge Discovery

Many advancements have been made in recent years in the areas of data mining (DM) and knowledge discovery in databases (KDD) [31, 32, 33, 34, 35, 36, 37]. Most of the advancements are in the area of algorithm development with only a few works presenting a detailed discussion on the usage of DM and KDD approaches to securing the cyberinfrastructure of the critical infrastructure power grid [38, 39, 40, 41]. This section provides the necessary background information regarding data mining and knowledge discovery necessary for the development of the detection framework presented in this dissertation.

The primary objective of DM and more generally KDD is to discover useful information from a large dataset. These processes describe the algorithms and overall implementation techniques utilized for the extraction of information. KDD describes the overall process starting with the collection and storage of raw data and ending with

details for representing the information concluded via the examination. A depiction of the knowledge discovery process (KDP) is shown in Figure 2.1 and is derived from multiple sources including [32, 37]. This process though generalized has five main steps and outlines the hierarchical structure for the detection framework developed in this dissertation. The details of each step are discussed below.

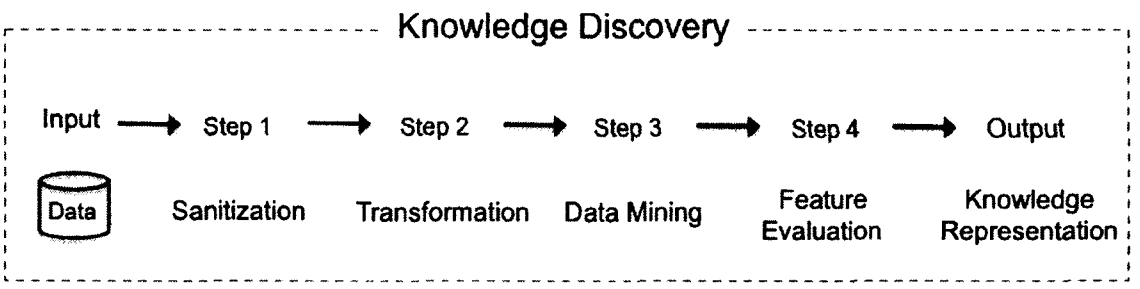

Figure 2.1: General Knowledge Discovery Process

1. **Sanitization:** Before information can be extracted, the data must undergo cleansing in order to remove noise and eliminate any inconsistent data. For simplicity, the selection of data is included in this step and involves the extraction of attributes of the original dataset to be analyzed. This could include the extraction of all attributes of the original dataset or a subset.
2. **Transformation:** Once cleansed the data needs to, in most cases, be transformed in some manner in order for the next step to be performed. An example of this is a dimensional transformation in which the information is presented in a new kernel or vector space. The type of technique used in the next step defines the type of transformation the data must undergo.

3. **Data Mining:** The data mining process uses various analysis tools and techniques for the extraction of patterns/knowledge. Some examples of tools and techniques include associative rule mining, clustering analysis along with prediction and classification methods.
4. **Feature Evaluation:** In most cases, not every pattern identified by the data mining approach can be considered relevant or interesting. This step identifies the patterns that are relevant to the analysis and validates those patterns based on multiple measures.
5. **Knowledge Representation:** The final stage of the KDD process details the clear and direct technique used to present the information to the user. This is generally done in the form of a graphical representation, i.e. an alarm.

Data mining is often described as the process of analyzing large amounts of data in some domain for the primary purpose of mining or extracting what would be normally hidden patterns or knowledge [37]. Extraction of patterns involves the discovery of implicit structures in the data or a detailed description of the data through a high level abstraction. Instead of just sifting the data, this dissertation seeks to present results in terms of a KD process (KDP) that can be implemented in an actual environment. A KDP model is then developed as the final framework model with a detailed description of model inputs and decisions produced by the output.

2.3.1 Learning Techniques

The two main types of learning techniques are unsupervised learning and supervised learning. Unsupervised learning involves the process that automatically

discovers formations in a dataset without the use of labels. Some examples of this type of learning include clustering and associative rule mining. Supervised learning predicts the existence of hidden patterns based on the information gained from a training set. Training sets consist of a set of observations containing a finite number of features and a classification label for each observation. The result of these methods place newly observed instances into labels based on the hidden patterns.

2.3.2 Detection via Classification

Detection via classification is the designation of observations or instances into classes based on a deterministic classification. Classes, in the case of this dissertation, can be in the form of a dichotomy placing instances into either class based on a minimization of a cost function. These classification approaches determine the likelihood that the instance or observation exists within each class and classifies according to the class that contains the highest likelihood value.

2.3.3 Validation

In order to examine the success of the developed detection scheme, several techniques for validation are utilized. To aid in and determine the success of the developed detection scheme, two main validation techniques were utilized: a) validation of machine learning algorithms, and b) validation of developed detection scheme. Each validation type encompasses a set of sub validation schemes and includes:

Validation of *Machine Learning Algorithms:*

a *Split, Cross Validation and Bootstrapping* are methods by which the training set and test set are rotated through the developed knowledge discovery algorithm for testing purposes. Though computationally more expensive,

Bootstrapping provides a means to quantify the error of the KDD model [37].

b *Confusion Matrix*, Figure 2.2, compares the successful classification into either class with the failed attempts to classify into either class [37].

		Prediction Class [P]		
		c_1	c_2	**total**
Actual Class[A]	c_1'	True Negative	False Positive	C_1'
	c_2'	False Negative	True Positive	C_2'
	total	C_1	C_2	

Figure 2.2: Classification Matrix

c *Receiver Operating Characteristics* (ROC) curves allow for the visual comparison of two or more classifiers and is a plot of True Positive rate vs False Positive rate [37].

d *Minimum Description Length Principle* (MPL) states that the complexity of a model M is measured by the length L of bits needed to encode the theory, plus the number of bits needed to encode the data D using the theory [37, 42]. This is a quantification of model performance and is shown as a minimization on $min[L(M) + L(D|M)]$.

Validation of *Developed Detection Scheme:* Not only are the developed machine learning algorithms tested against the rigors of the KDD discipline, the

approach also needs to be tested against the rigors of the application. Under this validation of the detection scheme, the following metrics were used to determine and compare the overall success of the unified approach.

a *Comparison with Existing Bad Data Detection Schemes*: Some techniques for power system bad data detection do exists and are utilized in the monitoring of live systems [28]. These more traditional approaches were compared on the basis of 1) time for conclusion and 2) successfulness to detect. Traditional detection schemes are computationally expensive [43, 44, 30, 45] and are vulnerable to multi-attribute attacks as revealed in [46, 47, 48] and therefore will provide a basis for comparing the developed methods.

b *Topological Assessment* will consist of a study on scalability and versatility. Scalable validation consists of a vertical approach focusing on increasing the size of n (the number of buses to analyze) while versatility will be horizontal in nature and is a test on different configurations of n.

c *Operational Analysis* describes the assessment on the required computational cost for the developed approach. Validation of this type consists of a constant observation and refinement based on the required CPU time.

CHAPTER 3

RELATED RESEARCH

3.1 Introduction

Many approaches have already been developed and continue to be developed to protect the critical infrastructure power grid. However, most of these efforts focus on security from a control reliability perspective and not a cybersecurity perspective. This is in part the result of the fact that the power grid is just now becoming interlaced with networked control devices. Furthermore, it has long been realized the value of knowledge discovery for various applications in the intrusion detection systems (IDS). Many surveys and review articles have been written on the subject and truly demonstrate the success of its application in the domain of detection for security [49, 50, 51, 52, 53, 39]. However, a clear distinction must be made between the power system's traditional security concern of reliability and the much more recent concern of power system cybersecurity. This is not to say that the warranted distinction implies mutual exclusivity, only that it is needed for a thorough literary review on current power system security methods. This chapter provides an overview of past and current efforts for power grid security along with a detailed examination of current IT based cyber-event detection schemes along with an examination at current approaches to cyber-event detection based on a physical perspective.

3.2 Bad Data Detection via State Estimation

Traditional approaches to intrusion detection are based on bad data detection via state estimation. Though not directly labeled as knowledge discovery through data mining, some of the techniques and statistical measures for securing the power grid focus on examining reported state parameters and the resulting state estimation. Such techniques include the bad data detection schemes presented in [43, 44, 30, 45] and analysis of variance techniques as those presented in [40]. These approaches examine reported state parameters on an instance by instance base and utilize circuit theory equations for the detection of anomalies in the resulting state estimation. Data anomalies are then labeled as bad data resulting from measurement errors or faulty equipment.

Early implementation of data mining approaches to bad data detection include the works of [46, 47, 48], wherein neurons are created that use patterns formulated based on historical or training datasets. Artificial intelligence is used in some of these approaches; however, these approaches do not utilize historical state parameters to reach conclusions. Rather these techniques use neurons for faster convergence of the state estimation process. Bad data detection in power systems can be accomplished alongside the state estimation process. State estimation, described previously in Section 2.1.2, mathematically derives a best estimate of the power system even in the presence of bad data. Throughout most of the literature, the objective function to be minimized in the state estimation process is considered to be related to a Chi square distribution.

Some attempts at the detection of injected state parameters via data mining approaches has been performed [54]. However, these approaches are still in their infancy and have no clearly defined structure for algorithmic implementation as that described in other applications of data mining. Data mining on load profiling has been examined in multiple texts where, for instance, decision trees are built via a temporal analysis [55].

3.3 Data Mining for Power Grid Security

An extensive survey of data mining approaches for power system security was conducted in [38] and [39] with a full text on the subject presented in [40, 41]. Most of the classification approaches use decision trees. However, the actual objects being analyzed range from transient stability to steady state power flows. Though not specific to the context of intrusion detection, the works of [56, 57, 58, 38] demonstrate successful implementations of machine learning algorithms for power system security focusing on control reliability. Using decision trees, actual [58] and modeled [57] power system data is used to build models for the purpose of establishing preventive measures for stabilization in instances of required contingencies. In [58], decision trees are also used for contingency analysis; however, the technique utilized is the Iterative Dichotomizer 3 (ID3) process and is based on the entropy of the dataset being analyzed. This ID3 algorithm is similar to the one utilized for power flow contingency analysis in [58].

3.4 Cyber-Event Detection via an IT Perspective

IT based intrusion detection offers another perspective into a possible detection scheme that uses computer based communication metadata and features that utilize standard protocols for the detection of anomalies. In the early stages of this dissertation, effort was taken to create attack vectors targeting control system applications and determine potential detection schemes for these vectors. This section explains some of these results amongst other IT based detection schemes for industrial control systems.

3.4.1 Proof of Concept ICS Attack

In an effort to explore IT based ICS intrusion detection schemes, an exploit using a known vulnerability was crafted and used against the Siemens S7-1200 programable logic controller (PLC) [59]. One major attack performed was a replay attack wherein legitimate command and control packets where captured, malformed, and re-injected into a simulated control LAN for a critical power application. This section describes the observations made during the attacks, focusing on the time differences between legitimate and spoofed command and control packets.

The experimental setup for testing involved four machines: the engineer's work station, the attackers work station, the monitoring workstation, and the Simatic S7-1200 PLC. The engineer's work station comes with Siemens Totally Integrated Automation Portal on a Windows 7 machine. The attacking machine is running Backtrack5r3 which has Wireshark, tcpreplay, and the Metasploit Framework 4.5.0 pre-installed. The experimental network topology is shown in Figure 3.1 and is based on the mirroring functionality of the switch connected to the control center to the

WAN. All traffic sent to the WAN is then mirrored to the monitoring workstation via the mirrored port. This type of assumption allows for the possibility that the attack can originate from either an outsider or insider threat, someone already inside the corporate network, i.e. disgruntle employee. The devices that encompass a control LAN have been discovered to be 'accidentally' connected to the Internet and are not isolated on an internal network [12]. Figure 3.1 shows the network topology for the Testbed with the associated IP address of each control LAN device.

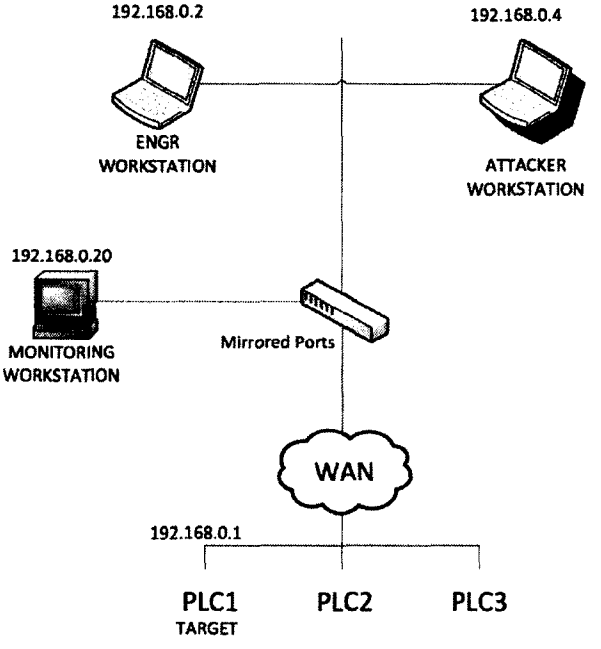

Figure 3.1: IT Based Detection Experimental Network Topology

While the exploits were being launched, the network traffic was being captured using the network analysis tool Wireshark by the monitoring workstation as shown in Figure 3.1. This allowed for a direct comparison in the time sequencing information between legitimate and spoofed command and control packets. Due to the severity of the attacks and the corresponding functionality granted to the engineer, a DoS

attack was used as the basis for comparison between legitimate and spoofed packets from the network traffic. A custom python script was used to extract the conversation streams based on the TCP/IP SYN flag of the start packet and the ACK flag of the subsequent packets in that conversation. The script also provided the difference in the timestamp of start SYN packets and all ACK packets in the TCP stream. In comparing the legitimate and spoofed packet streams, substantial time differences were found.

A total of six streams were plotted for both the attack and the command and control (CC) TCP/IP conversations to the controller. The resulting TCP streams from both the engineer and attacker are plotted in Figures 3.2 and 3.3, respectively. This observation can be numerically shown, where the timestamp for two streams are compared side by side. The legitimate stream, Figure 3.2, is a plot of the timestamp information of the packets from the control engineer while the attack timestamps, Figure 3.3 is a plot of the timestamps from the attacker stream. The delay shown is a direct result of the nature of the attack being conducted. The attack was executed using Metasploit modules, and as a result, it operates within the confines of the software application. Each packet had to be crafted individually with the payload stripped from the original control engineer's TCP packet stream. These findings suggest a unit of measure that may be used in future detection schemes which can differentiate between legitimate and spoofed command and control packets. However, these IT based metrics would not be able to detect a more sophisticated attack. An example of this would be if the engineer's computer become the source of the attack with or without the engineer's knowledge. Such a detection scheme would break down

as there is no longer an accurate basis for classification. It is for this reason the dissertation shifted in a search for a much more robust and context specific detection approach.

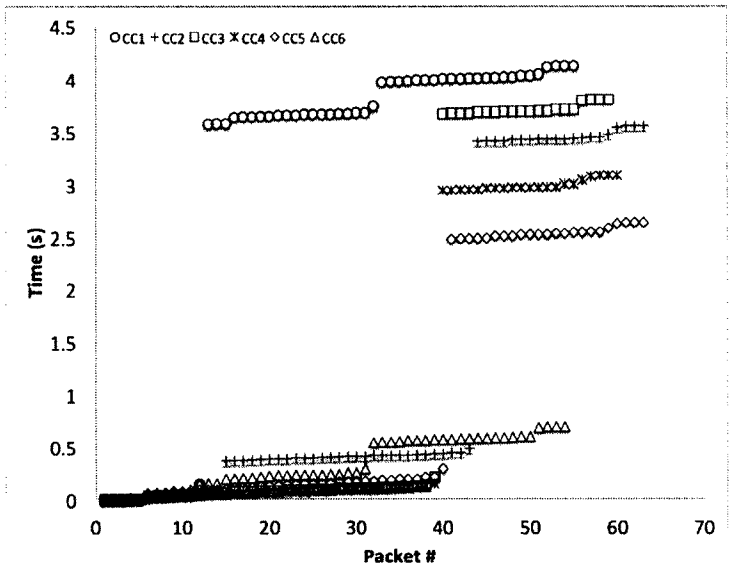

Figure 3.2: Engineer's Control Packet Timestamps

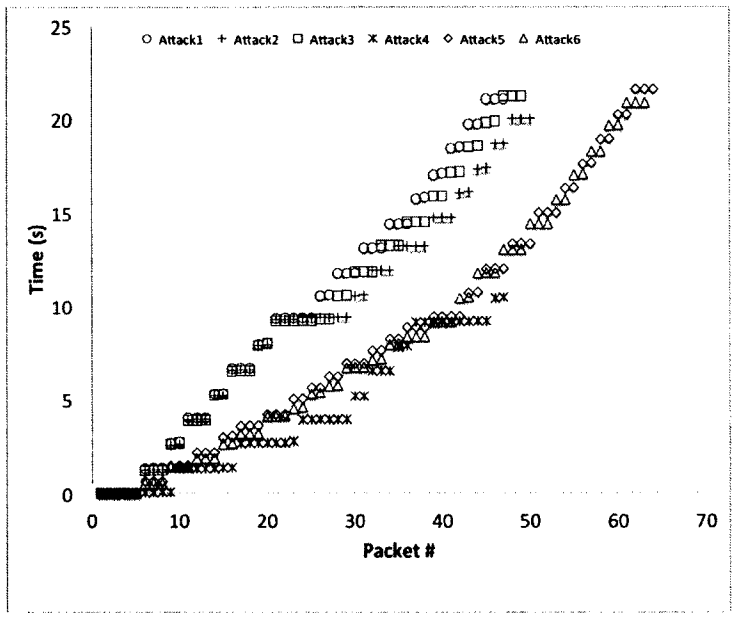

Figure 3.3: Attacker's Control Packet Timestamps

3.5 Cyber-Event Detection via a Physical Perspective

Only recently has cyber-event detection via the physical perspective been viewed as a reasonable option. This in part may be the result of the ever increasing computational power and communication capabilities of power system control and monitoring devices. In fact, several approaches use the distributed computational power for event detection and include [60, 61, 62, 63]. For instance, one possible approach to consider is the use of a state estimation data filter in a distributed manner to detect cyber attacks locally [60]. One drawback of these distributed approaches, however, is the increased latency on an already burdened control priority communication channels.

A very unique approach to the detection of data integrity attacks in a power system is presented in the work of Sridhar *et al.* [64]. In this approach, a physical perspective is used to detect the presence of state variable attacks focusing only on the controller for an automatic generator. Detection is based on real-time load forecasters which predict the generation operation over a given period of time. If the real time operation deviates from the predicted model based on the load forecasters, then a possible cyber-event has been detection.

More closely related to the approach developed by this dissertation, the approach presented by Coutinho *et al.* [65] uses the SCADA's historian databases for the detection of cyber-events. The particular classifier used is stated as a "rough classification algorithm" with little mathematical discussion on exactly how it detects the presence of cyber-events and is performed on a 6-Bus power system. In an early paper [66] by the authors, it was suggested that the rules are derived based on a

'rough set' of data stored in a trusted model. The derivation of rules correspond to deviation trees used to determine the bounds of a value under a certain set of other correlated values. In a more recent article by Giani *et al.* [67], the detection of state variable attack is performed using graphically defined observable islands that form both naturally and in the presence of cyber-events. By comparing the islands of a trusted model with a suspect observation, discrepancies can be identified. The drawbacks of this unique formalization is that it assumed DC load flow and lossless lines. These assumptions lessen the amount of correlated features that can be extracted.

3.6 Conclusions

A multitude of approaches exist for the detection of cyber-events in the power grid. Few, however, take into account the vast amount of information stored in historical SCADA databases. Furthermore, most of the approaches are based on IT centric solutions which require constant access control and patch updates. A direct example of the shortcomings of IT based solutions to the problem is outlined in [5] where it is stated that a government audit of the Tennessee Valley Authority (TVA) revealed several security issues. These issues included several misconfigurations of the DMZ firewalls along with several accounts which had no password for remote access. The audit also revealed that several of TVA's control servers were not up to date with the current patches.

Though not as well defined, approaches that utilize a physical perspective, appear to have the least devastating effect on a power system environment. Only a few of these cyber-event detection approaches exist with even fewer utilizing the complete

set of information that can be derived from analyzing historical SCADA databases. Also, as revealed by this chapter, the majority of the work being explored focuses on data mining approaches to the aspect of reliability security and not necessarily intrusion detection for security. This dissertation seeks to fill these gaps by the development and testing of a cyber-event detection framework based on uniquely crafted machine learning and classification algorithms that harness the topological power system knowledge stored in historical databases.

CHAPTER 4

DETECTION VIA STATE VARIABLES

Detection via state variables, as it is developed in this dissertation, describes the utilization of historical and contingency power system attributes combined with the topological knowledge of the power system for the successful detection and localization of cyber intrusions. By observing high level grouping phenomenon [68] in the reported state parameters, it is possible to replace a group of variables with a single new variable, greatly reducing the redundancy in the data. Examples of reported power systems state parameters include among others: bus voltages and angles, active and reactive powers of generators and loads. Figure 4.1 shows the overall process, the approach taken by this dissertation, and depicts where this detection scheme can be placed relative to an actual power system application. The state variable detection scheme developed throughout this dissertation utilizes multiple transmission systems for both the feature extraction and classification of malicious cyber activity in the power systems. The four main steps for this approach are described below Figure 4.1 and include the following: ***data aggregation***, ***pattern recognition***, ***hybrid classification***, and ***node(s) identification***.

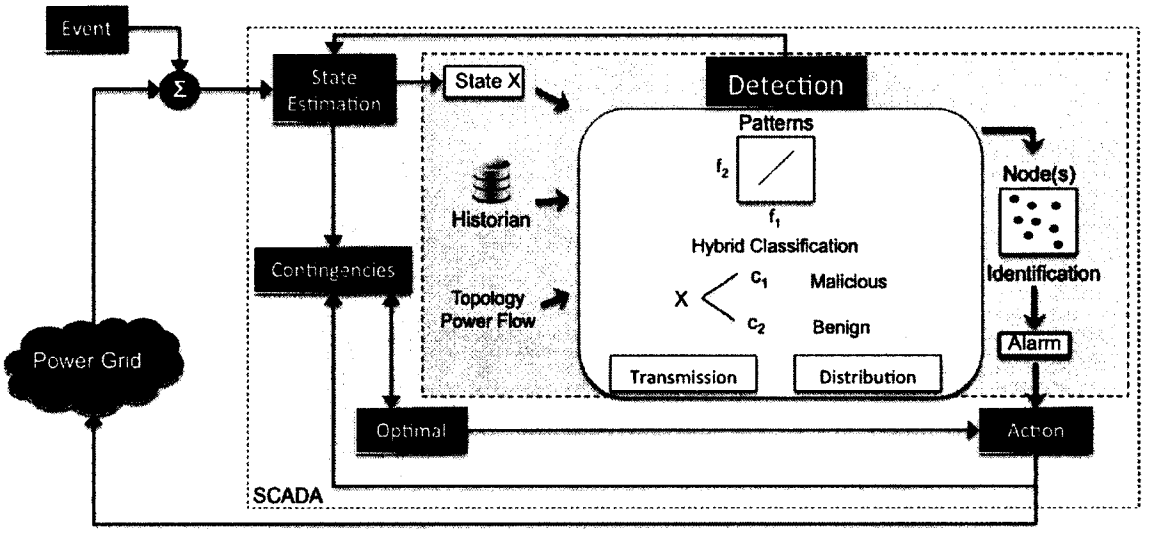

Figure 4.1: Detection Via State Variables Approach

1. **Data Aggregation**:

   Data aggregation is accomplished by combining all available information used to describe the power system. Available information is the result of a) past states, b) contingency states, and c) current incoming state X as shown in Figure 4.1. Past states are contained in the Historian of most SCADA systems and represent true dynamics of the observed system. Contingency states are the result of load profiling and estimates in the power flow based on operational planning. The current state X consists of all currently observed power system attributes. All this information was then accumulated during each experiment to provide an extensive training set for algorithm development.

2. **Pattern Recognition**:

   Pattern recognition is the result of information retrieval methodologies wherein patterns from the large datasets are extracted. Such patterns were extracted via the extensive analysis on the data aggregated, which contains a

collection of power system states. Dimensionality reduction and kernel transformations into different dimensional spaces provided a means for the extraction of information (patterns) provided by a decrease in redundant information.

3. **Hybrid Classification**:

   Classification is the process whereby exploiting the features identified through pattern recognition. Hybrid classification leverages multiple patterns to reach a successful classification. Such an approach guarantees a higher likelihood of true positive classification.

4. **Node(s) Identification**:

   The classification of each state is based on the hybrid approaches and feature extraction methods developed. Two cases exists for node identification. In the case where the classification of state X into the malicious class is based off a single attribute, then that attribute can be classified as malicious and trigger an alarm for further investigation. In contrast, if the overall state X is deemed malicious first, then further analysis was performed to identify the node or nodes that are at the root of the alert.

4.1 Implementation

As noted in Figure 4.1, the detection scheme developed by this dissertation is designed to be implemented alongside an existing SCADA system. Using the data aggregated from the Historian and from contingency analysis, new power system instances or observations are classified as either containing or not containing a cyber-event. Given the close proximity to the SCADA system, this approach can be

implemented in a live manner, classifying newly observed instances. Furthermore, this detection scheme is designed to be 100% passive in that it only reads from control LAN databases and does not issue commands to any control devices. Upon classification of a cyber-event, an alarm is triggered, alerting a security investigator or control engineer of the potential intrusion. Lastly, this detection scheme may also be implemented in a manner that can help forensically identify a cyber-event. This particular utilization of the developed detection scheme is outlined in Section 12.3.

4.2 Approach Overview

The developed cyber-event detection approach finds its power in the utilization of historical and contingency power system states. The approach described is illustrated in Figure 4.2. The detection scheme starts by first taking in the newly observed power system instance. This new instance represents the state of the power system at a given point in time and can include both measured and derived terms. Terms include state parameters that represent bus voltages, bus angles, line flows, real power supplied, reactive power supplied, real power consumed, and reactive power consumed. Upon the classification into the cyber-event set, the observed power system instance is then analyzed to find the source of the cyber-event. This approach takes into consideration the time and computational requirements for such an intrusion detection scheme. It is for this reason the developed detection scheme takes place in phases with advances to the next phase only occurring if required. Sections 4.3 - 4.5 explain each step in detail.

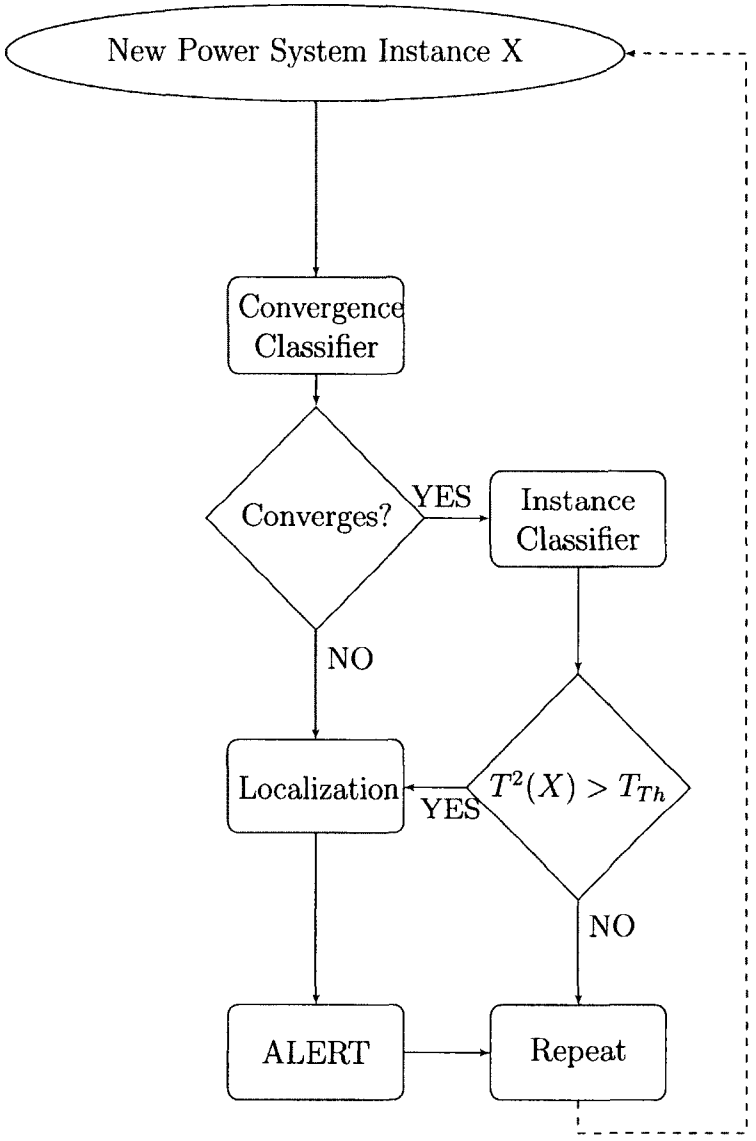

Figure 4.2: Approach Flow Chart

4.3 Convergence Classification

Convergence classification is performed as the first test and analyzes a subset of power system state variables. The subset variables contain the power system state variables that are the inputs to the power flow problem which is solved using the Newton-Raphson method [28]. Convergence classification is based on the fact that due to topological constraints and the fundamental circuit laws, Eqs. (2.1) and (2.2)

[1], the power system can only exists for a certain set of values. By performing several Monte Carlo simulations, as explained in Section 5.3, a full set of converging and non-converging power system instances were created.

The newly created converging and non-converging power system instances are used as training sets to train discriminant classifiers to classify newly observed power system instances. By testing a set of observed power system state parameters in the context of convergence, it can be determined whether or not those values make sense. Recall that non-converging power system instances represent a set of values where the system cannot exist and therefore warrants further investigation. Several discriminant classifiers were tested for this effort and include: linear, diagonal linear, quadratic, and diagonal quadratic.

4.3.1 Convergence Feature

Feature extraction based on power flow convergence exploits the information gained from knowing the power system before hand. A power system observation is bounded by topological, generation, and load constraints and based on those constraints will supply the required power to the load. In a simulated environment, the steady state dynamics of a power system can be obtained using an iterative method such as the Newton-Raphson method [28].

This approach assumes that all converging instances of the Newton-Raphson method represent observable or possible parameters of the power system. Non-converging instances however represent a set of inputs for which the system cannot exists; the system cannot handle that set of inputs and is therefore protected against

those set of inputs. These non-converging instances are labeled as belonging to a malicious set. By using the two classes of inputs, converging and non-converging (benign and malicious) instances, any number of classifiers can be used to predict the class of the incoming power system observation. The process for constructing the two classes is outlined in the flow chart shown in Figure 4.3.

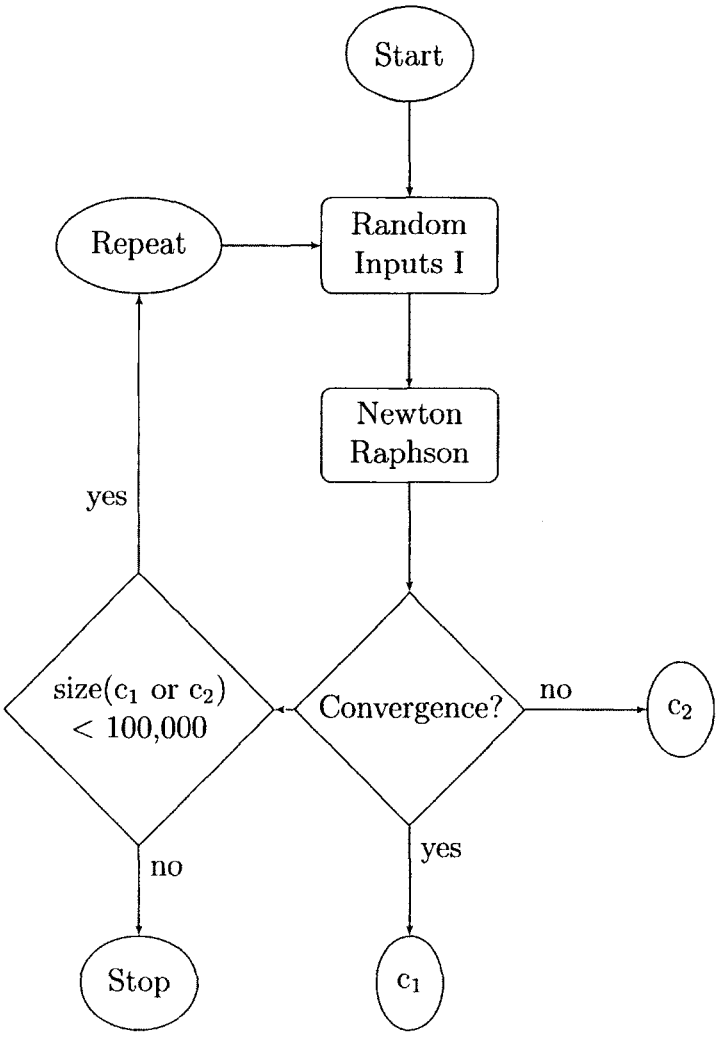

Figure 4.3: Building Classification Dataset

The training sets for both classes (benign and malicious) represent a near full range of possible instances of the 5-Bus power system. To guarantee this near full range of parameters, the inputs to the power simulation had to be properly chosen, then convergence was determined. If the simulated power system converges for a given set of power flow inputs $X_{inputs}^{system}(i)$, then it is possible that the state parameters described within this set may occur in a live *system* and therefore added to the class c_1. If the set of inputs did not converge, then that set of inputs $X_{inputs}^{system}(i)$ was added to the malicious class c_2. This continued until both classes $c_1$and c_2 exceeded a size of 100,000.

4.3.2 Discriminant Classification

Used as a means of classification, generally in cases of a dichotomy, techniques for discriminant analysis are used to place instances or observations into two or more classes, $c_1, c_i, \cdots, c_n$ with n being the number of classes for classification [37]. For development purposes, a total of five discriminant classifiers were tested and include: linear, diagonal linear, quadratic, and diagonal quadratic. Once a discriminant classifier has been built, subsequent instances can be mapped into the classes based on the values of the features or variables describing the observation. The goal of discriminant analysis can be described as an extension on Bayes' Rule, whose formal definition is derived from the axioms of probability. This rule defines a solution to the question of what is the probability that event B occurs given that event A has already occurred, formally $P(B|A)$. Using the two class structure described in Section 4.3.1, four classifiers are trained and tested iteratively against each set. The classifiers

analyzed include: linear discriminate analysis, diagonal linear discriminate analysis, quadratic discriminate analysis, and diagonal quadratic discriminate analysis. Several common evaluation methods are used to determine the best classifier for this particular type of analysis. These and similar analysis of variance (ANOVA) techniques have had successful implementation in many disciplines [69] including the area of power systems [70, 71, 72, 73]. However, these works do not provide a detailed examination on the utilization of discriminate analysis for the detection of cyber intrusions.

Discriminate analysis seeks to determine the conditional probability of each instance given a multivariate vector $\mathbf{x}$ of variables j. This process evaluates the probability that observation $\mathbf{x}_i$ can be placed into the class c_i, $P(c_i|\mathbf{x}_i)$. Observations or instances are then designated as members of the class for which $P(c_i|\mathbf{x}_i)$ is the greatest or lowest depending on the classifier used. In the case of a dichotomy and using a highest value classifier, if $P(c_2|\mathbf{x}_i) > P(c_1|\mathbf{x}_i)$, then the observation $\mathbf{x}_i$ can be labeled as belonging to the class c_2. We now can define a discriminant function for class i as $\delta_i(\mathbf{x}) = P(c_i|\mathbf{x})$. The boundary between the two classes is the region for which the discriminate functions are equal, $\delta_i(\mathbf{x}) = \delta_{i+1}(\mathbf{x})$. By extrapolating Bayes' Rule to the context of discriminate functions, it can be shown that

$$\delta_i(\mathbf{x}) = \ln\, p(\mathbf{x}|c_i) + \ln\, P(c_i|\mathbf{x}) \tag{4.1}$$

holds true [74],[37], where $p(\mathbf{x}|c_i)$ is the probability distribution functions for the feature vector $\mathbf{x}$ contained within the class c_i. Assuming a multivariate normal Gaussian distribution of the feature vectors within each class, the probability distribution

function can be defined as

$$p(\mathbf{x}|c_i) = \frac{1}{(2\pi)^{\frac{n}{2}}|\mathbf{S}_i|^{\frac{1}{2}}}\exp[-\frac{1}{2}(\mathbf{x}-\mu_i)^T\mathbf{S}_i^{-1}(\mathbf{x}-\mu_i)]. \tag{4.2}$$

By plugging Eq. (4.2) into (4.1) and expanding the logarithms while dropping the constant term, the quadratic discriminant function can be obtained. Any constant terms can be eliminated given that the functions are used to make a decision and are the same for all classes. In the case of a dichotomy, this can be formally seen by defining a *dichotomizer* as $d(\mathbf{x}) = \delta_1(x) - \delta_2(x)$. If the *dichotomizer* is positive, then the discriminate function for c_1 is higher than that of class c_2; thus, the instance can be classified a class 1 instance. The constant terms of the discriminate functions will cancel.

Linear

Linear discriminant analysis (LDA) assumes that the covariances are equal for all classes ($\mathbf{S}_i = \mathbf{S}_{i+1} = \mathbf{S}$) [75]. After expanding the quadratic and dropping the constant covariance term the linear discriminant function,

$$\delta_i(\mathbf{x}) = \mu_i^T\mathbf{S}^{-1}\mathbf{x} - \frac{1}{2}\mu_i^T\mathbf{S}^{-1}\mu_\mathbf{i} + \ln P(c_i), \tag{4.3}$$

can be obtained, where $P(c_i)$ is the priori probability distribution function for class i. A special type of LDA is the diagonal linear discriminant analysis (DLDA) for which the covariance matrix $\mathbf{S}$ in Eq. 4.3 is set to be a diagonal matrix.

Quadratic

In cases where the covariance matrixes are not the same for all the classes, the quadratic discriminant analysis (QDA) method can be used. Derived directly from

the logarithmic expansion of the probability distribution function, the discriminate function for quadratic cases can be calculated using

$$\delta_i(\mathbf{x}) = -\frac{1}{2}\ln|\mathbf{S}_i| - \frac{1}{2}(\mathbf{x} - \mu_i)^T\mathbf{S}_i^{-1}(\mathbf{x} - \mu_i) + \ln P(c_i), \tag{4.4}$$

where $P(c_i)$ is the priori probability distribution function for class i. Similar to LDA a special type of QDA is the diagonal quadratic discriminant analysis (DQDA) for which the covariance matrix $\mathbf{S}$ in Eq. (4.4) is set to be a diagonal matrix.

4.4 Instance Classification

Upon classification into the converging set via the discriminant classifier, each newly observed power system proceeds to the next test. This next test seeks to compare the newly observed power system observation to past observations to determine if it is an in-control power system instance. Every observable power system state variable is used in this second test covering the greatest amount of features. Classification is performed using a dimensional transformation scheme that transforms the power system instance into a new dimensional space where each axis is reflective of the covariances found in the training set. If the instance as a whole passes the second test, then it is considered an in-control instance, one that is possible given topology and historical knowledge, and the instance is classified as not having a cyber-event. The alternative to being classified as an in-control instance is if the discriminant classifier labels the newly observed instances as an out-of-control instance. If this is the case then localization is performed immediately.

4.4.1 Feature Extraction via Transformation

In any determinable system there generally is a finite number of driving forces which governs how the system behaves. By observing grouping phenomenon in the data, it is possible to replace a group of variables with a single new variable, greatly reducing the redundancy in the data. Principle component analysis (PCA) is a quantitative process for achieving a system simplification. A decrease in redundancy and an overall simplification of the data is made possible through a transformation into a new vector space where all the basis vectors are independent of each other. The basis vectors in the new dimensional space are called principal components. The complete set of orthogonal principle components mapped to the new space form what are called the orthogonal basis vectors for the data [37].

Perhaps one of the most commonly used statistical analysis linear transformation tools [37], PCA is based on the statistics of a training set to transform the set linearly in such a way that the new primary basis are independent of each other. The linear transformation used is based on a covariance matrix which is defined by the patterns found in the training set. PCA finds a linear transformation such that

$$\mathbf{Y} = \mathbf{W}\mathbf{X}, \tag{4.5}$$

where $\mathbf{X}$ and $\mathbf{Y}$ are mxn matrices related by a transformation $\mathbf{W}$. Based on Eq. (4.5) the following variables can be defined:

- $\mathbf{w_i}$ are the rows of $\mathbf{W}$
- $\mathbf{x_i}$ are the columns of $\mathbf{X}$
- $\mathbf{y_i}$ are the columns of $\mathbf{Y}$.

The row vectors of $\mathbf{W}$ $\{w_1, ..., w_m\}$ are called the principal components of $\mathbf{x}$. Before PCA can be applied to a dataset, it is first customary to preform a certain amount of sanitization on the data. This sanitization guarantees any unintended biassing of the new components.

Centering and Normalization

One aspect of sanitization is to ensure that the data matrix $\mathbf{X}$ is centered and normalized. Centering of the data matrix is accomplished by using the mean vector $\mu = E[\mathbf{x}] = [E[x_1], E[x_2], ..., E[x_{16}]]$ where $E[x_1]$ is the mean of the first column of the data matrix $\mathbf{X}$. These values are then subtracted from the associated columns to produce a centered data matrix $\mathbf{X_c}$. With this notation, a new data matrix $\mathbf{X}$ with dimensions mxn is created where each instance or run of the simulation produces a column vector. For instance, the first row of data matrix $\mathbf{X_c}$ produces a column vector $\vec{\mathbf{X}}_1$. This representation of the instances enables the creation of the new data matrix $\mathbf{X}$, where

$$\mathbf{X} = \begin{bmatrix} \vec{\mathbf{X}}_1 & \dots & \vec{\mathbf{X}}_n \end{bmatrix} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ x_{2,1} & \cdots & x_{2,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{1m,n} \end{bmatrix} \tag{4.6}$$

From here the normalized covariance $\mathbf{S_X}$ was determined using the unbiased estimator for normalization using

$$\mathbf{S_X} = \frac{1}{n-1}\mathbf{X}\mathbf{X}^T. \tag{4.7}$$

This produced a covariance matrix with dimensions mxm with the diagonal terms representing the variances and the off-diagonal terms representing the covariances of data matrix $\mathbf{X}$. The closer the off-diagonal terms are to zero, the closer the variables represented by the indices of $\mathbf{S_X}$ are to being completely uncorrelated. Conversely, the higher these off-diagonal terms are, the more correlated the two variables are. Also, the higher the off-diagonal terms are, the higher the redundancy is in the data matrix $\mathbf{X}$.

Solving PCA

The linear transformation produced by PCA selects a transformation $\mathbf{W}$ such that the principle components or basis vectors w_i produced are completely orthonomal. Orthonomality is ensured due to the fact that the dot product of each basis vector with another produces the Kronecker delta function, $w_i \cdot w_j = \delta_{ij}$. In addition to being orthonormal, the basis vectors are ordered based on the amount of variance that is being accounted for by that basis vector or principal component. This corresponds to the fact that PCA will produce a transformation matrix $\mathbf{W}$ such that the variance of data matrix $\mathbf{X}$ is mostly accounted for by principal component w_1.

The goal of PCA is to produce a transformation where little to no redundancy can be seen in the new vector space. As mentioned in the previous section, the lower the diagonal terms of the covariance matrix are, the lower the redundancy is in the data. Therefore, the solution to PCA seeks a covariance matrix $\mathbf{S_Y}$ such that the off-diagonal terms are zero where,

$$\mathbf{S_Y} = \frac{1}{n-1}\mathbf{Y}\mathbf{Y}^T. \tag{4.8}$$

Plugging Eq. (4.5) into Eq. (4.8) we have

$$\mathbf{S_Y} = \frac{1}{n-1}\mathbf{W}(\mathbf{X}\mathbf{X}^T)\mathbf{W}^T. \tag{4.9}$$

With this solution to PCA, it can be shown that the principal components of data matrix $\mathbf{X}$ are the eigenvectors of $\mathbf{X}\mathbf{X}^T$ or are the rows of $\mathbf{W}$. Also, the ith diagonal term of $\mathbf{S_Y}$ is the variance of $\mathbf{X}$ projected onto $\mathbf{p_i}$.

4.4.2 Classification

To use PCA for detection, we seek a method where for a suspicious data matrix $\mathbf{X}'$, this data can be projected into the new dimensional space and statistical inferences made such that the successful identification of malicious instance $\overrightarrow{\mathbf{X}'}_m$ is possible. If malicious instance $\overrightarrow{\mathbf{X}'}_m$ does not follow the statistical trends identified by PCA using the training set $\mathbf{X}$, it can be classified as a potential malicious instance. Once classified the instance, then it can be further investigated to identify the cause of the compromised reading $\mathbf{x}'_i$. This would allow the investigator or control engineer to isolate the intrusion. An example of this would be if, for $system = 5bus$, $\mathbf{x}'_3$ was found to be the malicious term in the malicious vector $\overrightarrow{\mathbf{X}'}_m$ and $\mathbf{x}'_3$ corresponded to $\mathbf{V}_5$ as shown in Table 4.1, then this would mean that the voltage at bus 5 has been compromised.

Table 4.1: 5-Bus Data Matrix Features

Variable	New Variable	Notes
V_1, V_2, V_3, V_4, V_5	$x_1 - x_5$	Voltages
$\theta_2, \theta_3, \theta_4, \theta_5$	$x_6 - x_9$	Voltage Angles
PG_1, PG_3	$x_{10} - x_{11}$	Real Power Generated
QG_1, QG_3	$x_{12} - x_{13}$	Reactive Power Generated
$PL_1 - PL_5$	$x_{14} - x_{18}$	Real Power Load
$QL_1 - QL_5$	$x_{19} - x_{23}$	Reactive Power Load

Hotelling's T^2

The Hotelling's T^2 value,

$$T^2 = n(\mathbf{X} - \mu)'\mathbf{S}^{-1}(\mathbf{X} - \mu), \tag{4.10}$$

is an extension of the t-test used to determine the difference between means of two independent variables. This extension allows for a statistical measure of the multivariate distance of each instance from the center of a dataset. The result allows for the detection of instances that occur at far distances from the data center as defined by data matrix $\mathbf{X}$. The detection approach presented in this dissertation is a probabilistic approach in describing how likely an instance is to occur. Instances that fit to the dynamics of the data matrix $\mathbf{X}$ or control set have a high likelihood of occurring while instances that lie on the boundaries are less likely to occur. It can also be shown [76] that the Hotelling's T^2 value follows the $\mathcal{F}$ distribution as defined by

$$T^2 \sim \frac{(n-1)p}{(n-p)}\mathcal{F}_{p,n-p}(x), \tag{4.11}$$

where p is the number of principal components retained and n is the number of instances in the sample space. The $\mathcal{F}$ cumulative probability distribution function returns the cumulative probability of obtaining a value x for given parameters p and n. By rearranging Eq. (4.11), we can calculate that the probability of observing at least T^2 is

$$P(\geq T^2) = 1 - F_{p,n-p}(z), \tag{4.12}$$

where

$$z = T^2\frac{(n-p)}{p(n-1)}.$$

The new formulazation allows for a probabilistic metric to determine whether or not an instance is in-control. If the instance is in-control, then it follows the dynamics as defined by the data matrix **X**. A low probability, as defined by Eq. (4.12), for observing at least that T^2 corresponds to a high T^2 value. This means that the instance is far away from the multivariate center and therefore is least likely to occur. Conversely, a high probability corresponds to a low T^2 value and is therefore closer to the center of the data.

Any in-control instance can be considered an instance whose variables follow the dynamics of the system. These instances can be considered instances that would occur under normal operation. An out-of-control instance would be an instance whose dynamics do not fit uniformly in with the dynamics of the in-control instances. Out-of-control instances are not considered normal operation and therefore any operation that exists outside of normal operation can be classified as an out-of-control instance. The Hotelling's T^2 value and the probabilistic metric aided in the classification of the instances into either an in-control set or an out-of-control set. An in-control instance would have a low T^2 value and high probability of occurring. While an out-of-control instance would have a low probability and a high T^2 value. Using this statistical metric classification of instances can be made such that instances that are not in-control are classified as a cyber-event.

Detection using the Hotelling's T^2 value is based on creating a quantile threshold. By transforming the trusted model into the new dimensional space where redundancy is reduced and plotting the Hotelling's T^2 value of each power system instance of the trusted model, a threshold value, T^2_{th}, can be created. The new threshold value is

determined by letting $T_{th} = Q_\alpha = inf\{q : P[T^2 < q] \geq \alpha\}$, where α is the probability. If for any newly observed power system instance that instance's Hotelling's T^2 value is found to be greater than T^2_{th}, then it can be classified as an out-of-control instance.

4.5 Localization

However, the challenge then comes to classify the node or source of the cyber-event. As the convergence feature is used to train discriminate classifiers and the dimensional transformation used for the instance classification, localization is a classification based on the statistics found within each variable independently. Localization is only performed once an event has been labeled as possibly containing a cyber-event. The flow algorithm depicting where localization is to occur in the detection scheme is shown in Figure 4.2.

4.5.1 Grubbs Test

The Grubbs test, also known as the maximum normed residual test, is used to detect outliers in a univariate dataset [77] [78]. Formally, the test can be defined as a means of hypothesis testing. By using the test statistic G as defined by

$$\mathbf{G} = \frac{max|Y_i - \bar{Y}|}{s}, \tag{4.13}$$

the result of the hypothesis test can either be H_0 for *no outliers in the dataset* and H_a if there is exactly one outlier in the dataset. With Y_i representing the measured value, $\bar{Y}$ representing the sample mean, and s representing the standard deviation of the state variable, it is also possible to define the critical region for each variable. With $t_{\alpha/(2N),N-2}$ denoting the critical value of the t distribution with

(N-2) degrees of freedom and a significance level of $\alpha/2N$ a formalization of the test hypothesis can be determined. The test hypothesis H_a is true if for a given dataset $Y = [y_1, y_2, \ldots, y_{N-1}, y_N]$,

$$G > \frac{(N-1)}{\sqrt{N}} \sqrt{\frac{(t_{\alpha/(2N),N-2})^2}{N-2+(t_{\alpha/(2N),N-2})^2}} \tag{4.14}$$

is found to be true.

For clarity, the Grubbs test is syntactically adjusted to fit the application of detecting the compromised power system state variable. For an incoming power system instance X_i, the dimensional transformation scheme, PCA, transforms it into a new vector space and a distance classifier is used to determine the validity of the instance. However, this does not identify the variable that was the source of the cyber-event. Therefore, after each power system instance cyber-event classification, the Grubbs test can be performed on each variable independently to determine any potential anomalies in that state variable based on historical readings. Each newly observed instance i is comprised of n variables with each variable labeled as $x_{i,j}$. By letting $Y_j = [x_{1,j}, x_{2,j}, \ldots, x_{N-1,j}, x_{N,j}]$, a new notation can be defined for the identification scheme. For instance, the vector Y_1 describes the full set of bus 1 voltages.

Since the newest power system instance is the one that has been identified as containing the cyber-event, the state variables of this N^{th} observation will be the ones analyzed by the Grubbs test. The Grubbs test can now formally be defined as

$$\mathbf{G} = \frac{|Y_{N,j} - \bar{Y}_j|}{s(Y_j)} \tag{4.15}$$

and

$$\mathbf{G} > \delta_{\alpha,N}. \tag{4.16}$$

In Eq. (4.16) a discriminate $\delta_{\alpha,N}$ is created that equals the right hand side of Eq. (4.14). Localization via the Grubbs Test is based on performing Eq. (4.16) for each of the state variables found in the suspicious power system instance. If $\mathbf{G}$ is found to be higher than $\delta_{\alpha,N}$, then that variable is flagged as being the potential source of the cyber-event.

4.6 Conclusions

Current solutions to detecting cyber-events in the power grid fundamentally lack a complete picture. Specifically, these more traditional approaches use a cyber perspective which fundamentally ignores the system's physical perspective. This chapter outlined a knowledge discovery approach for the detection of cyber-events based on a physical perspective. The physical perspective is built based on a trusted model extracted from the historical SCADA databases of the power system under analysis. Two uniquely crafted classifiers, a convergence classifier and an instance classifier are used for the detection of cyber-events while a localization classifier is used to identify the source(s) of the event(s).

The first classifier, the convergence classifier, is based on discriminate analysis and is used to determine if a subset of the power system instance variables mathematically satisfy the power flow equations. Next, the instance is placed through the instance classifier where the power system instance is transformed via PCA to a new dimensional space for comparisons against the trusted mode. If either classifier identifies the presence of an event, localization begins and is based on the Grubbs Test performed for each state variable of the suspicious power system instance. Results of

the cyber-event detection scheme outlined in this chapter are presented in Chapters 8 and 9. Furthermore, Chapter 12 outlines some additions that may increase the overall accuracy of the physically derived cyber-event detection scheme.

CHAPTER 5

SIMULATION MODELS

5.1 Introduction

The knowledge discovery approach for the detection of state estimation attacks utilizes a set of models to simulate power system dynamics and to produce a set of possible state estimation attacks. The two power system models used for this examination are often found in the literature [2, 79, 80, 81, 82] and provides a set of possible topologies for the testing and development of power system control and security detection schemes. The attack models include the changing of an observed power system instance in a manner that targets one or multiple power system state variables. It is considered, as described in Section 5.4, that this change can take on many forms.

5.2 Modeling Power Systems

The following two sections describe the two power system models utilized throughout this dissertation for the development and testing of the detection scheme. In an attempt to mirror live power systems for the development process, simulations include such factors as line impedances along with shunt capacitance for transmission lines greater than 50 miles. This approach is often utilized in both academia and industry and is considered the standard approach for power flow studies [1].

Furthermore, each system is examined in two different ways. The first is where only the following information is included: bus voltage amplitude, voltage angles, real and reactive powers generated, along with the real and reactive loads being consumed at each bus. The second considers everything previously mentioned while adding the real and reactive powers being injected into each bus via the transmission lines. An illustration of the injected powers is shown in Figure 5.1. The apparent power $S_{i,j}$ is made up of the real and reactive powers $P_{i,j}$ and $Q_{i,j}$, respectively.

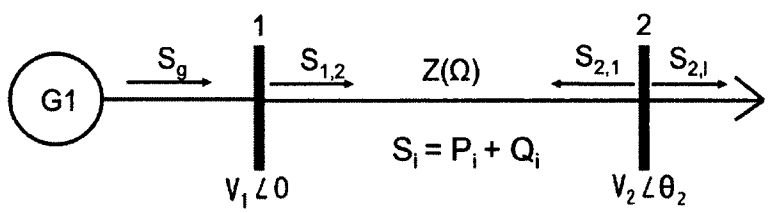

Figure 5.1: Power System Notation

The term powers when stated throughout the remainder of this dissertation represents both the real and reactive components. The subscripts i and j denote the bus numbers in sequence of the origin bus i and is directed at the destination bus j. Direction is maintained mathematically using negative sign notation. For instance, a value of $-S_{2,1}$ would denote that power is entering bus two from bus 1. Lastly, because the line impedances are being considered throughout this analysis, $S_{1,2} \neq -S_{2,1}$.

5.2.1 5-Bus

The first power system utilized for the development and testing of the detection scheme is a 5-bus 135 kV power system with a base power of 100 MVA. This system is provided in Stevenson *et al.* [2] as an example into approaches for power flow studies,

and for completeness, a one-line diagram and the corresponding system parameters are presented in Appendix A. System parameters include line impedances, and shunt capacitances. Also, provided in Appendix A is an example power flow simulation with inputs and outputs provided in Tables A.2 and A.3, respectfully.

5.2.2 IEEE 14-Bus

The second power system utilized is the IEEE 14-bus standard test case operating at 135 kV with a base power of 100 MVA. This particular system has been used extensively in the literature [79, 80, 81, 82] for the purpose of simulation and development of power control applications. The one-line diagram and corresponding system parameters for the IEEE 14-bus power system are shown in Appendix B. Similarly, system parameters include line impedances, and shunt capacitances. Also, examples of inputs and outputs of the IEEE 14-Bus for the power flow problem are provided in Tables B.2 and B.3.

5.3 Monte Carlo Simulations

In order to obtain a full set of power system attributes, several Monte Carlo Simulations were conducted using the 5-Bus [2] and IEEE 14-Bus [83] power systems described in Appendix A and Appendix B, respectfully. Monte Carlo power flow analysis is a well known method for probabilistic power flow studies [28] and can either have a deterministic set of inputs or a pseudorandom sample set of inputs. The probability density function of the uniform distribution utilized for the Monte Carlo simulations follows Eq. 5.1. The exact values of b and a include $a = -2$ and $b = 2$,

allowing for considerations twice that of the multiplied power system instance.

$$p(x) = \frac{1}{b-a} \tag{5.1}$$

Once a power system's Monte Carlo simulation is completed, the results are collected into a data matrix $\mathbf{X}$ with $\mathbf{X}_{5Bus}$ and $\mathbf{X}_{14Bus}$ denoting the trusted model of the 5-Bus and IEEE 14-Bus power systems, respectively. Furthermore, in the general sense the data matrix $\mathbf{X}$ will be denoted as $\mathbf{X}_{System}$.

Each newly constructed data matrix $\mathbf{X}_{System}$ is a full set of empirical readings that may exist for that given power system topology. This simulated data is to serve as the readings reported to and found in a transmission level SCADA system. The resulting power flow analysis is used to create a trusted model and random instances are then selected to build simulated cyber-events to test the developed detection scheme. It should be noted that the power flow analysis in a live implementation of the developed detection will serve on in a complimentary manner. The primary source of information will be provided by the Historian server which records live actual power system state parameters that may deviate from a mathematical model. This and the exact suggested implementation and live testing of the developed detection scheme is discussed in Chapter 11.

5.4 Cyber-Event Attack Models

The cyber-event attack model used for the development and testing of the detection scheme presented in this dissertation is based on single variate and multi-variate state estimation attacks. A state estimation attack is one where a reported state variable is maliciously recorded in the historical database of a SCADA system.

The approach this dissertation develops is two-fold in that it represents two possibilities that can occur in a power system. Event #1 can be considered to be a non-malicious incident in which the controller or sensor in the field making the measurement breaks or becomes damaged as a result of natural causes. Some examples of this may include natural disasters, faulty equipment, or wear on the device over the years. Event #2 can be classified as an actual malicious event in which an attacker purposely launches an attack against the control system. Examples of this include the falsification or spoofing of data values reported from a smart meter as revealed by Brinkhaus *et al.* [26]. This work currently makes no distinction of the two events, only that it is able to determine that an event has occurred. Once detection has occurred, that instance then can be further investigated and the actual cause of the event can be determined.

Each type of event can produce a multitude of numerical values depending on the extent of the device failure or malicious attack. In order to encompass the full range of event possibilities, two sets of values are simulated. A type I event is one wherein a cyber-event causes the power system state variable to read, measure, or record a value of zero. The second cyber-event, a type II event, is one wherein the power system state variable is read, measured, or recorded as being a value other than zero. For a structured examination, the taxonomy of attacks considered in this examination are described in Table 5.1. Furthermore, each type of attack, either a type I or a type II, producing a cyber-event reading of x_i' can target either a single (S) variable or target multiple (M) variables at once.

Table 5.1: Attack Type Notation

		Event Type	
		$x'_i = 0$ (I)	$x'_i \neq 0$ (II)
Attack Type	Single Variate (S)	SI	SII
	Multivariate (M)	MI	MII

5.4.1 Single Variate Attack of Type I

A single variate attack of type I is one wherein only a single variable is considered to be the source of a cyber event at a time. Also, this cyber event is one such that the resulting state variable that was attacked has a value of zero, $x'_i = 0$. To simulate these types of events, a random instance from data matrix $\mathbf{X}$ was selected. This random instance vector $\overrightarrow{X_r}$ serves as the basis for the event simulation. The selection of $\overrightarrow{X_r}$ of $\mathbf{X}$ is based on picking a random index i such that $\overrightarrow{X_r}|_{r=i}$ and $\{i \in \mathbb{Z}| \leq N\}$ where Nxn is the size of $\mathbf{X}$. Next, an initialization vector for the power system, $System$, of all ones and of length n is created and serves as the bases for the simulation, $I_{System} = [a_1 \cdots a_n] = [1 \cdots 1]$. To determine which variable will simulate the attack, a random index l is selected such that $\{l \in \mathbb{Z}| \leq n\}$, where n is the size of vector $\overrightarrow{X_i}$ and I_{System}. The element of I_{System} defined by random index l is now changed to zero, producing the initialized simulation attack vector $I'_{System}[a_l] = 0$. Using this notation a type I single variate attack instance for the power system $System$ is created according to Eq. (5.2) and is based on the Hadamard product,

$$\overrightarrow{X_i}' = \overrightarrow{X_i} \circ I'_{System}. \tag{5.2}$$

5.4.2 Multivariate Attack of Type I

In a type I multivariate attack, two or more state variables of a power system instance are considered to have changed to zero. To create the set of type I multivariate

attack instances for the power system, *System*, a vector of ones is created, $I_{System} = [a_1, \cdots, a_n] = [1, \cdots, 1]$. Using the data matrix $\mathbf{X}_{NXn}$ for the power system in question, a random row, $\overrightarrow{X_r}$, is selected to form the attack instance. The row $\overrightarrow{X_r}|_{r=i}$ is determined such that $\{i \in \mathbb{Z}| \leq N\}$, where N is the total number of power system instances retained in the system's trusted model. If the number of variables that will be attacked is represented by k and $k = 2$, then two random random indices l and j are picked such that $l \neq j$ and $\{l, j \in \mathbb{Z}| \leq n\}$. These indices provide the index for which two variables will simulate the attack, specifically the elements $I'_{system}[a_l] = 0$ and $I'_{System}[a_j] = 0$. Using this notation Eq. (5.2) can be utilized for the multivariate attack of type I as long as the initialization vector I'_{System} described in this subsection is used.

5.4.3 Single Variate Attack of Type II

In a similar manner, Equation (5.2) can be used to construct the single variate attack of type II, as long as the newly crafted initialization attack vector, I'_{System}, is crafted. To represent this type of attack instances for the power system, *System*, a vector of ones is created of size n, $I_{System} = [a_1, \cdots, a_n] = [1, \cdots, 1]$. Letting k represent the number of variables that will be attacked, $k = 1$ in the case of the single variate attack. For $k = 1$, a single random index l is picked such that $\{i \in \mathbb{Z}| \leq n\}$. This index l represents the origin of the simulated attack. Using this notation, the element $I'_{System}[a_l] = U(0, 1)$ where $U(0, 1)$ is the uniform random distribution function with bounds between 0 and 1. Following Equation (5.2), the attack instance $\overrightarrow{X_i}$ is created based on I'_{System}.

5.4.4 Multivariate Attack of Type II

The same approach described in the previous subsections is also used to construct the multivariate attack of type II. In this case, two or more variables are changed to a number other than zero. If the number of variables that will be attacked is represented by k and $k = 2$ then two random random indices l and j are picked such that $l \neq j$ and $\{l, j \epsilon \mathbb{Z}| \leq n\}$. Using the indices i and j, for when $k = 2$ the attack initialization vector becomes $I'_{System}[a_i] = U(0,1)$ and $I'_{System}[a_j] = U(0,1)$, where $U(0,1)$ is the uniform random distribution function between 0 and 1. Using this notation, a multivariate attack of type II for power system *System* is created according to Eq. (5.2) with the only substitution being the initialization attack vector, I'_{System}, formulated in this subsection.

5.5 Conclusions

This chapter laid the foundation in the formalization of simulation models used to develop and test the cyber event detection scheme outlined in this dissertation. Multiple probabilistic Monte Carlo simulations were ran based on the Newton-Raphason method to construct near realistic power system instances. A total of two power system topologies are used, a 5-Bus and the IEEE 14-Bus power system. For each system, two separate considerations are made. The first consideration is that only the bus voltages, angles, and powers consumed and generated are known. The second consideration assumes a more complete observation of the power system in that is takes into account the powers being injected into the transmission lines from each bus.

CHAPTER 6

FEATURE EXTRACTION RESULTS

6.1 Introduction

The following Sections describe the feature extraction results for the 5-Bus and the IEEE 14-Bus power systems. Instances were created for each system using the Monte Carlo simulations described in Section 5.3. Based on the simulations, several key features are extracted that describe power systems in general and that are unique to the individual system topologies. Features offer a perspective on normal operation and are used as classification metrics for the cyber-event detection scheme developed in this dissertation. The following list outlines were each extracted feature is used in the developed detection scheme.

1. Convergence Feature

   The convergence feature is used in the 1st step of the detection scheme called the convergence classifier.

2. Dimensional Transformation

   Features based on the dimensional transformation are used in the instance classifier.

3. Univariate Statistics

   The localization stage uses univariate statistics to localize or determine the source of the cyber-event.

6.2 Convergence Feature

Feature extraction of convergence information offers valuable insight into what the power system can and cannot handle. The set of state variables that produce a reasonable power system model collectively exist in what is called the feasible region [84]. If the power flow analysis converges for a set of inputs, then those set of inputs (topological, load, and generation constraints) produces a feasible power system instance that could potentially be observed in a live power system. The convergence feature describes the extraction of information when looking at only a subset, specifically the subset $\mathbf{C} = c_1 \cdots c_m$ where $\{\mathbf{C} \in \vec{X}\}$. In order to be placed in the converging set, the input parameters had to solve the power flow problem in less than 26 iterations with a tolerance of 0.01.

Convergence is considered important as it provides an initial check for the potential presence of a cyber-event as outlined in Figure 4.2. It is also recognized that in some instances the Newton-Raphson method may fail to converge even for an instance contained inside the feasible region [84]. However, the region that contains the feasible non-converging instances is small as compared to the region of feasible converging instances as developed by the Monte Carlo simulations. It is noted in the the future work, Chapter 12, how the convergence classifier could possible be modified to account for the slightly larger feasible region.

6.2.1 5-Bus

The 5-Bus power system state variables analyzed for convergence analysis are shown in Table 6.1 along with the descriptions of each variable. These variables serve

as the inputs to the power flow calculations and if converge represent possible power system state parameters. There are a total of 13 power system state variables that are used for inputs into the Newton-Raphson power flow problem. The voltage variables are considered voltage controlled buses as these values are inputs to the power flow problem. The voltage controlled parameters v_1 and v_2 are mapped in Figure 6.1 and show the area of convergence for the 5-Bus test system. This figure represents a total of 1,000 simulated power flow inputs with 500 making up the converging set shown using a triangle marker and 500 making up the non-converging set shown using a circle marker. Over 95% of the converging inputs are contained within the middle ellipsoid shown in Figure 6.1.

Table 6.1: 5-Bus Convergence Parameters

Variable(s)	Details
V_1, V_3	Bus 1 and 3 Voltage
PG_3	Bus 3 Real Power Generated
$PL_1, PL_2, PL_3, PL_4, PL_5$	Bus i Real Power Load
$QL_1, QL_2, QL_3, QL_4, QL_5$	Bus i Reactive Power Load

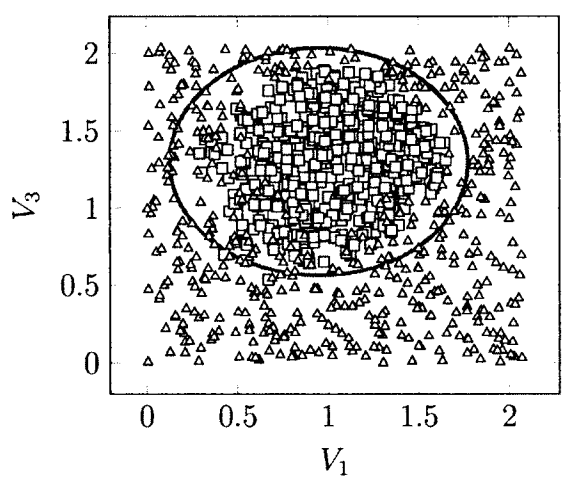

Figure 6.1: 5-Bus Convergence Map for Controlled Voltage Parameters

Figure 6.1 is explained given the fact that the power flow solution only exists for a set region or area of convergence [84]. The information shown in this figure provides insight into the possibility of using a discriminate classifier given the distinct separation between the two converging and non-converging classes.

6.2.2 IEEE 14-Bus

Similar to the 5-Bus analysis approach, the 14-Bus power state variables analyzed for convergence analysis are shown in Table 6.2 along with the descriptions of each variable. These variables serve as the inputs to the power flow calculations, and if converge they also represent possible power system state parameters. As Table 6.2 shows, there are a total of 31 power system state variables that are used for inputs into the IEEE 14-Bus Newton-Raphson power flow problem. Unlike the 5-Bus system, the 14-Bus system has a total of 5 voltage control busses.

Table 6.2: 14-Bus Convergence Parameters

Variable(s)	**Details**
V_1, V_2, V_3, V_6, V_8	Bus i Voltages
PG_2	Bus 2 Real Power Generated
QG_3, QG_6, QG_9	Bus i Reactive Power Generated
$PL_2 - PL_6, PL_9 - PL_{14}$	Bus i Real Power Load
$QL_2 - QL_6, QL_9 - QL_{14}$	Bus i Reactive Power Load

Figure 6.2 reveals an interesting trend showing a near linear convergence relationship between voltage controlled bus 1 and voltage controlled bus 2. For this reason, a convergence map showing the converging and non-converging regions is constructed that compares these two voltage controlled busses. These results indicate

that for the IEEE 14-Bus system the existence of distinguishable features that can be used for discriminate classification of the two classes.

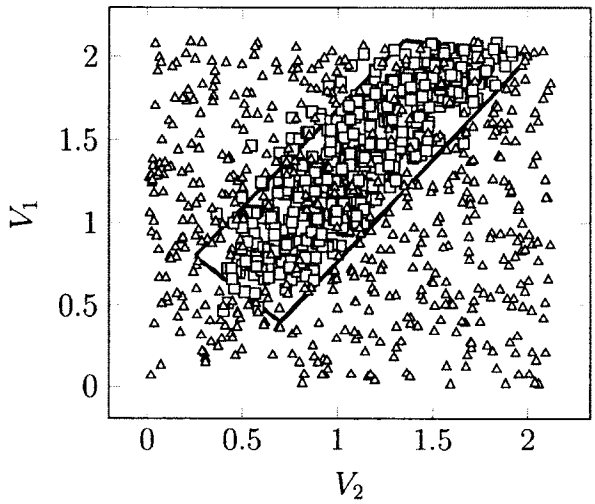

Figure 6.2: 14-Bus Convergence Map for Controlled Voltages Bus 1 and 2

6.3 Dimensional Transformation

The feature extraction process described in the previous section is binary in nature and examines a multivariate dataset to train discriminate classifiers to predict convergence. One benefit of initially starting with the classification of convergence is it is a subset of the entire feature allowing for faster computation time. The convergence classifier examines reported power system state variables in its original coordinate system. However, by transforming the data in such a way that corresponds to the variances in the dataset, new information can be revealed and therefore new features extracted. The transformation utilized to transform each power system instance into a new dimensional space is called principal component analysis (PCA). The features extracted during this process are used in the instance classifier for the detection of cyber-events.

The mathematical derivation and approach of applying PCA to power system state variables is described in Chapter 4, Section 4.4. This section summarizes the dimensional transformation results of the 5-Bus and IEEE 14-Bus power systems. For both topologies, the transformation is performed when line flows, injected powers, are not being considered, and when they are being considered. The exact state variables used for each case are described in next subsection. Afterwards, the results of the transformation for all four cases are summarized here while the raw results of transforming 500 power system instances are shown in Appendix C.

6.3.1 State Variables Retained for Transformation

Shown in Tables 6.3 through 6.6 are the state variables retained for analysis for the four cases considered. For the 5-Bus power system, two cases are considered with Table 6.3 listing the exact state variables used in the case of the first transformation. Here a total of 23 variables are retained for analysis. The second stage adds to this with the addition of the state variables listed in Table 6.4. Using the notation developed in Chapter 5 Section 5.2 the state variables listed in Table 6.4 show the injected powers of the 5-Bus power system. These additional features are added to the 23 stated in the previous case for a total of 47 state variables retained for analysis.

Table 6.3: 5-Bus State Parameters Without Line Flows

Variable(s)	Details
V_1, V_2, V_3, V_4, V_5	Bus i Voltage
$\theta_2, \theta_3, \theta_4, \theta_5$	Bus i Angles
PG_1, PG_3	Bus 1 and 3 Real Power Generated
QG_1, QG_3	Bus 1 and 3 Reactive Power Generated
$PL_1, PL_2, PL_3, PL_4, PL_5$	Bus i Real Power Load
$QL_1, QL_2, QL_3, QL_4, QL_5$	Bus i Reactive Power Load

Table 6.4: 5-Bus Power Line Flow Variables

Line #	Bus i to Bus j	$P_{i,j}$	$Q_{i,j}$	$P_{j,i}$	$Q_{j,i}$
1	1 - 2	P1-2	Q1-2	P2-1	Q2-1
2	2 - 5	P2-5	Q2-5	P5-2	Q5-2
3	2 - 3	P2-3	Q2-3	P3-2	Q3-2
4	3 - 4	P3-4	Q3-4	P4-3	Q4-3
5	3 - 5	P3-5	Q3-5	P5-3	Q5-3
6	4 - 5	P4-5	Q4-5	P5-4	Q5-4

Tables 6.5 and 6.6 describe the state variables used for each of the two cases for the larger IEEE 14-Bus power system. For the case where the lines, injected power, are not being considered, there are a total of 52 variables, each of which are described in Table 6.5. This includes the voltages, angles, powers generated, and powers consumed at each bus. For the IEEE 14-Bus case where the power through the lines are being considered, a total of 134 state variables are retained for the transformation. The exact variables added to those shown in Table 6.5 are shown in Table 6.6. These variables adhere to the notation developed perviously in Chapter 5, Section 5.2.

Table 6.5: IEEE 14-Bus State Parameters Without Line Flows

Variable(s)	Details
$V_1, \ldots, V_{14}$	Bus i Voltage
$\theta_2, \ldots, \theta_{14}$	Bus i Angles
PG_1, PG_2	Bus 1 and 2 Real Power Generated
QG_1, QG_2	Bus 1 and 2 Reactive Power Generated
QG_3, QG_6, QG_9	Bus 3, 6 and 9 Reactive Capacitance Supplied
$PL_2, \ldots, PL_6, PL_9, \ldots, PL_{14}$	Bus i Real Power Load
$QL_2, \ldots, QL_6, Q_9, \ldots, QL_{14}$	Bus i Reactive Power Load

Table 6.6: IEEE 14-Bus Power Line Flow Variables

Line #	Bus i to Bus j	$\mathbf{P}_{i,j}$	$\mathbf{Q}_{i,j}$	$\mathbf{P}_{j,i}$	$\mathbf{Q}_{j,i}$
1	1 - 2	P1-2	Q1-2	P2-1	Q2-1
2	1 - 5	P1-5	Q1-5	P5-1	Q5-1
3	2 - 3	P2-3	Q2-3	P2-3	Q2-3
4	2 - 4	P2-4	Q2-4	P4-2	Q4-2
5	2 - 5	P2-5	Q2-5	P5-2	Q5-2
6	3 - 4	P3-4	Q3-4	P4-3	Q4-3
7	4 - 5	P4-5	Q4-5	P5-4	Q5-4
8	4 - 7	P4-7	Q4-7	P7-4	Q7-4
9	4 - 9	P4-9	Q4-9	P9-4	Q9-4
10	5 - 6	P5-6	Q5-6	P6-5	Q6-5
11	6 - 11	P6-11	Q6-11	P11-6	Q11-6
12	6 - 12	P6-12	Q6-12	P12-6	Q12-6
13	6 - 13	P6-13	Q6-13	P13-6	Q13-6
14	7 - 8	P7-8	Q7-8	P8-7	Q8-7
15	7 - 9	P7-9	Q7-9	P9-7	Q9-7
16	9 - 10	P9-10	Q9-10	P10-9	Q10-9
17	9 - 14	P9-14	Q9-14	P14-9	Q14-9
18	10 - 11	P10-11	Q10-11	P11-10	Q11-10
19	12 - 13	P12-13	Q12-13	P13-12	Q13-12
20	13 - 14	P13-14	Q13-14	P14-13	Q14-13

6.3.2 Transformation Results

Using the state variables described in the previous subsection, PCA was used to transform each power system instance into the new dimensional space. The information extracted in this new dimensional space is used by the instance classifier to detect the presence of a cyber-event. For each of the four cases considered, there is a mXn data matrix $\mathbf{X}_{System}$ that is transformed to the new dimensional space. The number of rows m of $\mathbf{X}_{System}$ denotes the number of power system instances retained for transformation, while the number of columns n denotes the number of features retained. For each of the four cases considered, the size of $\mathbf{X}_{System}$ is stated in Table 6.7.

Furthermore, each column of $\mathbf{X}_{System}$ is assigned sequential to the features presented in the Tables described in the previous section.

Table 6.7: Data Matrix Sizes for Each of the Four Considered Cases

Case	m	n
5-Bus Without Injected Powers	500	23
5-Bus With Injected Powers	500	47
14-Bus Without Injected Powers	500	52
14-Bus With Injected Powers	500	134

As stated in Chapter 4, Section 4.4.1, the transformation offered by PCA is defined by the variances in the original dataset $\mathbf{X}_{System}$. The variances are used to construct each principal component with the first accounting for most of the variance in the data matrix $\mathbf{X}_{System}$. Figure 6.3 provides an example of this in the form of a scree plot where the variances accounted for by the first ten principal components are listed. This figure displays the transformation results for the 5-Bus power system when the injected powers or lines are being considered. As shown in the figure, the first principal component accounted for 35% of the variance with all ten accounting for over 90% of the variance. For completeness, the scree plots for each consideration is shown in Figures C.1, C.5, C.9, and C.13.

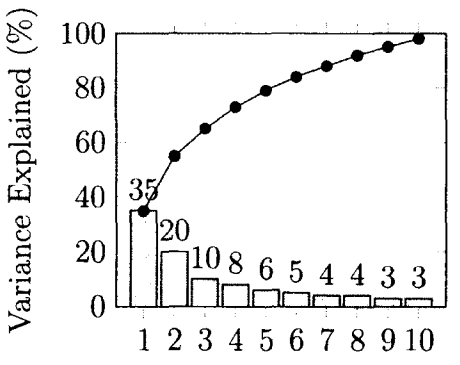

Figure 6.3: PCA Scree Plot for 5-Bus System With Lines

A summary of the percent variances accounted for by the first 10 principal components for each of the considerations is shown below in Figure 6.4. This figure reveals that the ability to preserve the variances in the first 10 components decrease when changing from a small topology, 5-Bus, to a larger topology, the IEEE 14-Bus. However, this may not be universally true. Such an analysis is currently out of the scope of the dissertation. Furthermore, for both system topologies the percent variance accounted for by the first 10 components increases when the injected powers (with) are included. For example, for the 14-Bus system the variance accounted for jumps from 66.4% to 81.5% when lines are considered. This may be contributed to the fact that the larger the system the more information is required for the extraction of correlations.

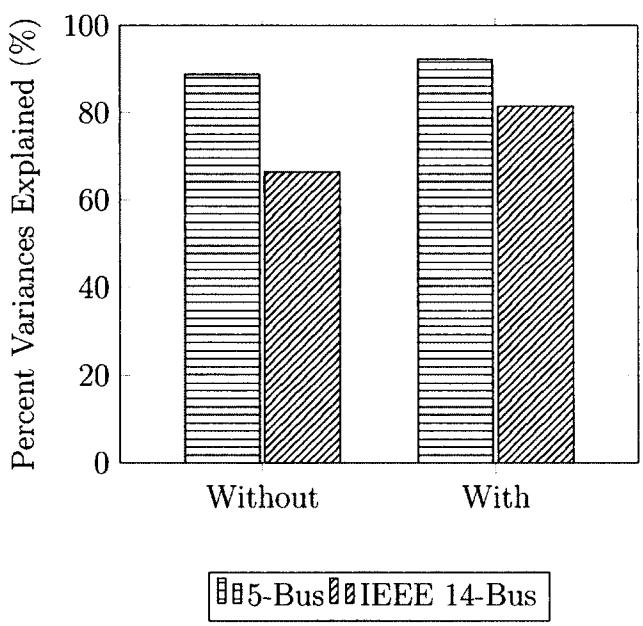

Figure 6.4: Percent Variances Accounted for by the First 10 Components of Each Transformation

With the state variable defined for each of the four cases, the power system instances can be mapped to the new dimensional space accordingly. The training models used for the development of the detection scheme are based on the power system state variables listed. By transforming them into a new dimensional space where redundancy is reduced, comparisons can be made offering substantial insight into normal operation of the power system topology under analysis. An example of the transformation is shown in Figure 6.5 where each power system instance is plotted as a single point according to the first two principal components for the 5-Bus power system when lines are not being considered.

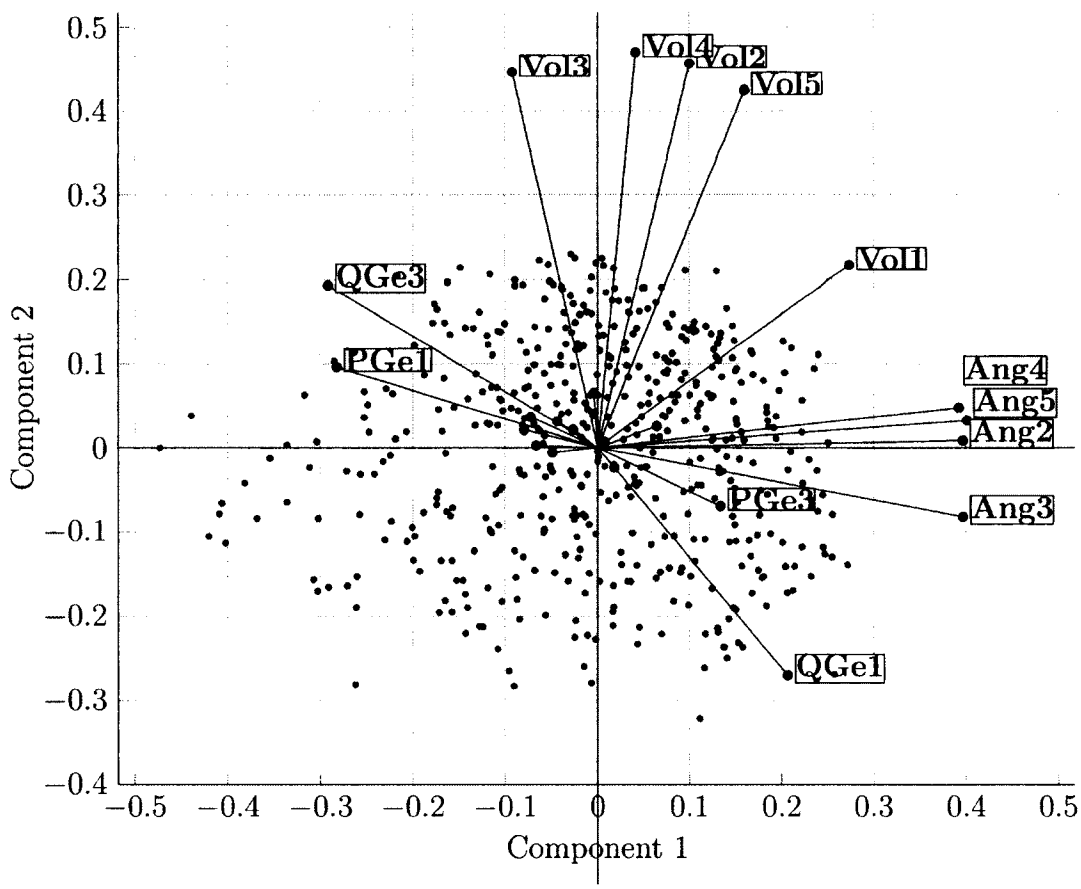

Figure 6.5: Scores and Feature Vectors Transformed 5-Bus Without Line Flows

Figure 6.5 represents 500 transformed power system instances for the 5-Bus system when the lines are not taken into consideration. As shown in the Figure 6.5, the 23 variables explained in Table 6.3 are mapped to the new space as vector projections forming individual vectors for each column in data matrix $\mathbf{X}_{5Bus}$. By close examination of the vector projections, Figure 6.5 reveals that the voltage angles contribute mostly to the first component while four of the five bus voltage magnitudes contribute mostly to the second component. Interestingly, the voltage magnitude at the slack bus, bus 1, contributes more to the first component then compared to its contribution to the second component. The plotted transformation results for each consideration are shown in Figures C.2, C.6, C.10, and C.14 in Appendix C.

Hotelling $\mathbf{T^2}$ Results

Continuing with using the 5-Bus power system as an example for this discussion, Figures 6.6 and 6.7, reveals the multivariate distance of each power system instance plotted in Figure 6.5. The first Figure shows the Hotelling's T^2 value for each of the 500 power system instances. This distance describes the distance to the origin or center cluster of the points in the new space. The greater this distance, the less the power system instance conforms to the patterns found in $\mathbf{X}_{5Bus}$. For this case, it was found that $max(T^2) = 107$ while the mean $\bar{T}^2 = 107$. The second figure, Figure 6.7, shows a Rayleigh distribution fitted to the Hotelling's T^2 values of the example case. This figure shows a statistical distribution of the values with 99% of the power system instances occurring below $T^2 = 80$.

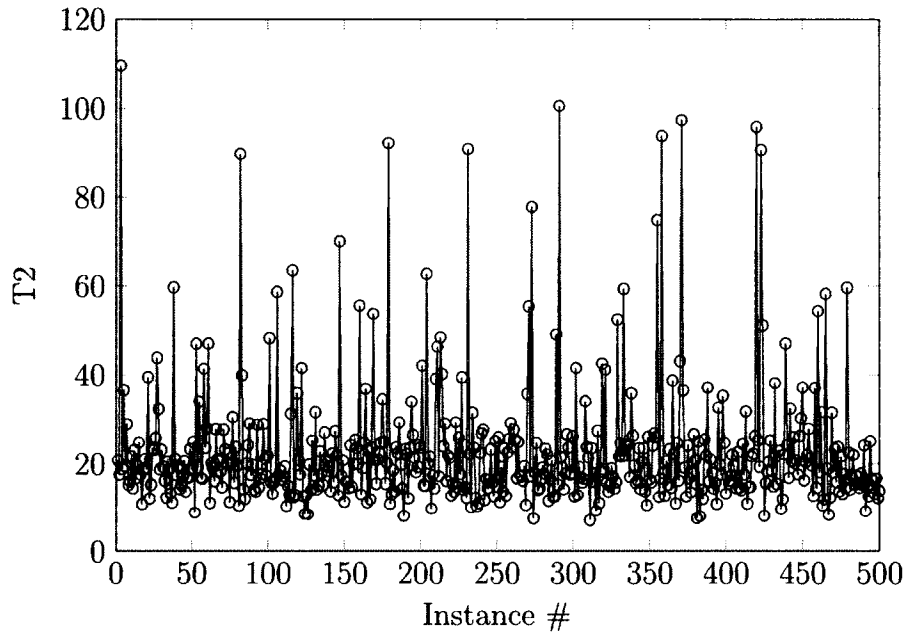

Figure 6.6: Hotelling T^2 of 500 5-Bus Instances Without Line Flows

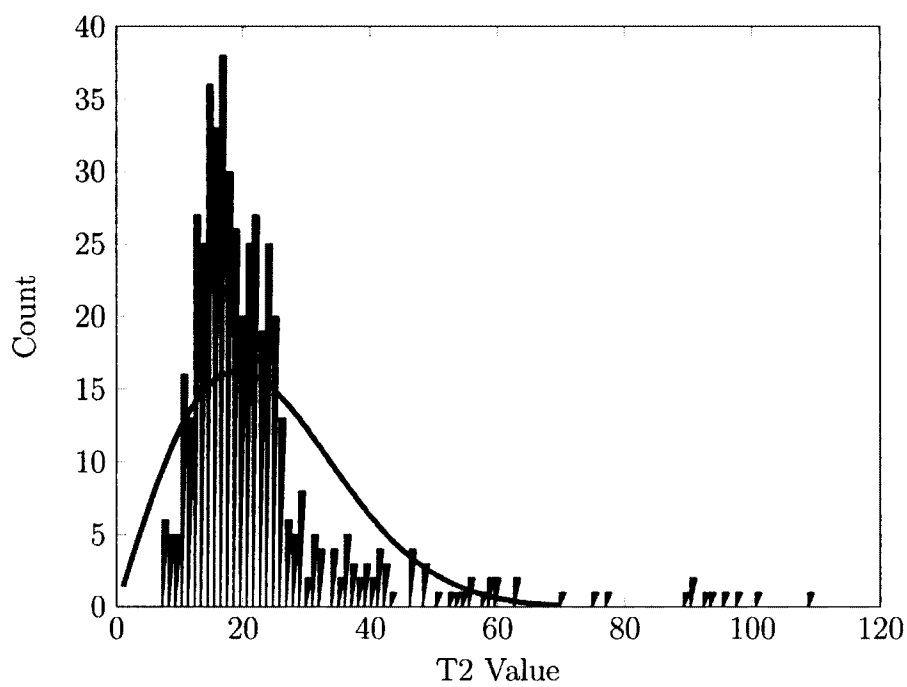

Figure 6.7: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows

The two plots described here were also created for each of the considered cases. Figures C.3, C.7 , C.11, and C.15 show the exact Hotelling's T^2 values while the histogram and fitted Rayleigh distributions are shown in Figures C.4, C.16, C.12, and C.16. For a comparative analysis, Table 6.8 summarizes the results shown in these figures. Based on the results presented in Table 6.8, the statistics of the Hotelling's T^2 values increase as the number of features are retained across each of the two considered power system topologies.

Table 6.8: Hotelling T^2 Statistics for Each of the Four Considered Cases

Case	**Max(T^2)**	**Mean μ**
5-Bus Without Injected Powers	109.7	22.5
5-Bus With Injected Powers	205.7	46.9
14-Bus Without Injected Powers	310.7	54.9
14-Bus With Injected Powers	395.5	137.4

The transformation features extracted, specifically the Hotelling's T^2 values allow for the development of a trusted model for each of the four considerations. These values then can be compared to newly observed power system instances for the classification into either a normal or suspect set. Furthermore, outliers in the trusted model were removed by calculating the T^2 value of each instance. An outlier is considered to exists if its value is more than three standard deviations away from the mean [85]. Outliers are removed in all four considerations of the two power system topologies. This is made possible given that extreme state parameter values in a live power system are prevented provided an adequate power system protection scheme. The resulting data matrix X is what is used as the trusted model for the remainder of the analysis. The exact Hotelling's T^2 threshold values are described in Chapter 7.

6.4 Univariate Statistics

Used for localization, the univariate statistics offers an understanding on the range of possible values for each power system state variable. This information is used to perform the Grubs' test to find the variable or variables that are compromised. Potential features are extracted from this information and are in the context of the Grubs' test formulated for this application in Section 4.5.1. In order to use the Grubbs test for localization, the sample mean $\bar{Y}$ had to be predetermined. By examining the change in $\bar{Y}$ over the change in training set size n, $\frac{\delta \bar{Y}_i}{\delta n}$, the preferred training set size was also determined. The size n was used when $\frac{\delta \bar{Y}_i}{\delta n} \approx 0$. The training size n for all state variables for each topology, the 5-Bus and IEEE 14-Bus, had to be calculated. The results of this are provided in the following two sections.

6.4.1 5-Bus

Instead of providing plots for $\bar{Y}$ for each variable of the 5-Bus system, only the voltage plots are provided in Figure 6.8. A summary of the determined sample size n where $\frac{\delta \bar{Y}_i}{\delta n} \approx 0$ for each of the 5-Bus state variables are provided in Table 6.9. For the purpose of coding, a stopping point of 0.00001 was used to determine the $\bar{Y}_i$ and n. These results provide the numerical value that is used in the Grubbs Test to localize the source of the cyber-event. By examining Figure 6.8, it was determined that the voltage averages appear to stabilize for values after $n = 200$ with only slight differences found. Similar observations for the other state variables were found to exist. Table 6.9 shows that for the 5-Bus case all averages were found to level off by $n = 1500$. Most of the variables were found to level off for $n < 500$.

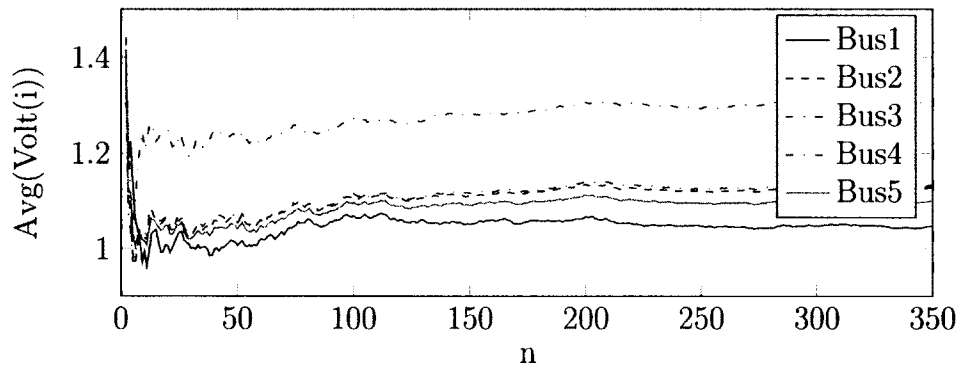

Figure 6.8: 5-Bus Average Voltages for Grubbs Test 'n' Selection

Table 6.9: 5-Bus Grubbs Test Parameters

Variable	n	Mean $\bar{Y}$	Variable	n	Mean $\bar{Y}$
1	293	1.051	25	434	-0.8570
2	208	1.134	26	220	0.71863
3	470	1.311	27	593	0.58711
4	385	1.130	28	666	-0.4464
5	202	1.113	29	303	-0.3921
6	57	-0.1285	30	440	-0.2466
7	46	-0.0912	31	83	0.40346
8	213	-0.1928	32	357	0.26391
9	53	-0.1207	33	164	0.88382
10	390	2.419	34	478	0.36981
11	366	2.034	35	250	-0.2199
12	1188	-0.5759	36	681	1.035
13	1429	4.739	37	377	0.8812
14	468	0.6291	38	230	-0.3243
15	377	1.073	39	850	2.174
16	201	0.6378	40	222	-1.4210
17	363	0.6353	41	227	-0.4612
18	781	0.8223	42	377	-0.9921
19	386	0.2961	43	289	0.6351
20	141	0.6319	44	265	-0.1836
21	188	0.4021	45	919	-0.3916
22	246	0.2937	46	273	1.397
23	97	0.4079	47	359	0.2902
24	410	-0.6228			

6.4.2 IEEE 14-Bus

Similar to the 5-Bus case, instead of providing plots for $\bar{Y}$ for each variable of the IEEE 14-Bus power system, only the voltage plots are provided in Figure 6.9. Also, a summary of the determined sample sizes n are provided in Tables 6.10 and 6.11. A stopping point of 0.00001 was also used to determine the $\bar{Y}_i$ and n. It was determined that the voltage averages appear to stabilize for values after $n = 150$ with only slight diviations found. All of the state variables analyzed were found to level off for $n < 500$.

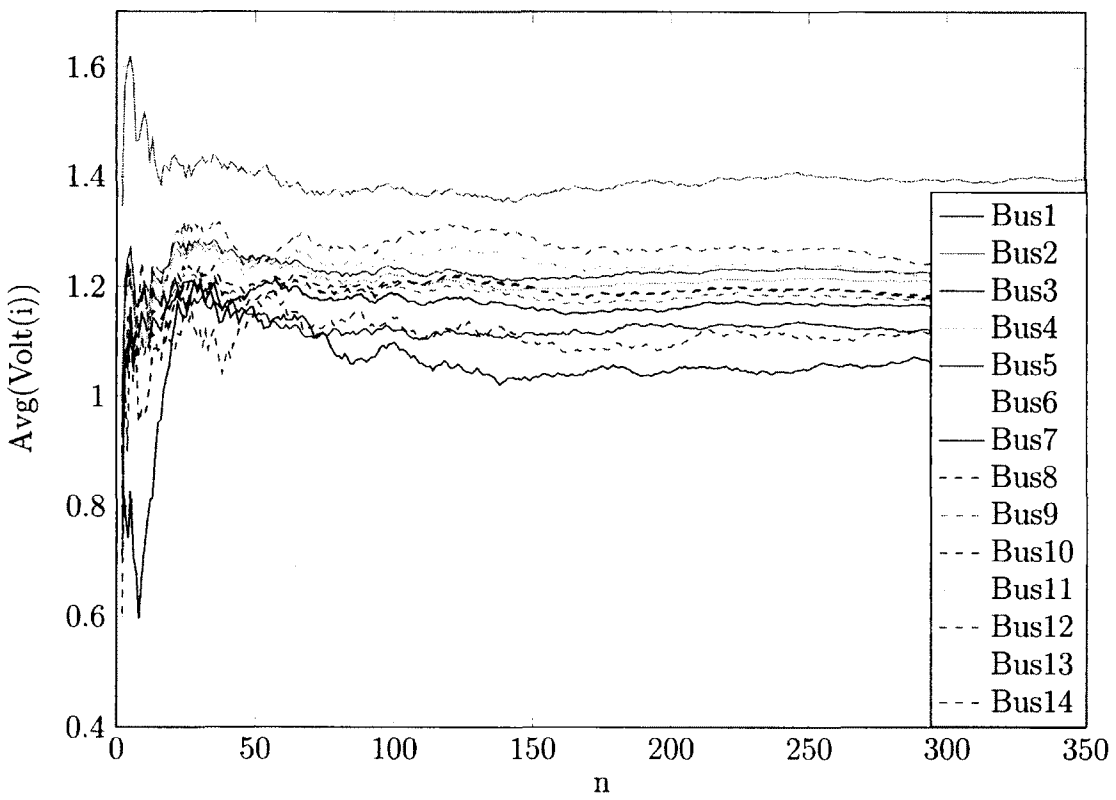

Figure 6.9: IEEE 14-Bus Average Voltages for Grubbs Test 'n' Selection

Table 6.10: IEEE 14-Bus Grubbs Test Parameters for Variables 1-68

Variable	n	Mean $\bar{Y}$	Variables	n	Mean $\bar{Y}$
1	239	1.128	35	162	0.23
2	232	1.3993	36	200	0.8606
3	560	1.0647	37	106	0.4952
4	299	1.2099	38	164	0.0721
5	263	1.2294	39	135	0.1093
6	194	1.2891	40	240	0.2861
7	572	1.1604	41	69	0.0893
8	308	1.1118	42	61	0.0361
9	614	1.174	43	86	0.0601
10	384	1.1802	44	274	0.1400
11	187	1.235	45	175	0.1433
12	470	1.2478	46	128	0.1337
13	176	1.2586	47	224	0.1897
14	109	1.2068	48	46	-0.037
15	229	-0.182	49	35	0.0139
16	208	-0.312	50	78	0.0737
17	98	-0.258	51	219	0.1662
18	213	-0.246	52	56	0.0555
19	154	-0.353	53	31	0.0171
20	125	-0.318	54	60	0.0169
21	125	-0.318	55	104	0.0584
22	327	-0.342	56	134	0.0471
23	304	-0.352	57	398	-1.572
24	100	-0.347	58	247	-0.950
25	79	-0.358	59	878	2.5586
26	344	-0.368	60	524	-0.697
27	340	-0.428	61	369	-0.807
28	577	3.5907	62	245	-0.630
29	76	1.7773	63	342	1.3644
30	1334	-5.916	64	466	0.6552
31	1384	14.368	65	339	1.0128
32	174	0.2563	66	227	-0.181
33	16	0.0126	67	246	0.8723
34	96	0.0192	68	287	-0.300

Table 6.11: IEEE 14-Bus Grubbs Test Parameters for Variables 69-136

Variable	n	Mean $\bar{Y}$	Variable	n	Mean $\bar{Y}$
69	265	-0.164	103	1033	2.9684
70	89	1.0412	104	767	0.7958
71	214	0.7876	105	537	1.6455
72	279	-0.813	106	1284	0.4551
73	283	-0.618	107	104	0.2756
74	283	0.6184	108	716	-0.026
75	148	-0.133	109	178	-0.001
76	60	-0.104	110	161	-0.371
77	177	-0.232	111	229	1.6143
78	287	0.3003	112	354	-0.194
79	2	-1.283	113	492	0.9477
80	287	-0.300	114	1372	-0.136
81	2	1.5266	115	730	-0.427
82	265	0.1648	116	252	-0.086
83	287	0.3004	117	139	-0.346
84	364	-0.055	118	585	0.3748
85	212	-0.067	119	611	0.8482
86	82	0.0747	120	345	0.1097
87	315	0.0762	121	480	-0.055
88	401	0.1701	122	66	0.0939
89	302	-0.028	123	817	-0.018
90	81	0.1088	124	112	0.3009
91	89	-0.041	125	325	0.1517
92	152	0.2524	126	254	-0.184
93	89	0.0444	127	757	0.4157
94	302	-0.071	128	458	0.5109
95	261	0.1025	129	742	-0.302
96	292	0.1162	130	345	0.0874
97	2174	8.3377	131	132	-0.077
98	255	0.9015	132	283	0.3257
99	276	-5.458	133	132	0.0804
100	564	-0.101	134	163	-0.245
101	1011	-1.035	135	699	-0.113
102	245	-1.124	136	319	0.2941

6.5 Conclusions

This chapter outlined the several feature extraction methods that are utilized in the cyber-event detection scheme developed and tested by this dissertation. Features extracted included convergence, dimensional transformation, and univariate statistics. By first performing the feature extraction approaches outlined in this chapter, it was realized that a detection framework could be created that looked at the date in a reduced and concise manner. The feature extraction techniques were performed for both power system topologies, and for the instance classifier ad analysis on the two different conditions was also performed. This included transforming each power system's data matrix into the new space when the injected powers are and are not being considered. The last feature retained for analysis was the univariate statistics of each state parameters for each power system topology. This information is retained for the purpose of localizing the source of the cyber-event via the Grubbs Test.

CHAPTER 7

SELECTION OF CLASSIFIER PARAMETERS

7.1 Introduction

In an effort to develop an efficient detection scheme with high true positive rates and low false negative rates, certain classifier parameters had to be selected. This chapter describes the analysis and selection of these parameters for both the convergence and instance classifier. Parameters selected includes the sampling training size n and other various statistical parameters. Recall that according to Chapter 4, the objective of the convergence classifier is to place a subset of the power system variables on to one of two classes. The first class is the converging or non-malicious set and the second class is the non-converging or malicious class. For the convergence classifier, variations include: training size n and type of discriminant classifier.

The second classifier, the instance classifier, collectively examines all the variables of a power system instance. These power system instances are then transformed to a new dimensional space where a multivariate distance, the Hotelling's T^2 value, is calculated for each one. Based on these values, it can be determined if a new incoming instances fits with the trusted model as described in Chapter 4, Section 4.4.

7.2 Convergence Classifier

Using a subset, X_{System}^{inputs}, of state variables, the convergence classifier seeks to determine whether or not a set of power system state variable will converge to a feasible set of power flow values. Recall as described in Chapter 4, Section 4.3.1, a total of four discriminant analysis classifiers are considered as possible classifiers. These four include linear, diagonal linear, quadratic, and diagonal quadratic. Evaluation of these four discriminant analysis classifiers is based on varying the training size n along with setting a probability of 0.5 for each converging and non-converging training sets since that there are only two sets. Furthermore, to increase the robustness of the selection criterion a k-fold cross validation of $k = 10$ is used for each training size n.

7.2.1 5-Bus

Using the notation developed earlier in Chapter 4, the power system instance input subset X_{system}^{inputs} for the 5-Bus power system contained a total of 13 power system state variables, $size[X_{5bus}^{inputs}] = 13$. Figures 7.1 and 7.2 outline the results of analyzing the varying training size n for the four discriminant classifiers. As shown in Figure 7.1, the quadratic classifier outperformed the three others with a true positive classification rate on average of 91% for various sizes n. The misclassified data shown in Figure 7.2 accounts for the sum of the false negative and false positive results combined. The objective of this particular analysis is to determine for what value n produced the lowest misclassification rate. As shown in the figure, the lowest for all three classifiers occurred for $n = 3000$.

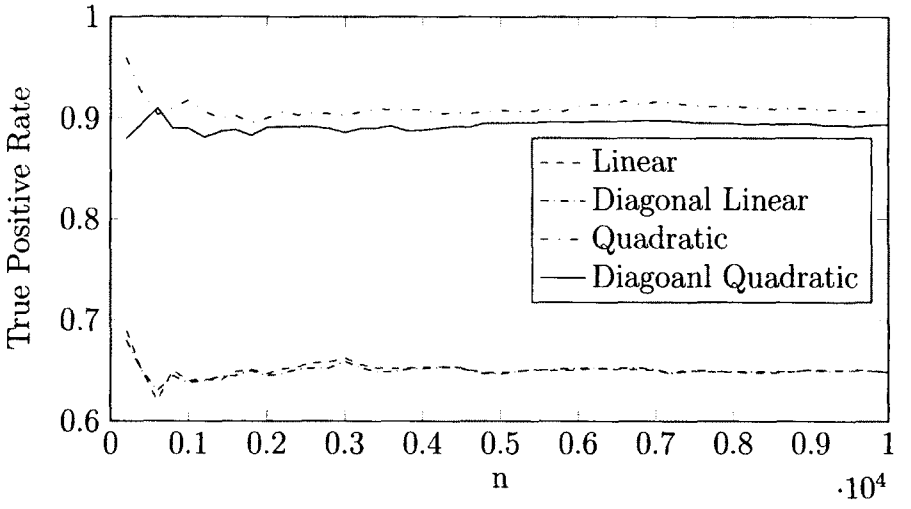

Figure 7.1: 5-Bus Convergence Discriminant Classifier Comparison

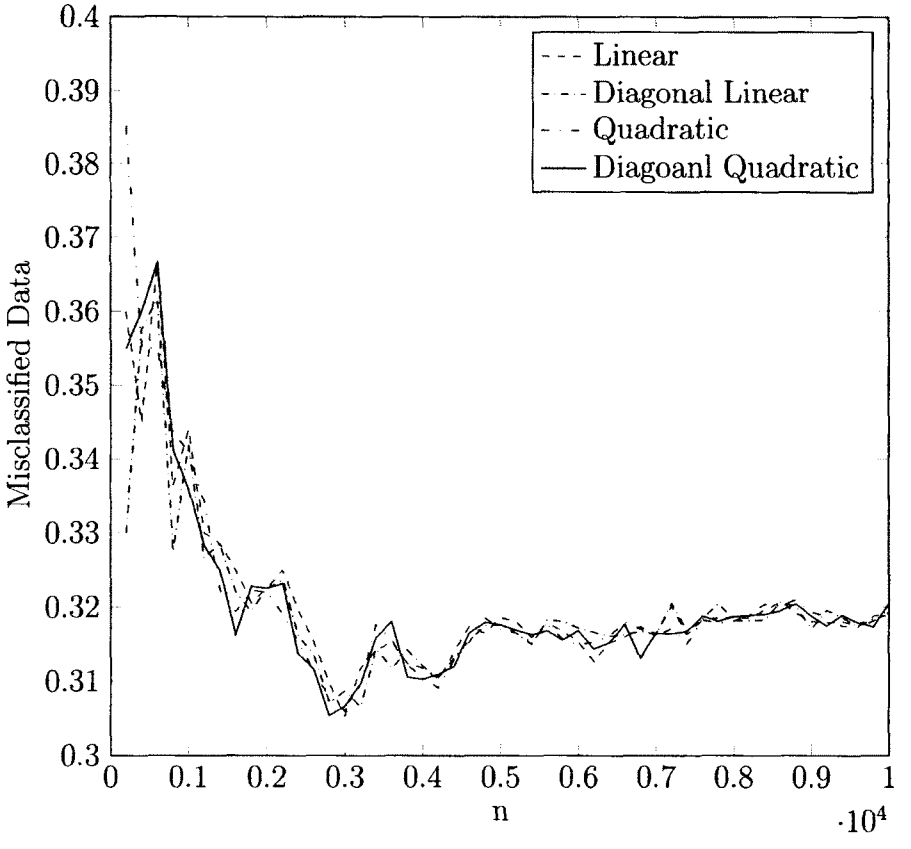

Figure 7.2: 5-Bus Convergence Discriminant Classifier Misclassification Rate

7.2.2 IEEE 14-Bus

Keeping to the notation, the instance input subset $X_{inputs}^{system}(i)$ for the IEEE 14-Bus power system contained a total of 31 power system state variables, $size[X_{inputs}^{5bus}(i)] = 31$. Using the same analysis process used to determined parameters for the 5-Bus system, the results of the 14-Bus system are show in Figures 7.3 and 7.4. Results are quite similar and as revealed in Figure 7.3, the discriminate classifier that outperformed the others was the quadratic classifier. True positive classification for the quadratic classifier averaged at 85% for varying size n.

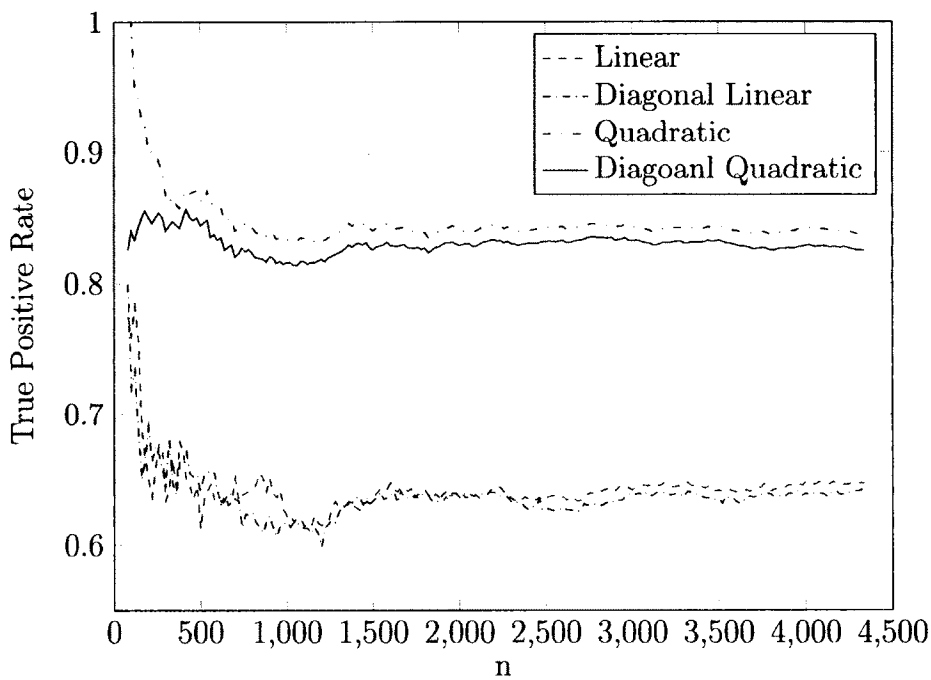

Figure 7.3: IEEE 14-Bus Convergence Discriminant Classifier Comparison

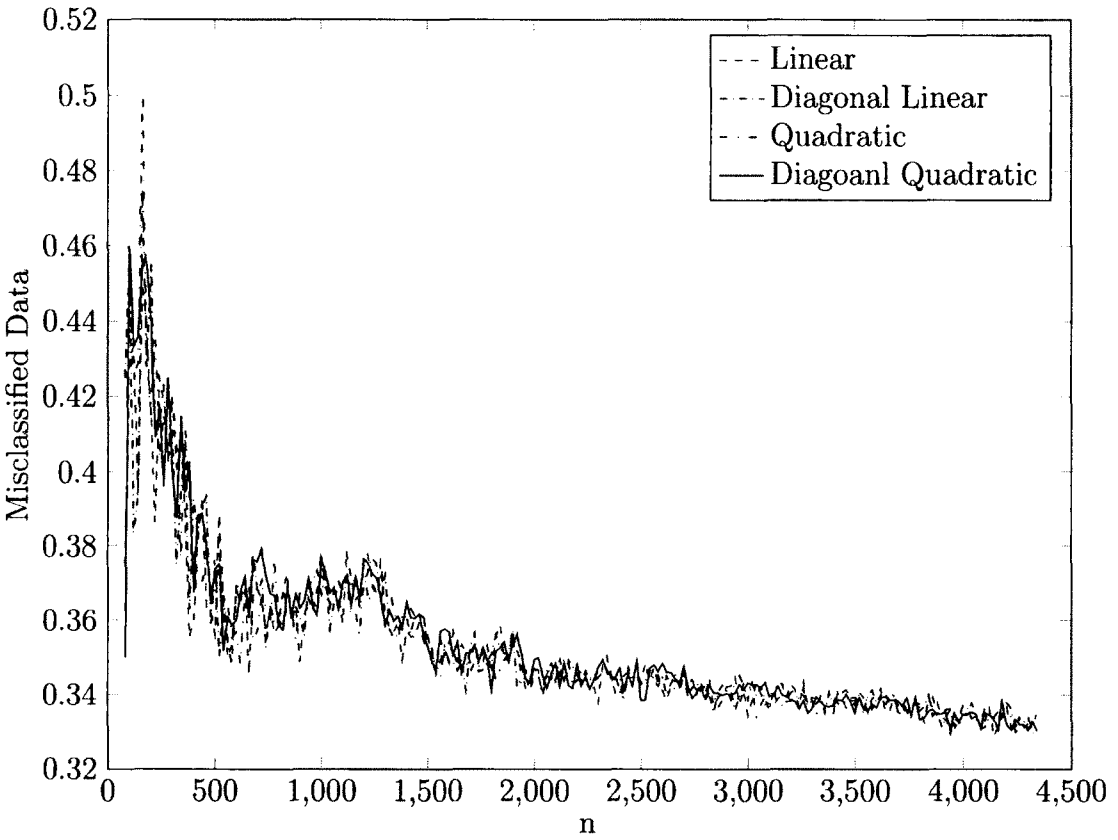

Figure 7.4: IEEE 14-Bus Convergence Discriminant Classifier Misclassification Rate

For the misclassification of data, it appears that by examining Figure 7.4 there is a steady decrease as an increase of n is made. Therefore, for any selected size above $n = 3000$ not much difference will be observed for the misclassification rate.

7.2.3 Classifier Parameters Selected

Based on the analysis performed in the previous subsection, the parameters summarized in Table 7.1 reveal the parameters selected for the convergence classifier. These parameters are used in the convergence stage classifier of the developed detection scheme whose results are shown in Chapter 8. Furthermore, it is mentioned in the future work, Chapter 12, that modifications of these parameters may lead to higher

true positive and lower false positive classification results. In order to assess the scalability of the developed cyber-event detection approach, it is desired to keep the parameters for the two power system topologies as close together as possible. The results performed in this section reveal that this is indeed possible.

Table 7.1: Selected Convergence Classifier Parameters for Each Topology

System	Classifier Type	Training Size n
5-Bus	Quadratic	3,000
IEEE 14-Bus	Quadratic	3,000

7.3 Instance Classifier

The instance classifier is based on the transformation given by PCA into a new dimensional space. Recall that each power system instance once in this new space has an associated multivariate distance, Hotelling's T^2 value, to the origin. This distance is what the instance base classifier uses to determine if a cyber-event exists in a new observation of the power system under analysis. This section uses the transformation results of Section 6.3.2 to determine the threshold values for each of the power system cases under consideration. Recall that a total of four cases are considered, two for each system topology. For each topology, the two cases included when the injected are being considered and when they are not being considered. The resulting T^2 threshold values for each consideration are shown in Table 7.2 and are based on the 90% quintile of the trusted models' Hotelling's T^2 values.

As shown in Table 7.2, results indicate that the threshold distances increase when more variables are added for a given system topology. Using the 5-Bus power

system as an example, the consideration without injected powers has a $T^2_{Thr} = 37.2$, and when injected powers are considered, the threshold value more than doubles to $T^2_{Thr} = 86.2$. These observations correspond to the fact that more variables are contributing to the principal components in the new dimensional space. For each case considered, these values list the value utilized for instance based classification. If a newly observed power system instance is plotted in the new space and is found to have a Hotelling's T^2 value greater than the threshold values, $T^2 > T^2_{Thr}$, then that instance is considered to contain a cyber-event. The results of the instance classifier using these threshold values are presented in Chapter 8.

Table 7.2: Selected Instance Classifier Hotelling T2

System Topology	**Hoteling T^2 Threshold Value T^2_{Thre}**
5-Bus Without Injected Powers	37.2
5-Bus With Injected Powers	86.2
14-Bus Without Injected Powers	84.9
14-Bus With Injected Powers	229

7.4 Conclusions

This chapter outlined the steps and values taken to determine the parameters for both the convergence and instance classifiers. Based on the convergence classification results, the classifier that has the highest success is the quadratic discriminant classifier. The quadratic classifier produced an average true positive rate of 92% for the 5-Bus system and 85% for the 14-Bus system with a training size $n \geq 1000$. The parameter associated with the instance classifier includes the Hotelling's T^2 value.

CHAPTER 8

CYBER-EVENT IDENTIFICATION RESULTS

8.1 Introduction

With classifiers and respected parameters selected, full simulation of the detection framework described in Chapter 4 can be performed. This chapter analyzes the results of the cyber-event identification. Recall that according to the approach, Figure 4.2, cyber-event identification can occur at either the convergence stage classifier or the instance stage classifier. Both identification classifiers are designed to identify the presence of a cyber-event at which point localization is then performed. Localization is considered the identification of the the origin of the cyber-event and can only take place once a power system instance has been identified as containing a cyber-event. The localization results for the cyber-events identified here in this chapter are presented in Chapter 9. The relationship between the classifiers and the localization stage of the detection framework is presented in Figure 8.1. If the convergence classifier is not able to detect the presence of a cyber-event, the observed state variables are passed to the instance classifier where a more extensive analysis is performed via the dimensional transformation. Only upon event identification is localization performed.

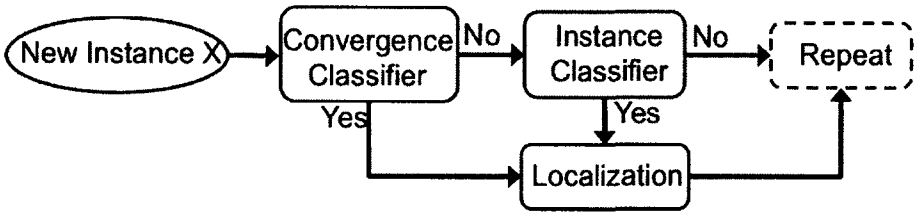

Figure 8.1: Cyber-Event Identification Approach

For each power system topology, a total of ten sets of analysis are performed and include the simulation of the different attacks under different conditions. Recall that the details of the simulated attack types are described in Chapter 5, Section 5.4, and that each are formed from a randomly selected trusted power system instance. The two main simulation categories shown above include the system when the injected powers are and are not being considered. As discussed in Chapter 5, injected powers describe the real and reactive powers traveling through the transmission lines. The ten sets utilized for each power system topology include:

1. The Power System Without Line Flows
   (a) Single variate Type I Attack (SI)
   (b) Single variate Type II Attack (SII)
   (c) Multivariate Type I Attack (MI)
   (d) Multivariate Type II Attack (MII)
   (e) False Positive Analysis
2. The Power System With Line Flows
   (a) Single variate Type I Attack (SI)
   (b) Single variate Type II Attack (SII)
   (c) Multivariate Type I Attack (MI)

(d) Multivariate Type II Attack (MII)

(e) False Positive Analysis.

The raw identification results of the two classifiers are shown in Appendix D and are presented here in a consolidated manner in order to make direct comparisons across each simulated condition. These consolidated results include the false positive and true positive cyber-event classification of power system instances for the 5-Bus and IEEE 14-Bus power systems. An example of the raw identification results is presented in Figure 8.2 and Table 8.1. These results are for the 5-Bus power system when the injected powers or lines are not being considered.

Figure 8.2 shows the classification results for each power system state variable. In this figure, the total number of attacks simulated are provided by the "cyber-event count" curve. These results indicate that the instance based or PCA classifier returned the highest true positive classification counts. Furthermore, upon close inspection of Figure 8.2, it is revealed that every attack performed on the two voltage controlled buses where detected by the convergence classifier. In addition to the TP results presented for each consideration, a false positive (FP) analysis is performed with the results presented in the next Section. The benefit of such an exhaustive analysis permits the determination of the required conditions that lead to the most optimal conditions for increased true positive classification while decreasing the false positive classification.

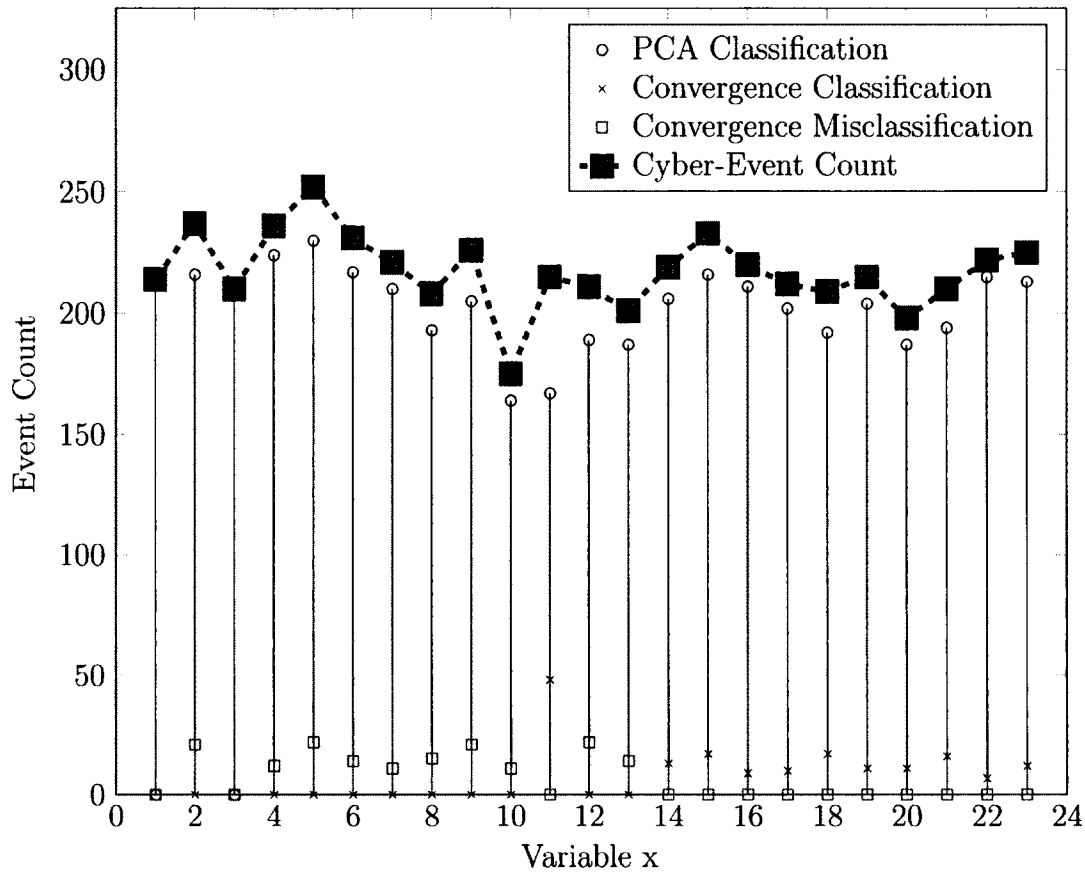

Figure 8.2: 5-Bus Without Line Flows SI Classification Results

Table 8.1: 5-Bus Without Line Flows SI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
163	595	0	4242
Total Number of Simulated Malicious Instances = 5,000			
Total Number of Simulated Cyber-Events = 5,000			

8.2 False Positive Analysis

The false positive results for the two classifiers are presented in Figure 8.3 and were performed by selecting random instances from the trusted models and placing

them through the developed detection scheme. The selection of a random instance from the trusted model provides a form of cross validation and determines how the developed cyber-event detection scheme performs when no event is present. This process was performed for both power systems and for each case where line flows are included and where line flows are not included. Therefore, a total of eight bar graphs are shown in the figure. This information is also presented in Table 8.2 and includes the percent that returned false positive. A total of 20,000 power system instances were randomly selected and ran through the developed detection scheme.

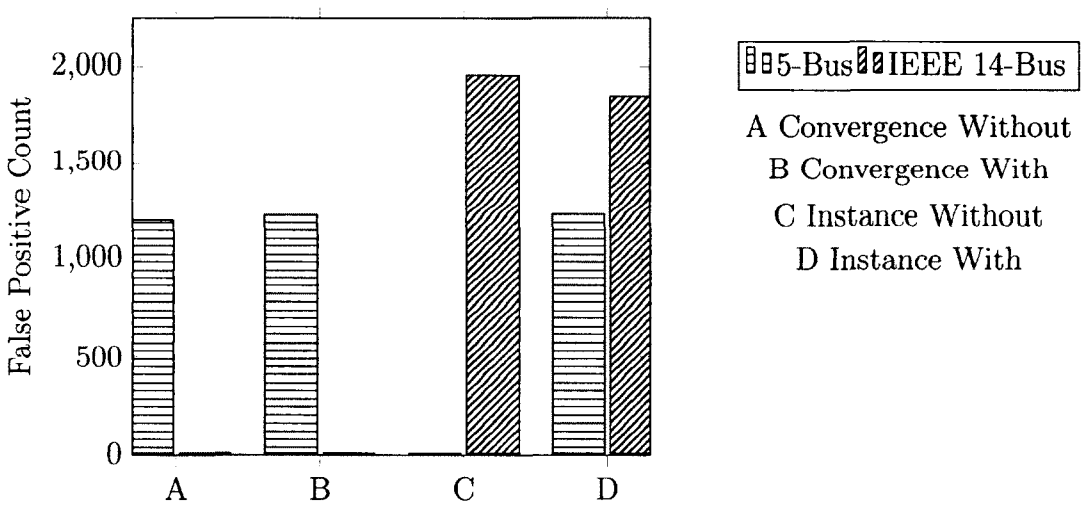

Figure 8.3: False Positive Classification

Table 8.2: Detection Scheme False Positive Results

			5-Bus		14-Bus	
Classifier Stage	**Without Lines**	**With Lines**	**FP Count**	**% FP**	**FP Count**	**% FP**
Convergence	X		1205	6.03	0	0
Convergence		X	1226	6.13	0	0
Instance	X		0	0	1961	9.81
Instance		X	1229	5.65	1849	9.25

The results indicated by Figure 8.3 and Table 8.2 show that the False Positive rate for increases for the instance based classifier when an increase in the size of the topology is made. This perhaps is in part due to the number of contributing projections provided by the covariance matrix of PCA. An increase in the number of features transformed by PCA lessens the contribution of that feature to the new dimensional space. Therefore, state variable attacks that slightly deviate about the trusted mean are less likely to be detected for bigger systems.

Chapter 12, Section 12.2.2 proposes a few modifications that may make it possible to lower this FP rate when an increase in size is made for a given system topology. Another interesting and less understood observation is the exact cause of the zero FP count for the convergence classifier for the 14-Bus system. Combining all the results, the developed cyber-event detection scheme falsely identified 4.67% of the 160,000 trusted power system instances tested. Furthermore, it is suspected that with the additions and parameter adjustments proposed in Chapter 12, this number could be decreased to about 1%, if not lower. Parameters adjustments may include varying the parameters outlined in Chapter 7 for each system consideration.

8.3 5-Bus Identification

This section outlines the results of the developed cyber-event detection when tested using the 5-Bus power system. Results described include the overall true positive (TP) classification along with detailed examinations into the performance of the convergence and instance classification stages. Raw results of the detection scheme for the 5-Bus power system are presented in Appendix D, Section D.1. Furthermore,

a false negative (FN) analysis was performed in a manner similar to the TP analysis. These results are included in the last subsection of this section and offer a great deal of insight into what types of events and conditions the developed detection scheme failed to successfully classify a cyber-event.

8.3.1 True Positive Analysis

For the five bus system, the true positive count is the total number of times that a cyber-event was successfully recognized. Successful classification can occur at either the convergence stage or the instance stage. The results of the true positive classification are presented in Section D.1 and include the cases where injected powers are and are not being considered. By combining the results, the developed detection scheme successfully identified a total of 163,511 out of the 175,000 simulated malicious power system instances. This corresponds to an overall true positive classification of 93.4% for the 5-Bus power system. These results are broken down for each attack and for each classifier in Figure 8.4 and Table 8.3.

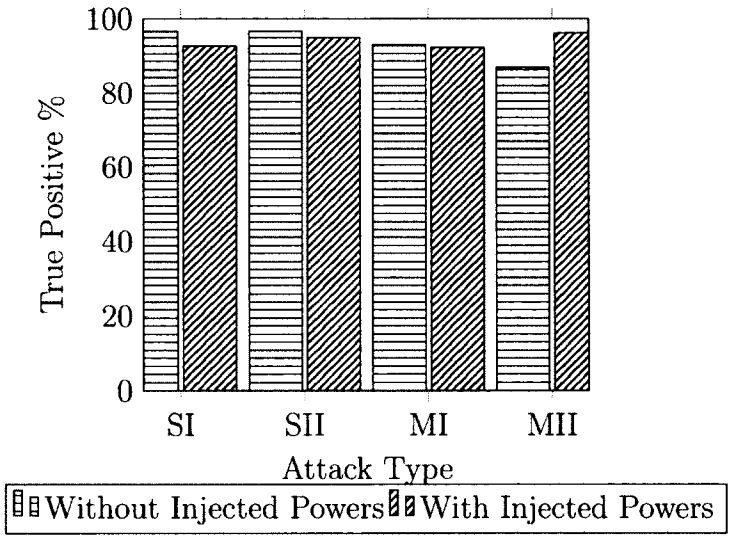

Figure 8.4: 5-Bus Overall True Positive Results for Each Attack Type

Table 8.3: Detection Scheme True Positive Results

			5-Bus		
Classifier Stage	**Without Lines**	**With Lines**	**TP Count**	**Total Events**	**% TP**
Convergence	X		12,450	55,000	22.6
Convergence		X	15,546	120,000	13.0
Instance	X		38,069	55,000	69.2
Instance		X	97,446	120,000	81.2

While the developed detection scheme was able to identify in all cases over 85% of the simulated events, evidence would suggest a preference for the condition where the injected powers are not taken into consideration. As shown in Figure 8.4, for three out of the four attack types, true positive classification was higher in the case where the powers were not taken into consideration. For the MII attack, the case where the injected powers are considered, resulted in a higher TP rate than the case without. Recall that this attack was constructed by changing two power system state variables to a value other than zero. For the MII attack type, the case where powers are being considered the scheme successfully classified 96.3% while the case without classified only 86.9%. Similarly, results are also observed in trying to access which classifier functions best under which conditions. These results are shown in Table 8.3.

The results presented in Table 8.3 show that with including the injected powers the instance stage classifier successfully classified a higher percentage of the simulated cyber-events. A total of 81.2% were successfully identified while for the case without the power injected the instance classifier successfully classified only 69.2% of the instances. It is expected that this is the result that the injected powers offer more correlated features for the detection of the inconsistencies brought forth by the state

variable attacks. These and other observations of the results of the two classifiers are discussed in the following two subsections. Recall that if the convergence classifier does not classify the cyber-event the power system state variables are then analyzed via the instance classifier. This means that for the case where the lines are being considered, 13% of the simulated events were detected by the convergence classifier while 81.2% were classified using the instance classifier for a total TP classification of 94.2%. Therefore, it should be noted as shown in Table 8.3 that low convergence TP percentages does not necessarily mean low TP percentages for the developed cyber-event detection framework.

8.3.2 Convergence Classification

This subsection discusses the results of the convergence classifier for the 5-Bus system looking at specifically which state variables had the most success when it comes to true positive classification. Only a subset of the total power system state variables are considered at this stage of the detection scheme and therefore only those state variables will be analyzed. For the 5-Bus power system there are a total of 13 state variables that are used by the convergence classifier. These are stated in Chapter 6, Section 6.2.1 and include a subset of the system voltages, powers generated, and powers consumed. The overall TP count for the convergence classifier for each type of attack is presented in Figure 8.5.

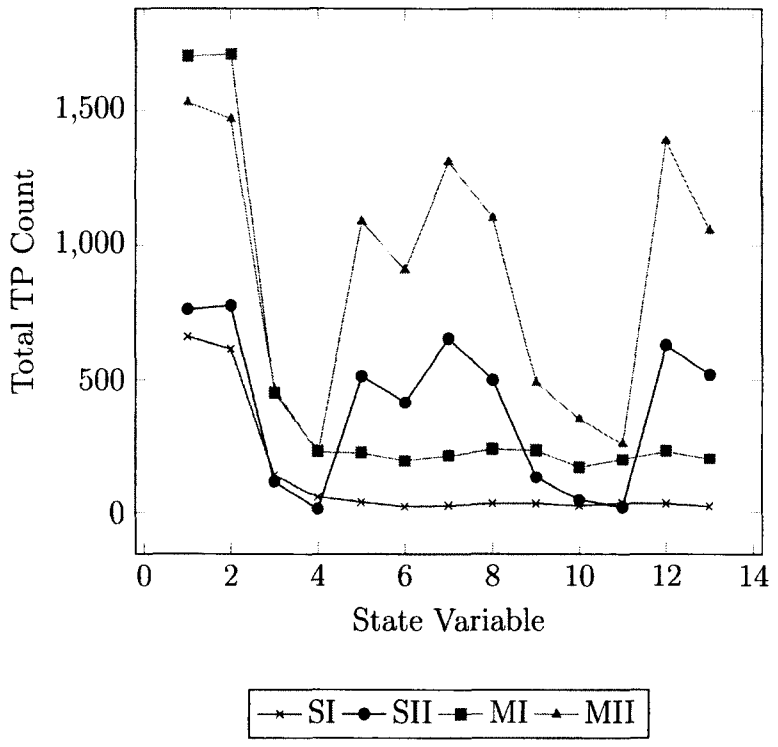

Figure 8.5: 5-Bus Overall True Positive Convergence Classifier Results

As shown in Figure 8.5, there are several dips in the classification count of the convergence classifier. These dips appear to occur at the convergence state variables c_4, the real power being consumed at Bus 1, and c_{11}, the reactive power being consumed at Bus 3. Furthermore, these dips are more pronounced for the type II events. As stated in Section 5.4, a type II event is one where the state variable is changed to a value other than zero. The increase in count value of the single variate (S) to multivariate (M) makes sense as there are more attacks occurring. Interestingly, however, the pattern of the results is maintained when going from the S attack count to the M attack count. These results indicate cyber-event occurring at convergence state variables c_1 and c_{11},

and all four attack types have a low probability of being detected by the developed detection scheme.

For the attack type I there is a steady decrease in the TP count from c_1 to c_4, and remains steady though c_{13}. Converging state variables c_4 and c_{13} correspond to the real and reactive loads at each of the five buses. These low counts for these values correspond to the fact that the per unit values of the loads are approximately zero, making it harder to distinguish these types of attacks.

8.3.3 Instance Classification

Instance classification describes the classification based on the PCA transformation described in Chapter 4, Section 4.2. The instance classifier transforms the power system into a new dimensionally space where redundancy is reduced at which point the classifier then classifies according to a trusted model. The TP percentage for each of the four attack types are presented in Figure 8.6. For comparison, the two conditions, with injected powers and without injected powers, are plotted.

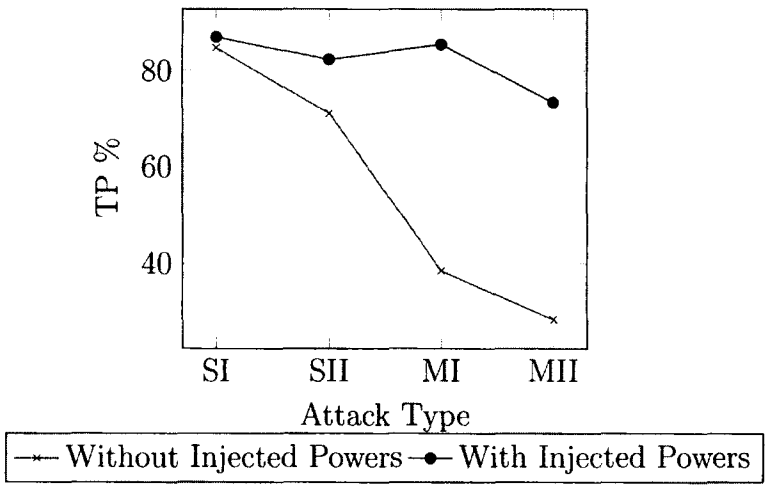

Figure 8.6: 5-Bus Overall True Positive Instance Classifier Results

Examination of Figure 8.6, reveals that for the instance classifier, the retention of the injected powers in the calculation produces higher TP classification. A trend is also noted that as the attack types become more sophisticated, the TP percentage also decreases. This is more profound for the case where the injected powers are not taken into consideration. For this case, for the MII attack, the TP percentage drops below half as compared to the SI attack. The decreasing trend is believed to be related to the fact that more instances are being flagged as suspect by the convergence classifier. This would cause the instance classifier to decrease in its classification as compared to the overall count of the total number of simulated power system instances.

Another analysis approach is to plot the instance detection against all state variables of the 5-Bus power system. This is shown in Figures 8.7 and 8.8, revealing which attacks on which variables have the highest likelihood of being detected by the instance classifier. The case where the injected powers are not being considered are presented in Figure 8.7, while the results for the case where they are being considered is presented in Figure 8.8.

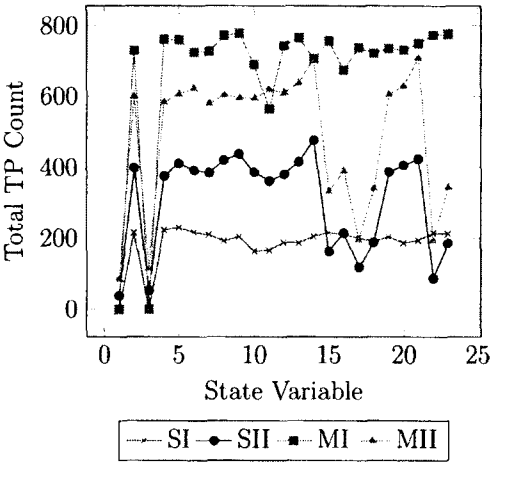

Figure 8.7: 5-Bus Overall True Positive Instance Classifier Results, Without Injected Powers

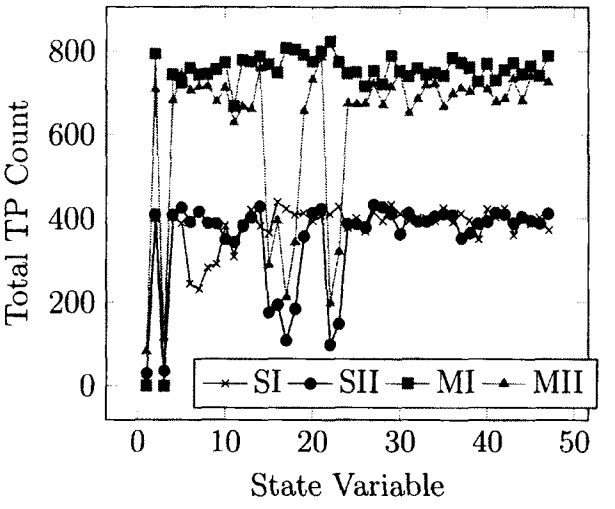

Figure 8.8: 5-Bus Overall True Positive Instance Classifier Results, With Injected Powers

Interestingly, for both topological considerations, the MI attack type has the highest instance based classification. Furthermore, upon inspection of Figure 8.8, it is revealed that the TP count remains relatively constant for state variables $x_{24} - x_{37}$. These variables correspond to the injected powers in each bus and are described in Table 6.6. Furthermore, the figures reveal that on average the attack type SI was the hardest to identify by the instance classifier. Lastly there are noticeable dips in the TP counts for attack types SII and MII. Both are attacks where the values are altered to a value other than zero.

8.3.4 False Negative Analysis

The false negative (FN) analysis describes the events that were falsely classified as having no cyber-event. This was performed in a similar manner to the true positive analysis. For a power system instance to be placed in the non cyber-event class, it has

to be classified as such by both classifiers. Once the convergence classifier determines no cyber-event is present, the instance base classifier then proceeds to detect for the presence of a cyber-event. The results of the FN analysis are presented in Figure 8.9.

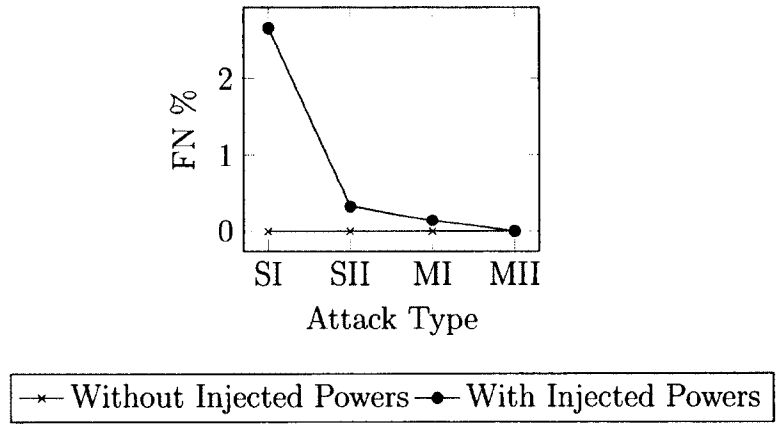

Figure 8.9: 5-Bus Overall False Negative Instance Classifier Results

The results shown in Figure 8.9 reveal that zero FN instances occurred for the case without injected powers while the case with never reached above 3% FN. Also, it is revealed that by increasing the complexity of the attack, this decreased the FN count down to zero for the most sophisticated attack simulated, the MII attack. It is also interesting to note which power system state variables when compromised produced the FN results. Given that the FN results indicate which variables are not detectable using the developed detection a much more extensive analysis of these results are presented in Chapter 10 Section 10.2.

8.4 IEEE 14-Bus Identification

Similar to the 5-Bus topology, two instances of the 14-Bus power system are considered for the developed detection scheme. The first is when the injected powers in the transmission lines are not being considered and the other case is when they are being considered. In both considerations, a total of four different attack types are considered along with a false positive (TP) and false negative (FN) analysis. Raw results of the convergence and instance classifiers for the IEEE 14-Bus power system are presented in Appendix D, Section D.2.

8.4.1 True Positive Analysis

The true positive classification results for the IEEE 14-Bus power system are presented in Section D.2 with the results summarized in Table 8.4 and Figure 8.10. Recall that successful classification or identification of the cyber-events can occur at either the convergence or instance classifiers. Combining the results across all eight considerations the developed cyber-event detection scheme accurately identified a total of 146,392 of the 160,000 simulated cyber events. This corresponds to a true positive classification rate of 91.5% for the 14-Bus system.

Table 8.4: Detection Scheme False Positive Results

			14-Bus		
Classifier Stage	**Without Lines**	**With Lines**	**TP Count**	**Total Events**	**% TP**
Convergence	X		10,659	80,000	13.3
Convergence		X	4,769	80,000	5.96
Instance	X		56,821	80,000	71.0
Instance		X	74,143	80,000	92.7

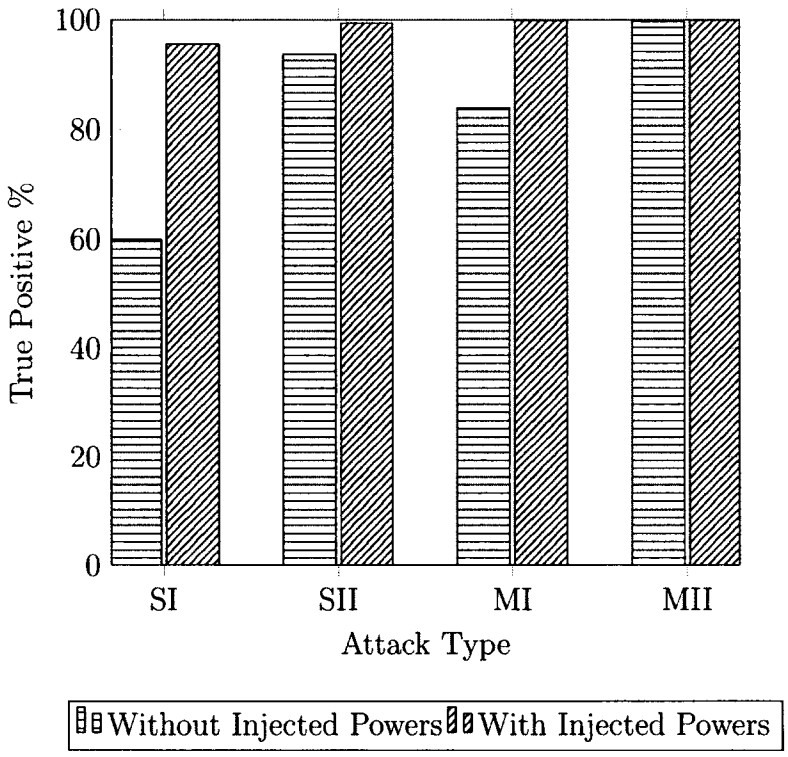

Figure 8.10: IEEE 14-Bus Overall True Positive Results for Each Attack Type

The lowest true positive classification occurred for the SI attack type when the injected powers are not being considered. Recall a SI attack type is one wherein the state variable is changed to zero. The TP classification of the SI attack type was 60% for the case without the injected powers while the TP rate when the injected powers are included was 95.5%. Furthermore, for all attack types the TP results increased when the injected powers are being considered. This is perhaps due to the fact that PCA has more correlated variables allowing for the detection of anomalies in the data.

To better understand the results in Figure 8.10, the TP results for each classifier under each consideration are presented in Table 8.4. The lowest TP count

was by the convergence classifier when the injected powers are considered. For this consideration, the convergence classifier was only able to determine 5.96% of the cyber-events simulated. One reason this could be so low is that most of the cyber-events simulated did not occur on the input subset, X_{14Bus}^{inputs}, making it impossible for the convergence classifier to classify. The highest classification TP count was by the instance classifier for the same consideration with a TP count of 92.7%. Recall that if not initially detected by the convergence classifier, the power system instance moves to the instance classifier for detection. This appears to play a part in the low TP count for the convergence classifier and a high TP count for the instance classifier. These and other performance observations of the two classifiers are described in the following two subsections.

8.4.2 Convergence Classification

This subsection discusses the performance results of the convergence classification for the IEEE 14-Bus power system by looking at which state variables had the most success when it comes to true positive classification. Recall that for the 14-Bus power system the total number of input or converging state parameters is $size(X_{14Bus}^{inputs}) = 31$. The exact state parameters included in this subset are stated in Chapter 6, Section 6.2.2 include a series of voltages, real and reactive power generated, and real and reactive powers consumed. The overall TP counts for the convergence classifier for each type of attack type are presented in Figure 8.11.

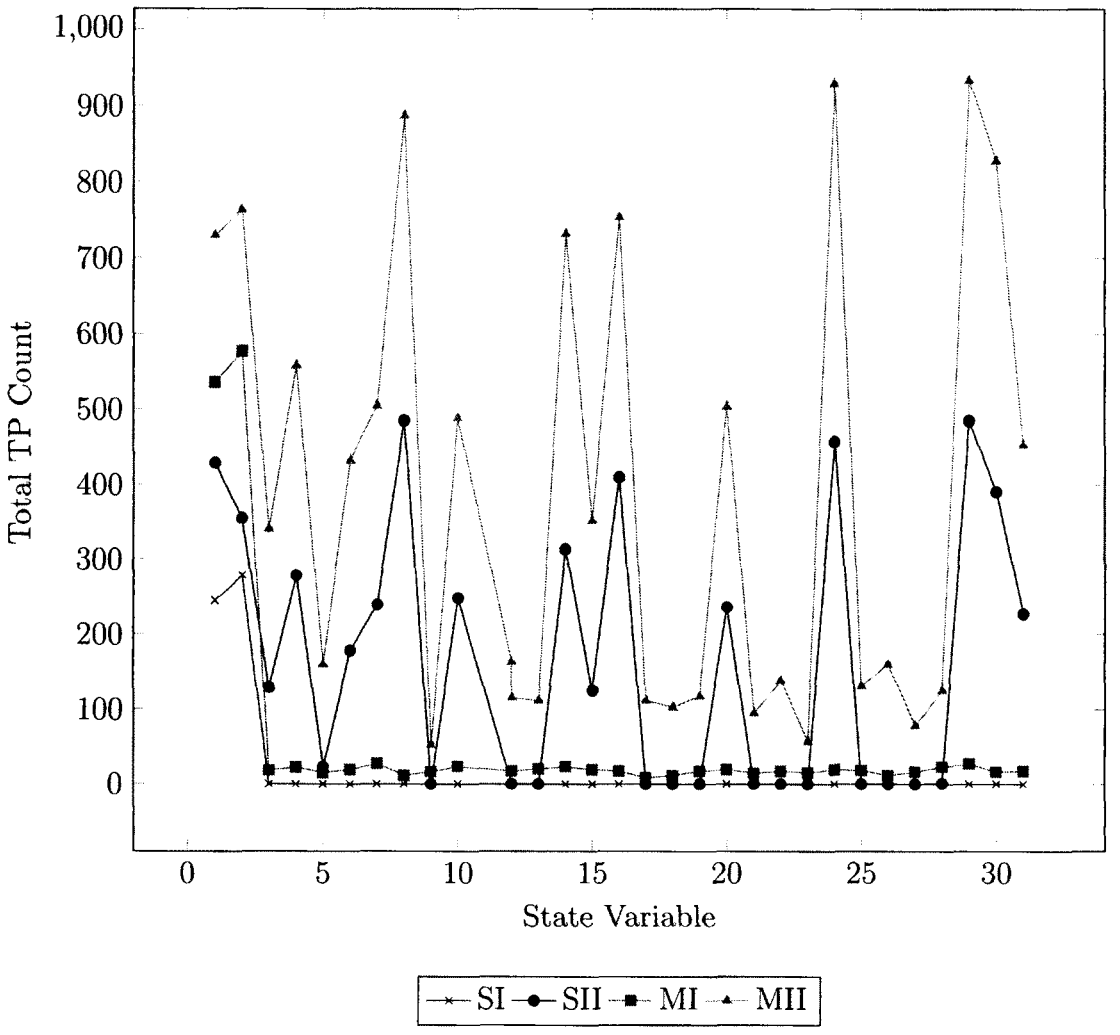

Figure 8.11: IEEE 14-Bus Overall True Positive Convergence Classifier Results

The results of the TP convergence count presented in Figure 8.11 are similar to those presented for the 5-Bus power system. A MII attack type was found to have the highest overall TP count. Recall for this type of attack two state variables are changed to a value other than zero. The attack type SII produced a slightly scaled down version of the MII attack type graph. Both attack types alter the state parameters to a value other than zeros with the only difference being one is a single (S) variate attack while the other is a multivaraite (M) attack. Interestingly the attack I type attacks follow

the similar scaled pattern with MI attack type possessing a higher classification count. These results indicate that attacks of type I, a changes to zero, are easier to detect for convergence state variables c_1 and c_2. These parameters correspond to the voltage readings at bus 1 and bus 2. For the attack type II, the highest TP counts occurred for converging variables c_1, c_2, c_8, c_{14}, c_{16}, c_{24}, c_{29}, and c_{30}. The exact state variables represented by these converging state parameters are shown in Table 8.5 along the with corresponding electrical descriptions.

Table 8.5: IEEE 14-Bus Converging State Variable Physical Representation

Converging State Variable	Instance State Variable	Variable Description
c_1	x_1	Voltage at Bus 1
c_2	x_2	Voltage at Bus 2
c_8	x_{33}	Reactive Power Generated Bus 6
c_{14}	x_{39}	Real Power Consumed Bus 6
c_{16}	x_{41}	Real Power Consumed Bus 10
c_{24}	x_{49}	Reactive Power Consumed Bus 5
c_{29}	x_{54}	Reactive Power Consumed Bus 12
c_{30}	x_{55}	Reactive Power Consumed Bus 13

8.4.3 Instance Classification

Instance classification is based on a dimensional transformation into a new space where comparisons can be made against a trusted model. The TP percentage for each of the four attack types are presented in Figure 8.12 for the case for the 14-Bus power system. For comparisons, the results for each of the two considerations, with injected powers and without injected powers, are plotted. Results presented in Figure 8.12 are consistent with those presented for the case of the 5-Bus topology. For the case where the injected powers are considered, the average TP percentage

is 92.7%, while for the case where injected powers are not considered, there was an average of TP classification percentage of 71.0%.

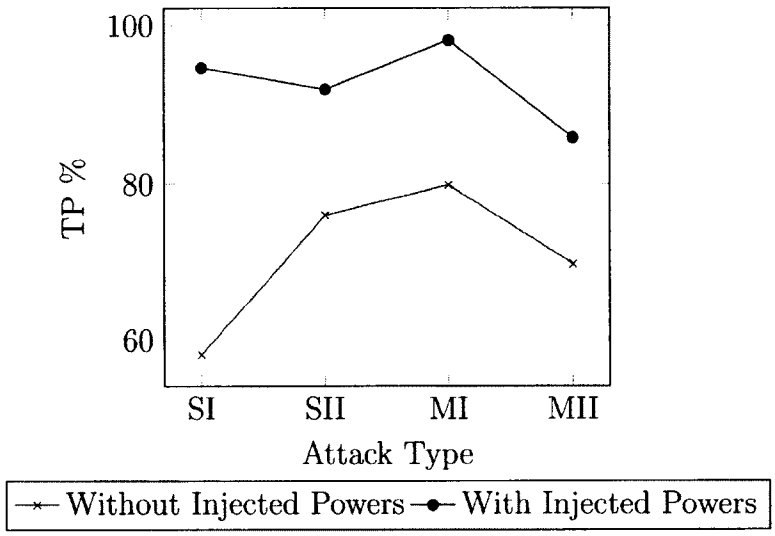

Figure 8.12: 14-Bus Overall True Positive Instance Classifier Results

In an attempt to determine which variables produced the highest instance classification, Figures 8.13 and 8.14 were constructed. This plot shows the TP count vs. power system state variables and is plotted for all four attack types simulated. Figure 8.13 reveals the results when the injected power are not being considered while Figure 8.14 presents the results for when they are being considered. By examining Figure 8.13, it is revealed that for the first 26 variables the MI attack type had the highest TP dropping below MII. The lowest was found to be the SI attack type which matches the previously stated results for this attack type.

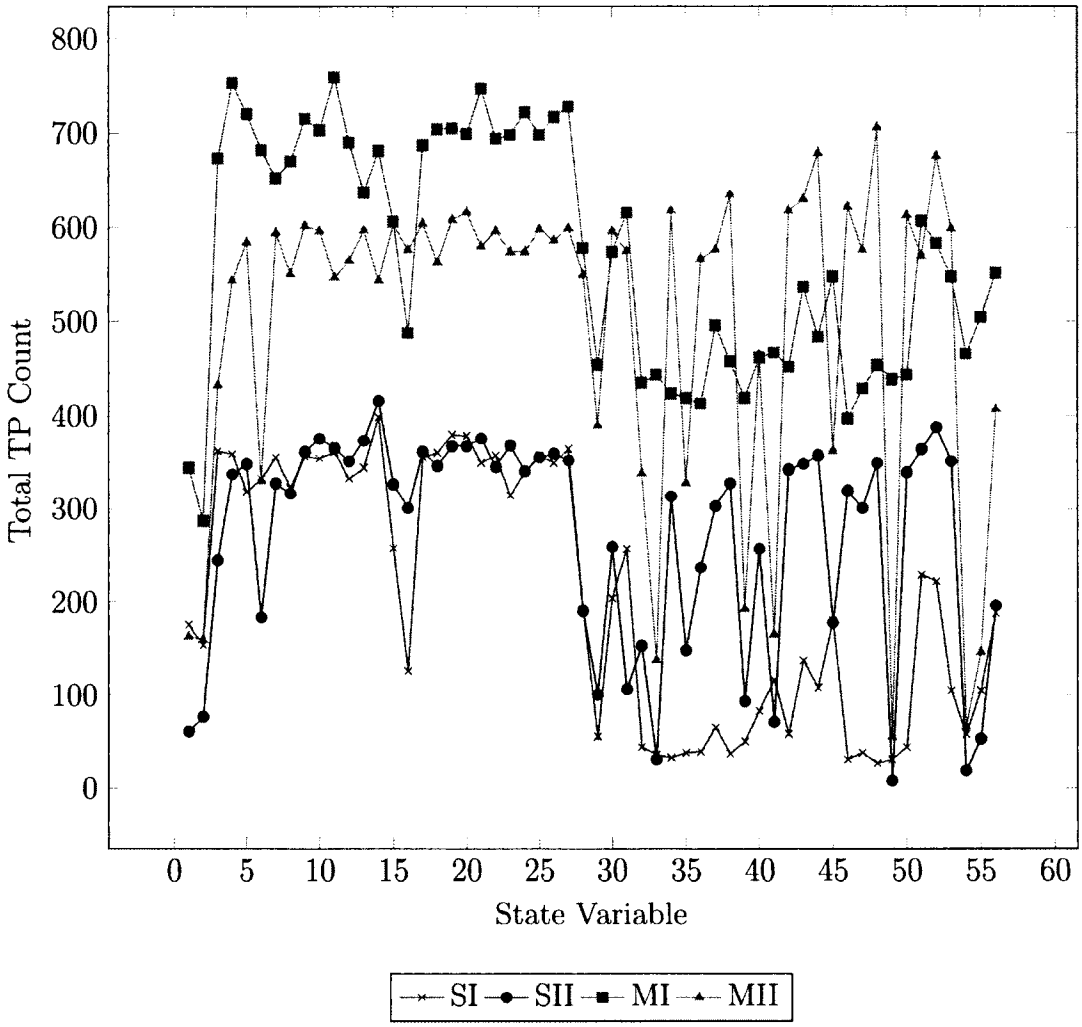

Figure 8.13: IEEE 14-Bus Overall True Positive Instance Classifier Results, Without Injected Powers

For the first 56 state variables, Figure 8.14 maintains similar plots to that of Figure 8.13, both of which have strong dips between variables $x_{29} - x_{56}$. These variables are outlined in Table 6.5 and correspond to the reactive power generated, real power consumed, and the reactive power consumed at each bus of the 14-Bus power system. From the state variables $x_{57} - x_{136}$, the TP count relatively stabilizes

with only slight fluctuations. These variables correspond to the injected powers of the system and are outlined in Table 6.6.

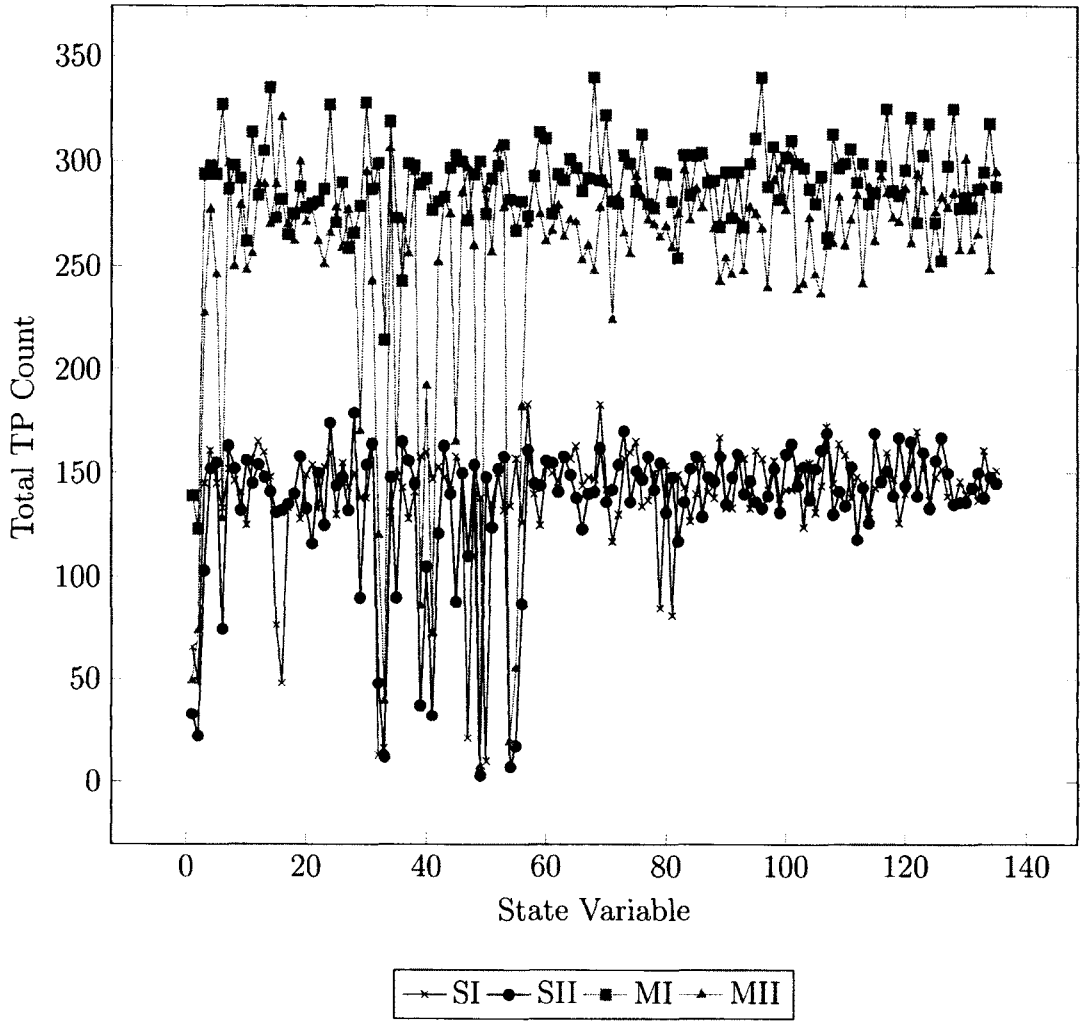

Figure 8.14: IEEE 14-Bus Overall True Positive Instance Classifier Results, With Injected Powers

8.4.4 False Negative

False negative (FN) classification is the classification of a cyber-event in a the non-malicious class. Recall that in order for this to happen, both the convergence

classifier and the instance based classifier have to label the power system instance inaccurately as not containing a cyber-event.

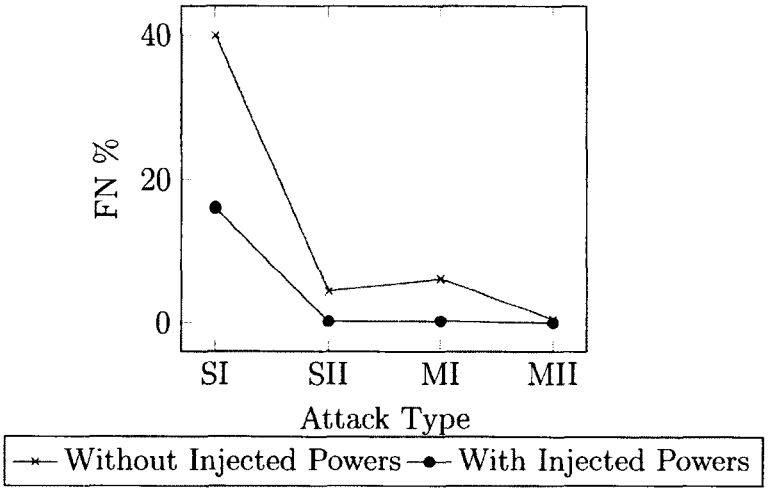

Figure 8.15: IEE 14-Bus Overall False Negative Instance Classifier Results

The results shown in Figure 8.15 reveal that for three out of the four simulated attack types produced a near zero FN percentage. Startling results indicated that for the SI attack type, the case where injected powers are not being considered produced a FN percentage of 40%. Not as high, but still alarming is the other case where injected powers are being considered, which produced a FN percentage of 16.1%.

8.5 Conclusions

The performance assessment of the identification classifiers resulted in a total true positive classification of 309,903 out of the total 335,000 simulated cyber-events. Results indicate that the developed detection scheme identified 92.5% of the simulated cyber-events. Identification could happen at either the convergence or instance classifiers at which point localization is then performed. Furthermore, the assessment

consisted of a total of four attack types being simulated with noticeable difference being observed in the developed detection scheme's ability to detect each type. By collectively examining the results the hardest event to detect is a SI type attack where only one state variable is changed to zero at a time.

CHAPTER 9

CYBER-EVENT SOURCE LOCALIZATION RESULTS

9.1 Introduction

Event localization is the identification of the exact source(s) of the cyber-event(s). In the developed cyber-event detection framework, source localization is only performed once the presence of a cyber-event has been identified. The exact mathematical derivation of the localization approach utilized is presented in Chapter 4, Section 4.5. This chapter outlines the localization results of the cyber-events simulated in the previous chapter. The output of the localization for the case of a single variate attack is the identification of the power system state variable that was the source of the attack. With this particular knowledge in a live implementation of the developed detection scheme, a power engineer or cyber security expert is able to go right to the source of the problem.

For this assessment, a false positive analysis is performed along with a true positive analysis of the localization results for each of the considered cases. Results are presented in a composite form allowing for direct comparisons across each considered power system topology. These composite results are derived from the results shown in Appendix E. Figure 9.1 serves as an example for the discussion outlining the raw results associated with localization. This figure displays the results for each of the 23

power system state variables when a SII attack is performed against the 5-Bus power system. The total number of events are shown in the "cyber-event count" plot. The state variable that produced the lowest localization results was found to be x_{13} with a localization count of 11% while the highest was found on state variable x_{19} with a localization count of 89%. Recall that according to Table 6.3 the electrical meaning of x_{13} describes the reactive power being generated at bus 3 while x_{19} represents the reactive power being consumed at bus 1.

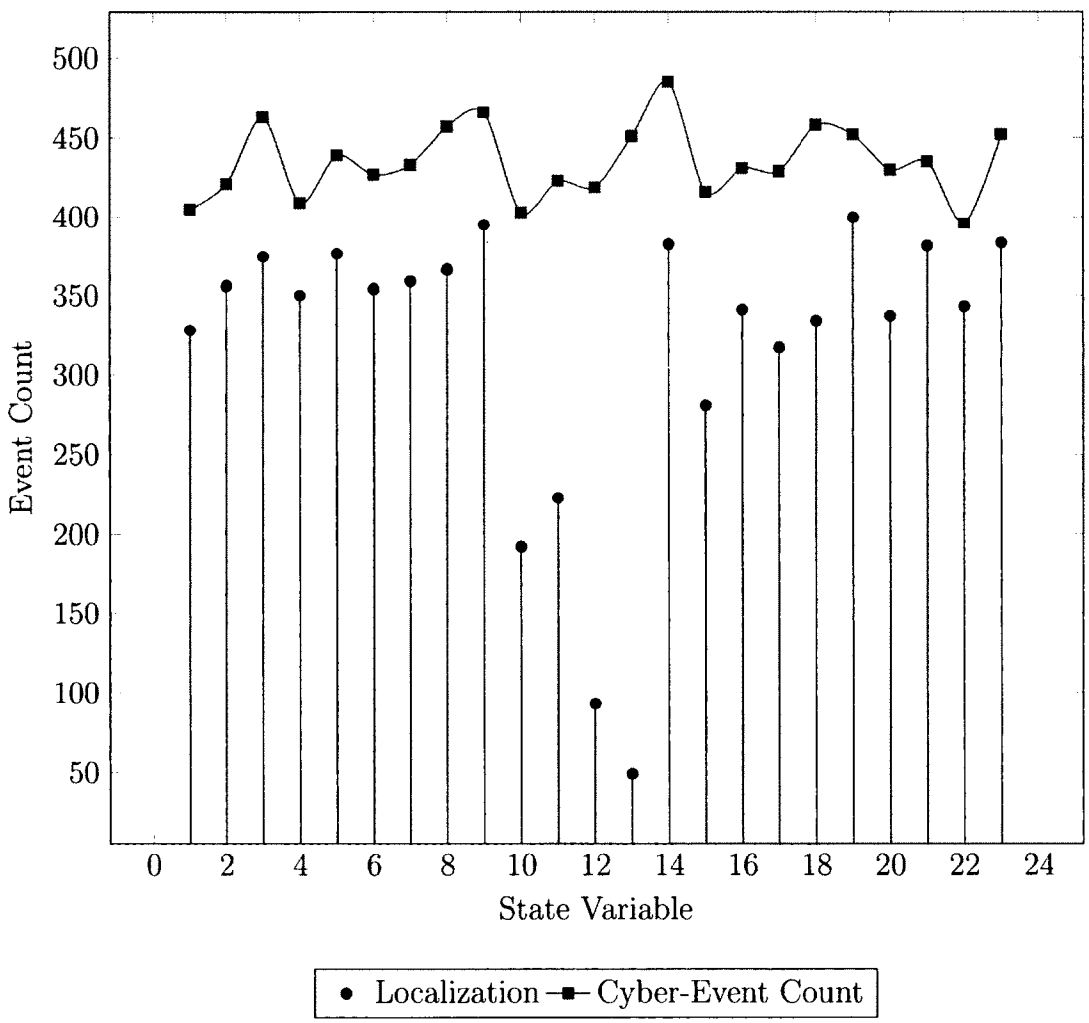

Figure 9.1: 5-Bus Without Line Flows SII Localization Results

9.2 False Positive Analysis

The false positive (FP) localization results for each considered topology are shown in Figure 9.2. A false positive localization is the labeling of a power system state variable as being the source of an event when the simulated event occurred on another state variable. Results are plotted for each topology and each consideration according to the attack type tested. The FP % is a total percentage out of the total number of attacks simulated for that given system's consideration.

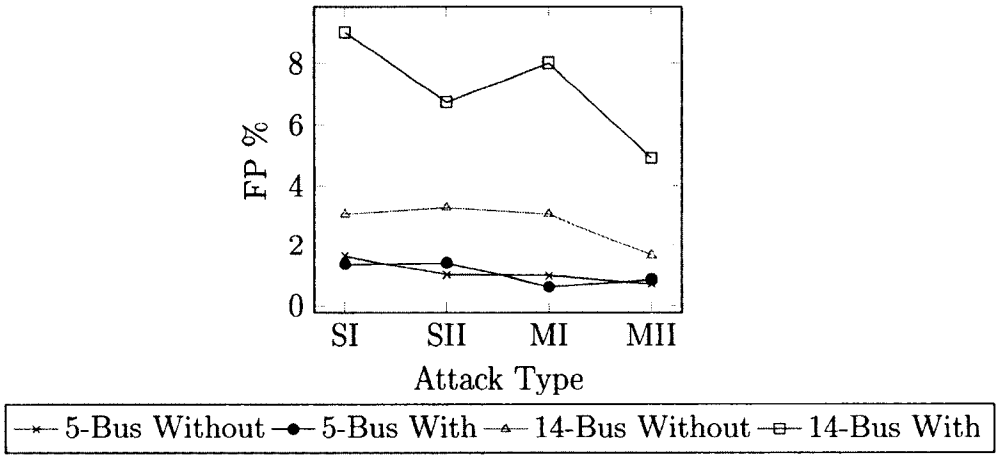

Figure 9.2: Overall False Positive Localization Results

The results shown in Figure 9.2 reveals that the 14-Bus power system had the highest FP rate for any given system. The 14-Bus system for the case where injected powers are included at the highest with an average of 7% for all four attack types simulated. The event detection scheme for the 5-Bus power system had a FP percentage of on average 1% for each consideration, during each of the four simulated attack types. This corresponds to a very low FP rate and means that for the 175,000 simulated attacks on the 5-Bus system only 1,750 were inaccurately localized.

9.3 True Positive Analysis

This section assesses the overall performance of the localization approach by comparing the true positive (TP) classification of each system under each consideration. TP classification for the localization stage describes the exact identification of the source of the cyber-event. Results of this analysis are presented in Figure 9.3. These results are presented in the form of percentages showing the relative succsseful classification for each system.

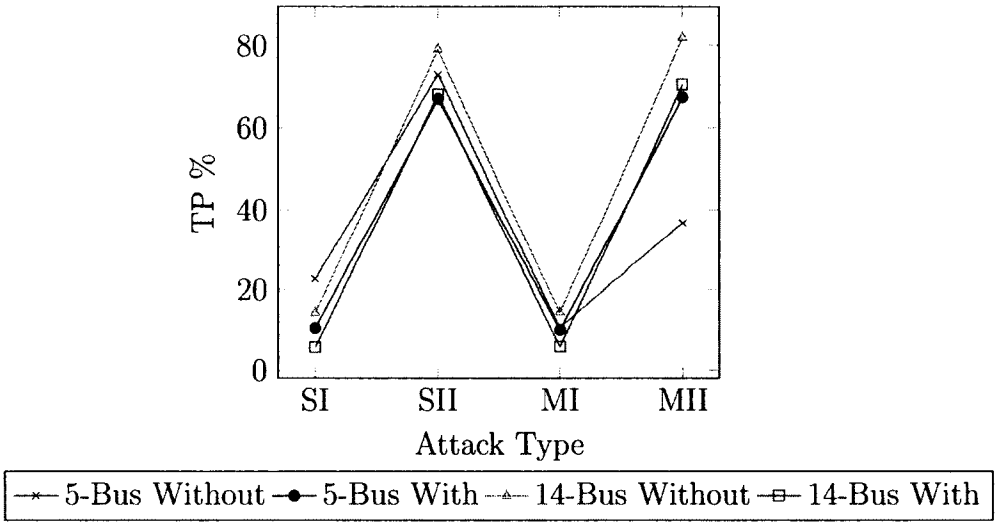

Figure 9.3: Overall True Positive Localization Results

The results shown in Figure 9.3 reveals a common trend among each considered power system topology. For the type I attacks, the average of all four considerations was found to be 11.7%. As noted in the previous sections, a type I attack is hard to detect because these type of attacks are small fluctuations away from the means of most normalized state variables. For all but one consideration, the TP classification results were found to be over 65%. This exception was for the 5-Bus power system whose TP

percentage was calculated at 36.8%. The localization true positive and false negative results for each system are described separately in the next two sections. Though these results are not ideal, they are promising. Possible approaches for increasing the TP rate while decreasing the FP classification of the localization stage are described in Chapter 12, Section 12.2.3.

9.4 5-Bus Localization Results

In an attempt to better understand the results of Figure 9.3, the true positive results are analyzed in this section, specifically for the 5-Bus power system. This analysis also goes on to determine exactly which variables had the highest TP counts and which had the lowest. The TP percentages are shown in Figures 9.4 and 9.5 for the 5-Bus system when the injected powers are not and are being considered. Figure 9.4 examines the TP percentages for the case where the injected powers are not considered while Figure 9.5 examines the case where they are being considered. The results shown in both figures are relative to the number of attacks that were performed on each specific power system state variable. For instance, for the power state variable x_1 shown in Figure 9.4, a total of 214 SI attacks were performed with a TP localization count of 213. This corresponds to a TP percentage of 99.5% as shown in 9.4.

According to Chapter 6, Section 6.3, for the case where the injected powers are not being considered there are 23 power system state variables being analyzed. The exact electrical meaning of each variable is shown in Table 6.3. As shown in Figure 9.4, the bus voltages for attack types SI and MI have the highest TP percentages with

near 100% classification rates. For both attack types, however, the percentages drop to near zero values. For the other two attack types, SII and MII, the TP percentage is an average 80% with the exception of the SII attack type for only 4 variables. These exact four correspond to the real and reactive powers being generated at bus 1 and bus 3. The cause of these drops corresponds to the fact that these state variables have a higher range of acceptable values which still produce feasible power system instances. The box and whisker plots for each of these variables is shown in Figure A.4. Upon close inspection of Figure A.4 it is determined that the reactive power at bus 3, 'QG3', has the greatest range causing the lowest localization results for the corresponding state variable, x_{13}, as shown by Figure 9.4.

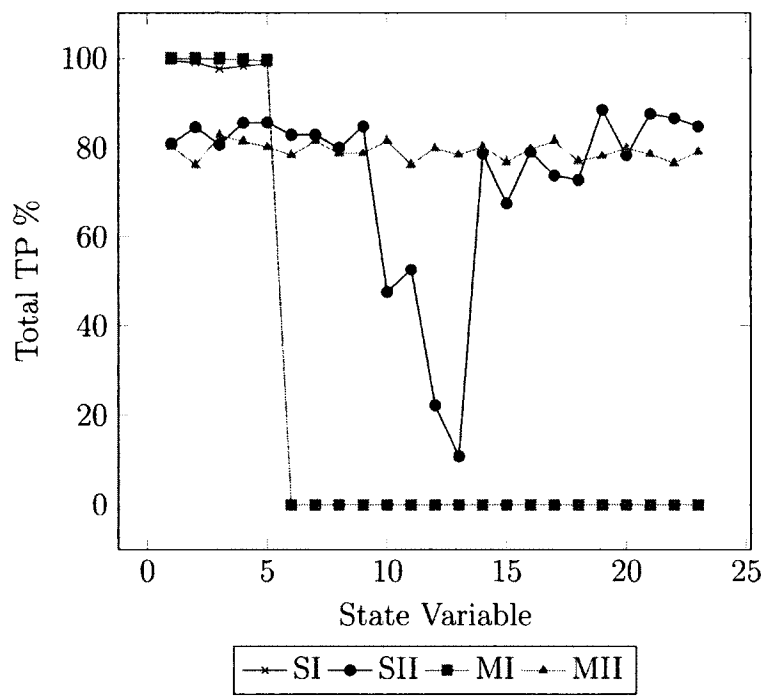

Figure 9.4: 5-Bus True Positive Localization Results, Without Injected Powers

Similar to the previous plots in Figure 9.4, Figure 9.5 shows the TP percentages for the 5-Bus power system when the injected powers are taken into consideration. The corresponding electrical meanings of each state variable x_i are shown in Table 6.4. For the first 23 state variables results are near consistent with those of the case without considering injected powers. One of the major differences, however, is found in the consistent drop in the average of the MII attack type. These results indicate a 70% average while before the average was 80%. Lastly, there appears to be three distinct groups for the SII attack type after state variable x_{14}.

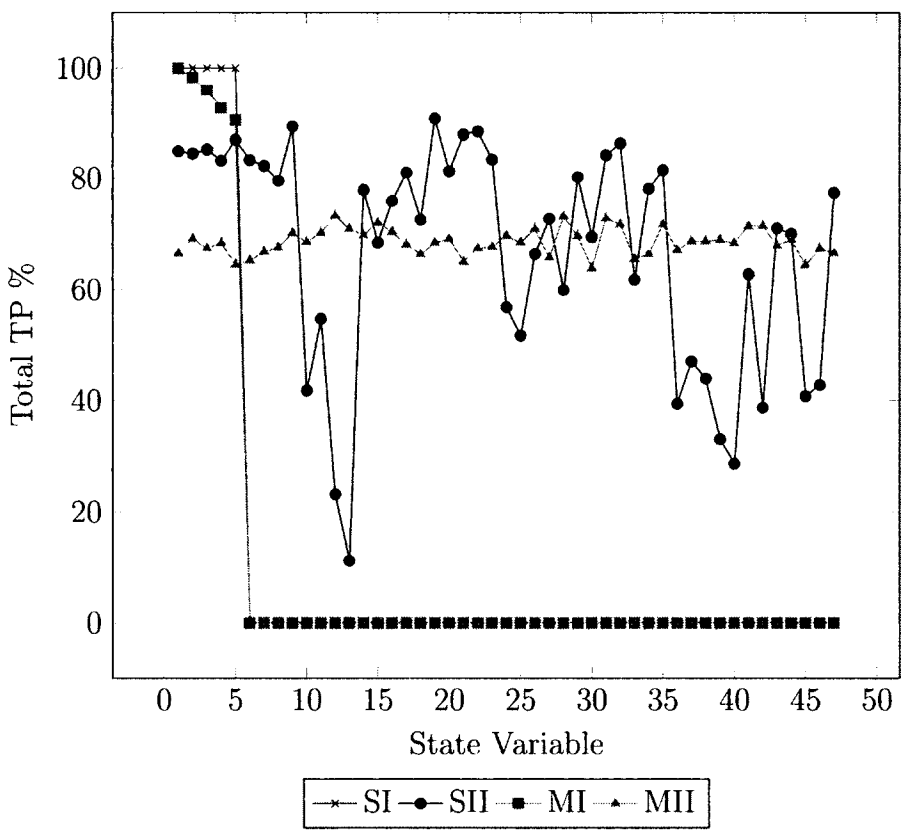

Figure 9.5: 5-Bus True Positive Localization Results, With Injected Powers

9.5 IEEE 14-Bus Localization Results

Similar to the analysis performed for the 5-Bus system, the TP percentages shown in Figures 9.6 and 9.7 are the relative counts for the IEEE 14-Bus power system. The corresponding electrical meanings of the state variables for the case where the injected powers are not being considered are listed in Table 6.5. Upon close examination, the results are also consistent to the type of attack and to the electrical meaning of the state variables the attack was performed on. For instance, as shown in Figure 9.6, the highest TP percentages with near 100% counts occurred during MI attacks for the voltages on voltages controlled busses. For the non-voltage controlled busses, the percentages drop to near 0% for MI attacks. These trends occur for both the SI and MI attack types.

With only a few exceptions, for attack types SI and MII, there is a consistent average of the TP percentage of 81%. The exception corresponds to when SII attack types are performed on state variables x_{28}, x_{29}, x_{30}, and x_{31}. These four variables correspond to the real and reactive powers being generated at busses 1 and 2. Unlike the 5-Bus case, for the state variables $x_{38} - x_{56}$, the SII attack types resulted in higher TP percentages than those of the MII attack type. Another observation that is similar to the 5-Bus system are results of the IEEE 14-Bus system for the first 56 state variables. These variables are consistent across both considerations as shown in Figures 9.6 and 9.7.

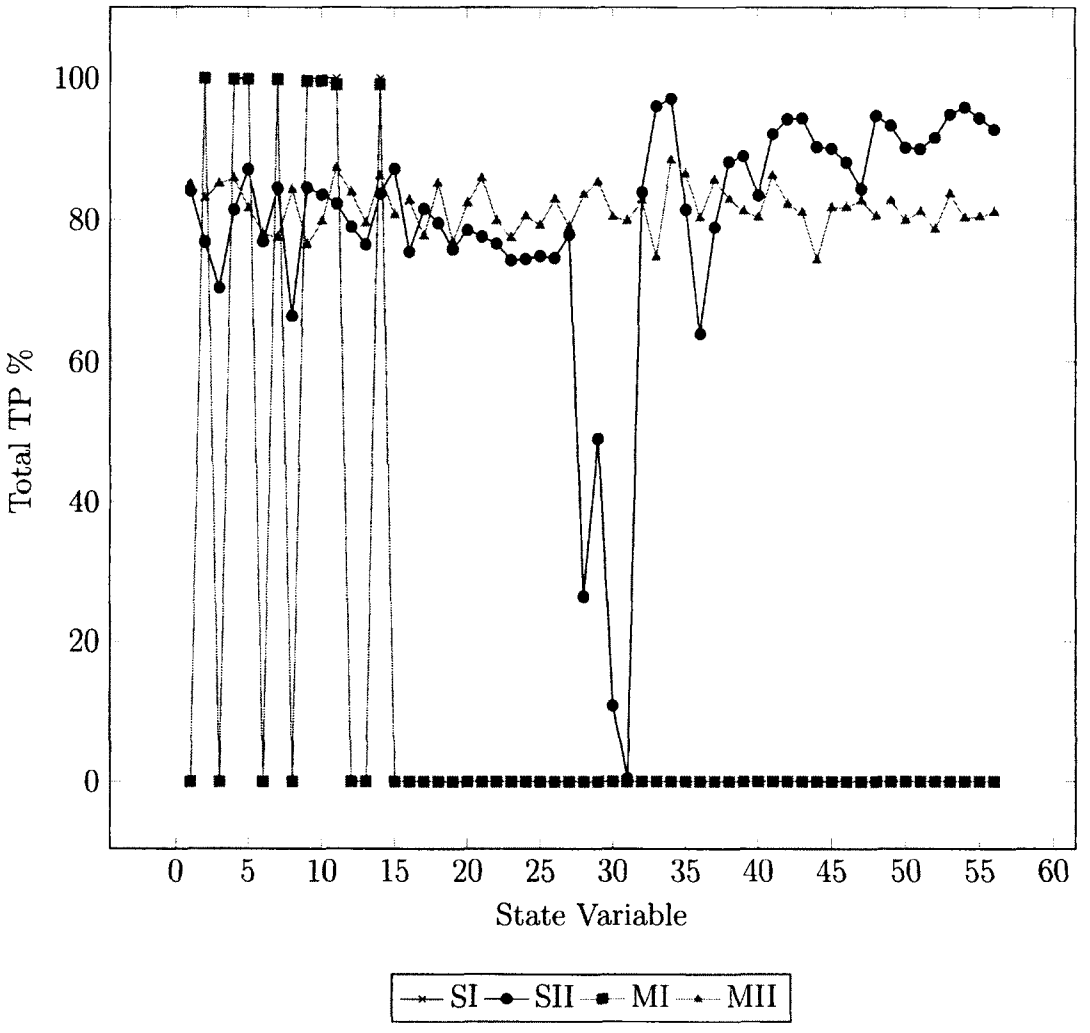

Figure 9.6: IEEE 14-Bus True Positive Localization, Without Injected Powers

The electrical meaning of the state variables plotted in Figure 9.7 are listed in Table 6.6 and include the injected powers flowing through the transmission lines. These results are consistent with those shown in the previous figure and exhibits the same trends as that of the 5-Bus power system. As shown in Figure 9.7, the attack types MI and SI have roughly the same TP percentages dropping down to near zero for all state variables after x_{14}. There is also a grouping pattern for the line flows with the first set between $x_{56} - x_{96}$ and the second between $x_{97} - x_{136}$.

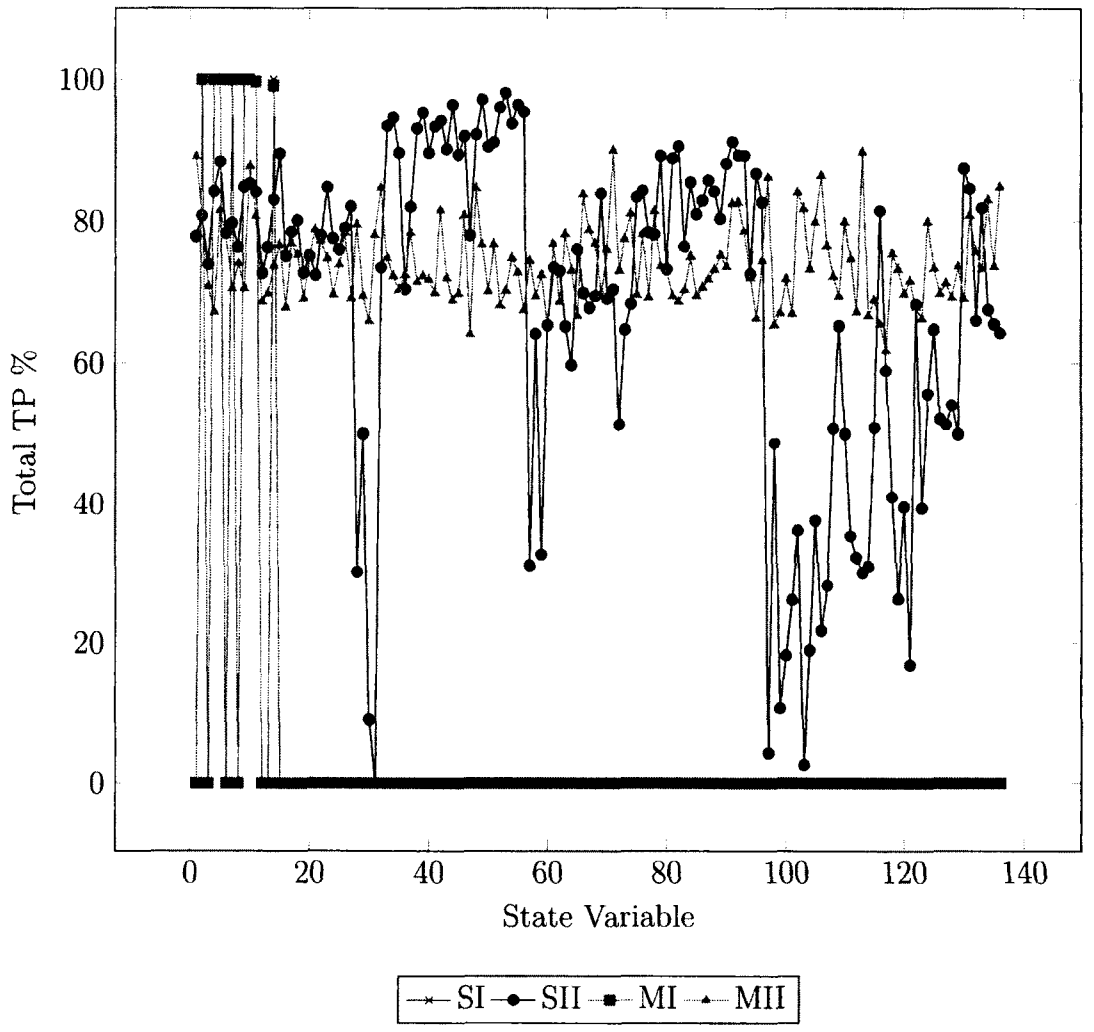

Figure 9.7: IEEE 14-Bus True Positive Localization, With Injected Powers

On average, it appears that for attack type SII, the injected real powers, $x_{56} - x_{96}$, have a higher TP percentage than the injected reactive powers $x_{97} - x_{136}$. This average was fount to be 74% with only two dropping below 40%. The reactive powers, however, for the SII attack type fluctuated with a TP percent range between 2.6% and 90%. For the IEEE 14-Bus power system the localization results indication extreme difficulties in the identification of SI and MI type attacks.

9.6 Conclusions

The localization results presented in this chapter examines the collective false positive results along with performing a detailed examination into the true positive localization of each power system. These examinations are measured according to the the total number off attacks performed on a given state variable. Results indicate a near 100% successful localization for the voltage state variable only on voltage controlled busses all power systems when a SI or MI attack is performed. SII attacks for both power system topologies produce a near constant TP average between 60% and 80%.

CHAPTER 10

STEALTHY ATTACKS

10.1 Introduction

A stealthy attack is one that evades the identification and localization of the developed cyber-event detection scheme. This chapter analyzes these events in an effort to extract patterns and gain insight into what the developed scheme is not able to detect. Results are presented according to the attack types simulated and the power system topology utilized. Such an analysis provides insight into the regions of detectability and provides a basis for improving the scheme as outlined in Chapter 12. Results are presented in the following two sections for the 5-Bus and 14-Bus power systems. The results presented in this chapter correspond to the false negative (FN) results presented in the two previous sections, collectively. However, in the case of this examination, emphasis is on determining which state variables, when attacked, produced a false negative classification. Results presented here are in the form of relative percentages corresponding to the total number of attacks performed on that specific power system state variable.

10.2 5-Bus

Figures 10.1 and 10.2 reveal the false negative results of the developed detection scheme for the 5-Bus power system. Figure 10.1 reveals the FN percentages in the case where the injected powers are not being considered while Figure 10.2 presents the results for when they are being considered in the calculation. The electrical meaning of each power system state variable x_i for the 5-Bus power system are listed in Tables 6.3 and 6.4. As shown in Figure 10.1, every attack performed for this scenario was detected by the developed framework corresponding to a successful identification rate of 100%.

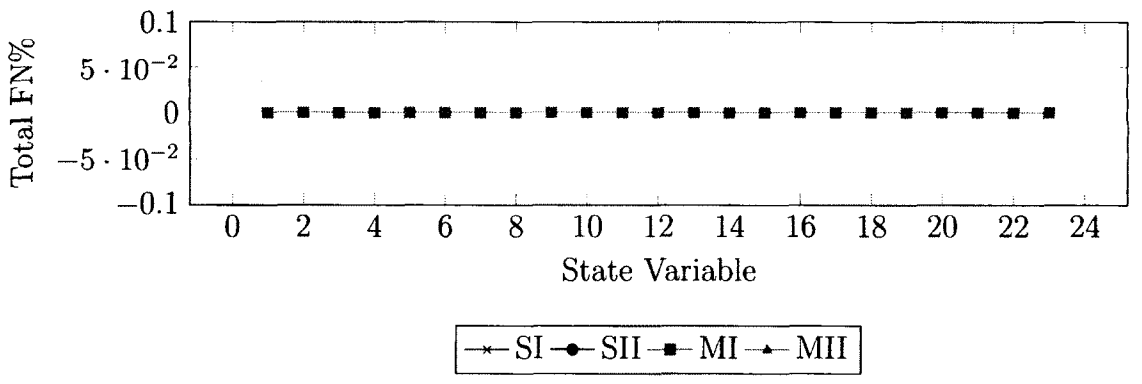

Figure 10.1: 5-Bus False Negative, Without Injected Powers

For the case where the injected powers are included, however, not every attack was detected. For instance, by examining Figure 10.2, it is revealed that the developed detection scheme was not able to detect certain SI attacks. The state variables that produced these unobservable attacks include the bus voltage angles θ_i at busses 2, 3, 4, and 5. Results indicate the highest included θ_2 corresponding to a failed detection

of 36.6% for this particular state variable. Failure to detect attacks on the bus voltage angles θ_i was also noticed for SII and MI attack types. Though for these two attack types, failure to detect remained under 5%. The SII attack type also produced interesting results for the bus voltages $x_1 - x_5$. Failure to detect a SII type voltage attack on bus three was found to be 4%. Though not a high number, this is cause for some concern. Recall that according to the one line diagram shown in Figure A.1, bus 3 is a PV bus and any inaccurately reported voltage parameters on this bus may have devastating effects on the generation capabilities.

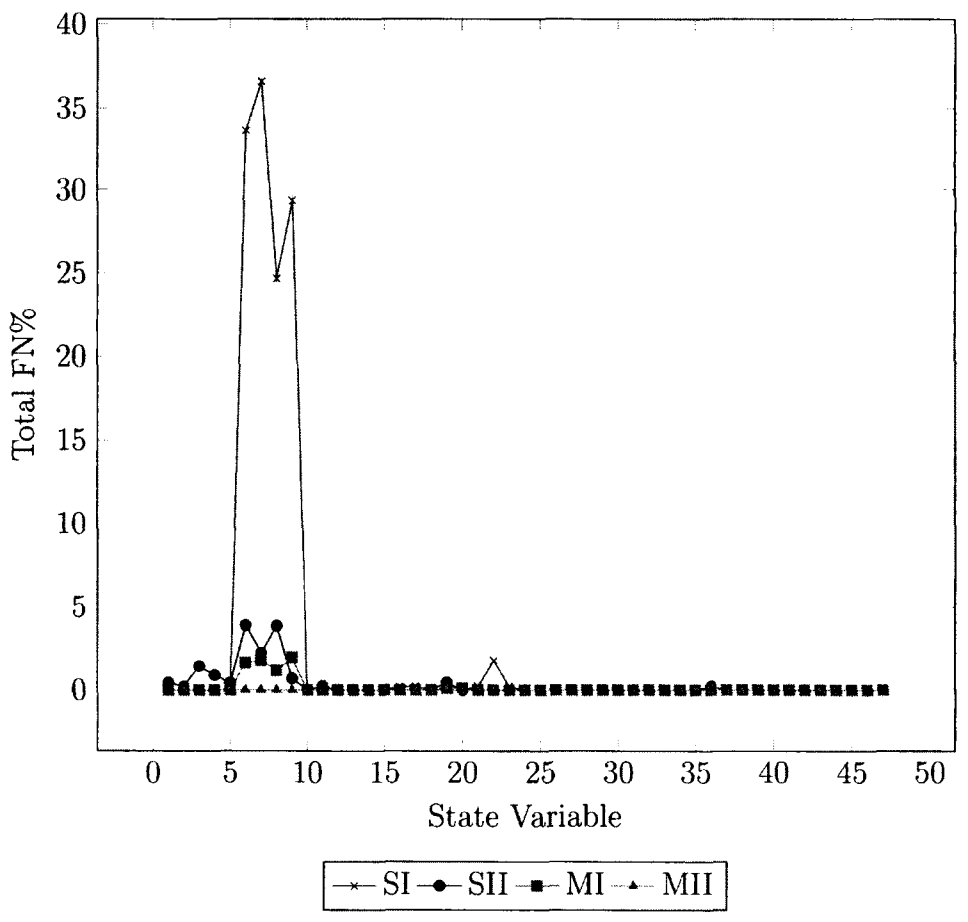

Figure 10.2: 5-Bus False Negative, With Injected Powers

10.3 IEEE 14-Bus

The results of the stealthy attack analysis for the IEEE 14-Bus power system are shown in Figures 10.3 and 10.4. The electrical meaning of each power system state variable x_i for the IEEE 14-Bus power system are listed in Tables 6.5 and 6.6. Figure 10.3 presents the results for when the injected powers are not being considered while Figure 10.4 reveals the results for when the injected powers are being considered. The results presented in Figure 10.3 are not directly consistent with those presented for the 5-Bus case. However, the detection performance of each attack type was similar with SI still remaining the hardest to detect.

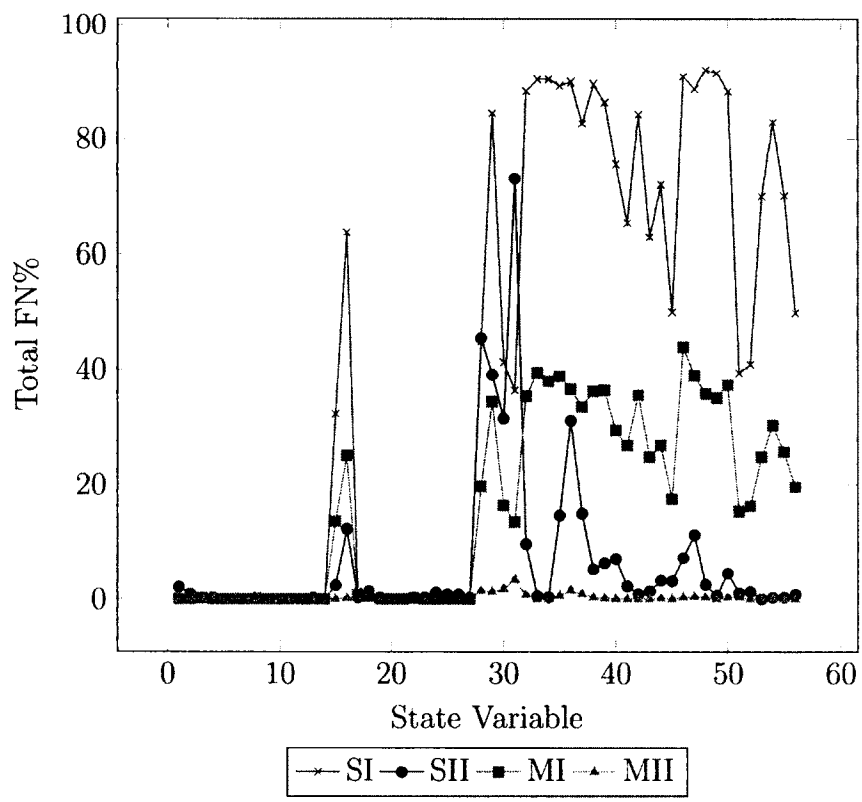

Figure 10.3: IEEE 14-Bus False Negative, Without Injected Powers

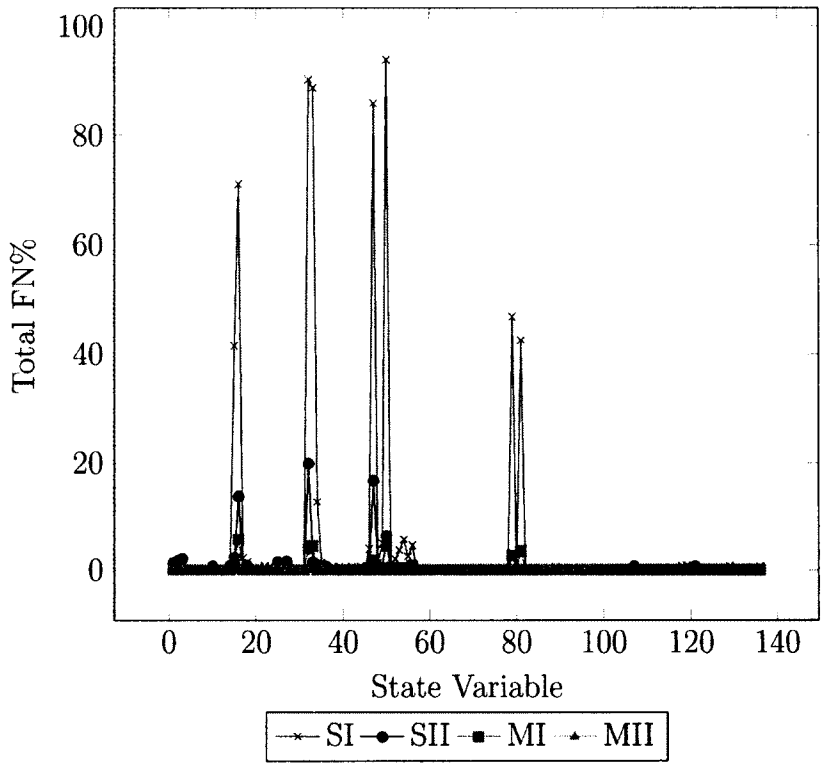

Figure 10.4: IEEE 14-Bus False Negative, With Injected Powers

For the case where the injected power are not considered, the attacks compromising the loads appear to have the highest failure to detect percentages. This information is revealed in Figure 10.3 and shows that for SI attack type failure to detect on average load parameter attacks was 75%. The average failure to detect for load attacks dropped down to 31% for MI type attacks and to 8% for SII type attacks. Furthermore, for the voltage angles, only two busses contribute to the failure to detect percentages. The highest was for a SI attack on the voltage angle θ_3 with and FN value of 64%. Other spikes in the FN percentages were found to exist on this particular state variable. Specifically, failure to detect a MI attack was found to be 25% while failure to detect for SII events was 12.2%.

For the case where the injected powers are considered, there appears to be four distinct groups in the failure to detect percentages. Specifically as shown in Figure 10.4, these four groups include attacks on state variables $G1 = [x_{15}, x_{16}, x_{17}, x_{18}]$, $G2 = [x_{32}, x_{33}]$, $G3 = [x_{47}, x_{50}]$, and $G4 = [x_{79}, x_{81}]$. G1 corresponds to the voltage angles for bus 2, 3, 4, and 5. G2 corresponds to the reactive powers generated at Busses 6 and 7. The G3 grouping corresponds to the bus 3 and 6 reactive loads. The last grouping, G4, corresponds to the injected powers specifically P_{4-2} and P_{4-3}. Recall that according to, this notation P_{i-j} means that the power flowing from i to j.

The highest failure to detect percentage was found in G3 and corresponds to an SI attack on state variable x_{50} with a $FN_{SI}(x_{50}) = 93\%$. This variable corresponds to the reactive power being consumed on bus 6 which drops down to below 10% for both the SII and MI attack types. The highest failure to detect for SII attacks was calculated to be on state variable x_{32} with a $FN_{SII}(x_{32}) = 19.9\%$. This corresponds to the reactive power generated at bus 6.

10.4 Conclusions

The work performed in this chapter assessed the developed cyber-event detection scheme by determining a set of attacks which evaded detection. Looking at all the attacks performed, there is only a small subset that was able to avoid detection by the developed framework. The analysis was performed in the context of the electrical parameters. As expected, the results indicate that the easiest attack to detect was a MII type attack while the hardest was found to be SI attacks. Nevertheless, it was determined that only certain SI attacks remained undetectable by the detection

scheme. Generally, SI type attacks that compromised the voltage angles while those that attack other state variables were for the most part detectable. For the 14-Bus power system, it was determined that the hardest attacks to detect was those which occurred on bus 6.

CHAPTER 11

CONCLUSIONS AND RECOMMENDATIONS

11.1 Introduction

Using uniquely crafted machine learning algorithms, this dissertation successfully demonstrated a cyber-event detection framework based purely on the extraction of information from the physical perspective of two power systems. Examination targeted a 5-Bus power system [2] and the IEEE 14-Bus power system [79]. The physical perspective utilized by the detection framework was derived by extracting key features from power system state variables including voltage magnitudes, voltage angles, real and reactive powers generated, along with the real and reactive powers consumed. Furthermore, effort was taken to replicate the losses of each power system by including the impedances of each transmission line.

For this examination, a total of four attack types were simulated encompassing both single variate and multivariate attacks which compromised randomly selected power system state variables. The objective of the framework was to detect and localize these attacks or cyber-events. Two classifiers were used to identify the presence of a cyber-event while a form of outlier detection was used to localize the event. The developed framework was able to identify a total of 92.5% of the 335,000 events and for certain considerations localized over 80%.

11.2 Framework Classifiers and Parameters

The developed cyber-event detection framework relies on a combination of trained classifiers to identify and localize events. Both identification and localization could only be performed once the parameters of each classifier were determined. This section outlines the selection results of the classifier parameters which were then used in the detection framework. The following list provides a summary of the recommended parameters for the developed framework while Section 11.4 describes the resulting performance observations of the detection approach.

1. Convergence Classifier

   A total of four discriminant classifiers were tested for each of the considered power system topologies. The tested classifiers included linear, diagonal linear, quadratic, and diagonal quadratic discriminant classifiers. For each considered power system topology, the classifier that outperformed was the quadratic discriminant classifier when a training size of $n \geq 3000$ was used. Based on the initial test results the quadratic discriminant was selected for the first stage of the developed framework.

2. Instance Classifier

   Instance classification is based on transforming the power system instance into a reduced dimensional space where new features were then extracted. Using the Hotelling's T^2 value of each power system instance in the trusted models, a distribution was created that defines normal operation for each system. If the Hotelling's T^2 value of a suspect power system instance was found to be more than three standard deviations away from the distribution

of the trusted model, then the associated power system instance was labeled as containing a cyber-event. The T^2 distribution could either be calculated before or during inspection of the new power system instance.

3. Localization Classifier

   Localization is based on the Grubbs Test, which also uses a trusted power system instance to derive a trusted model. The test is univariate in nature when looking at each state variable, independently. For this reason, it is suggested that the associated statistics of the Grubbs Test be calculated prior to event localization.

11.3 Computational Constraints

With the parameters and classifiers selected according to the details outlined in the previous section, an analysis into the computation constraints was performed. Though not mathematically derived, the computational constraints of the developed cyber-event detection framework were measured using CPU time. The execution time for each topology under each consideration is shown in Table 11.1. These results indicate an increase in the computational complexity provided the given times required to compute the existence of a cyber-event. Recall that if a cyber-event is detected by the convergence classifier the instance classification, or PCA transformation, is skipped. This substantially reduces computation time for the detection of the cyber-events.

The results shown in Table 11.1 were computed on a Dual-Core Intel Xeon with a processor speed of 3 GHz and 16 GB of RAM. The most computational intense aspect of the scheme is the PCA transformation, which in its current setup is calculating the

Table 11.1: Detection Scheme Computational Time (s)

	5-Bus		14-Bus	
	Convergence	**Instance**	**Convergence**	**Instance**
Without	0.11	0.78	0.16	2.55
With	0.14	2.04	0.31	10.5

transformation of the trusted model every time a new power system instance is placed in the queue. This, however, does not have to be the case as the transformation of the trusted model can be calculated offline and updated periodically. The developed cyber-event detection scheme was tested using the Matlab [86] framework and is considered an interpreted language, resulting in slower execution times. Also, through code optimization it is believed that the developed detection scheme can meet the real time analysis constraints. Furthermore, it is believed that given the current rate of growth for CPU/GPU power, the developed detection scheme will not reach hardware limitations for small to medium size power system topologies. Such hardware limitations are becoming non-existent and computational efficiency can be reached in software [87].

11.4 Framework Performance

The developed cyber-event detection framework relies on a combination of trained classifiers to identify and localize events. This section outlines several key observations made by analyzing the identification and localization results of the developed framework. These observations are based on the true positive and false negative classification of the 335,000 simulated cyber-events. A list of parameters and summary observations of the developed detection framework include the following:

1. Detectability of Attack Types

Upon analyzing the results, it was determined that some attack types were easier to detect than others. The overall order of difficulty in detectability from hardest to easiest for the four attack types are: SI, SII, MI, and MII. These differences however small are presented in the TP results shown in Tables 8.4 and 8.10.

2. Weakness to Specific State Variable Attacks

   Discussed in the stealthy attack chapter, Chapter 10, the variables that appeared to avoid detection the most were attacks on the bus voltage angles. One possible explanation for this is that these state variables have a much larger range of acceptable values than the other power system state variables. Also, mathematically the angles contribute predominately to the first principal component which appears to diminish the events' contribution to the Hotelling T^2 value.

3. False Positive Analysis

   The false positive analysis performed in Chapter 8 never reached over 10% with three of the eight simualtion conditions producing a near 0% FP percentage.

4. True Positive Analysis

   The true positive analysis revealed that 93% of the simulated attacks were identified while the source of the event was successfully localized for 90% of the state variables. The 10% that were not able to be localized occurred only on specific state variables. Furthermore, it is noted that even though the exact source of the event has not been identified, the power system

instance has been labeled as containing a cyber-event and can undergo additional analysis. These additional modifications are described in Chapter 12.

11.5 Conclusions

The identification of 93% of the simulated attacks indicates that the developed detection framework demonstrates the latent potential that exists in using historical power system state information for the detection of cyber intrusions. Based on the results presented in this dissertation, it is recommended that the scheme be tested in live power systems, or at the very least, receive additional testing using historical SCADA databases from active power systems. The developed cyber-event detection scheme is currently designed to be completely passive, executing only read privileges of system databases. Furthermore, several additions/enhancements have been suggested in the future work section of this dissertation. These modifications will certainly prove to be valuable in the future development of the framework and lays the foundation for the creation of an intrusion detection system specifically tailored for the power grid and other cyber-physical systems.

CHAPTER 12

FUTURE WORK

12.1 Introduction

With the successful development and assessment of an application centered cyber detection scheme described in this dissertation, future advancements to this scheme can be made. This chapter explores the different avenues that can be pursued to either improve or complement the developed detection scheme. Some improvements include computational modifications to the classifiers while the complementary work includes adding an IT based perspective for a correlated cyber-physical intrusion detection scheme. Other possible avenues include the utilization of the developed detection scheme in the context of incident response. If a cyber-event is believed to have occurred on a power system state variable, then with some modification, the scheme could be used to isolate the event proving fruitful as a forensics tool. Such forensics analysis could be performed on the SCADA Historian servers. The suggested modifications require additional power system topologies and more integrated mathematical constructs and therefore are out of the scope of the current approach developed by this dissertation.

12.2 Modifying Classifiers

The results of the developed detection scheme discussed in the previous three Chapters, Chapters 8, 9, and 10, are promising. Through certain modifications of the developed classifiers, it may be possible to increase the classification results to even more desired levels. This section proposes some possible modifications that may prove fruitful in the future development of the cyber-event detection scheme.

12.2.1 Convergence Classifier

Recall that according to Section 4.3, the convergence classifier uses discriminate analysis to determine if a subset of power system state variables form a feasible set. The training models were based purely on solutions to the power flow problem which was solved using the Newton-Raphson method. However, one drawback of using only the Newton-Raphson method is that this approach may not converge even for feasible inputs into the power flow problem [84]. The power flow analysis therefore will bias the convergence classifier in favor of the non-converging class or the malicious class. This is because even though the inputs create a feasible power system instance, the set of inputs are placed in the wrong set by the training of the classifier.

A possible approach to this problem is through the integration of a variety of known solutions to the power flow problem. Such a variety will ensure that the feasible region is covered in the classifier. Other possible iterative solutions to the power flow problem include the Guess-Seidel method [1] and modifications to the power flow problem itself as those discussed in [88, 89, 90]. Lastly, the works presented in [91, 92]

actively seeks to mathematically define the boundaries of the feasible regions will not doubt be of use in these enhancements of the convergence classifier.

12.2.2 Instance Classifier

The instance classifier used a technique known as principal component analysis (PCA) to transform power system instance into a new dimensional space for comparisons. Comparisons are made against a trusted model in effort that is designed to detection anomalies. This process is mathematically presented in Section 4.4. One problem with this particular approach is when an attack occurs on a state variable whose feature projections on the first few principal components are small to non-existent. Using the current detection method, this type of attack would go unnoticed. Potential solutions to this problem include a technique known as weighted PCA which has produced promising results in the areas of biometric identification [93, 94] and diagnostic medicine [95, 96].

12.2.3 Localization

The localization of cyber-events was based on a form of outlier detection and therefore is week against attacks that inject state variables on x_i that are close to the mean $\bar{x}_i$ of the trusted models. If temporal data along with other key features are retained, as explained in Section 12.4, this will increase the number of attacks that can successfully be localized.

12.3 Examining Forensics Implementation

Current implementation of the developed cyber-event detection scheme is geared towards live power systems. As noted previously in Chapter 4, the trusted

models are built on historical power system state variables stored inside the SCADA system. With slight modification however the developed approach may be able to be used in the context of a forensics analysis. By performing the detection scheme utilizing an iterative form of cross validation on a suspicious historical dataset, it would be possible to isolate and identified when the attack occurred and on what power system state variable.

12.4 Increase Power System Features

Power systems are a unique environment with set operational limits that are either defined by fundamental electrical laws or are set in place by the system's design engineers. In any case, these constraints offer additional insight into the status of the power system. By adding this treasure trove of data to the developed intrusion detection, it is possible to create an even more intelligent intrusion detection system. Potential power system features include the following:

1. Generation Contraints

   Generation contrasts are based on rated values of various generation facilities throughout the power system topology and includes the limits on real and reactive powers generated. By incorporating this information beforehand into the training models of the convergence and localization classifiers, a decrease in the feasible region will be observed, enabling more accurate classification.

2. Economic Dispatching

   Economic dispatching is the act of dispatching power generation according to cost functions predetermined by the power system design engineers. This

process can save a utility millions annually [1, 28] and places more limits on the generation of each generation facility.

3. Load Profiles

   Load profiles describe the retention of power consumption by the loads through the topology and is temporal in nature [28]. Integration of these features may provide a basis for more sophisticated localization approaches including neural nets.

4. Device Configuration

   Similar to generation constraints, the retention of device configuration will set limits into the computational analysis used to develop the trusted models. Configurations may include position of tap changing transforms, relay settings, and the settings of other intelligent electronic devices spread throughout the topology.

12.5 Integration Into a Cyber-Physical Detection Scheme

A new high confident detection scheme can be developed that merges the work described here with the information gained by observing information technology parameters. Such a detection scheme can be called high confident as it brings together the physical and cyber perspectives into a unified perspective that is self verifying and complementary. Therefore, an extension of this dissertation includes the development of a unified cyber-physical high confident intrusion detection scheme for the critical infrastructure power grid. High confident detection is provided by the correlation of the cyber control infrastructure and the physical power system perspectives resulting

in a derived approach which encompasses the interacting dynamics between them. This derived approach will yield a new unified perspective for the creation of a novel high confident intrusion detection scheme.

By observing high level grouping phenomenon in both the power system (bus voltages, phase angles, circuit breaker status, and tap changing transformer position, among others) and cyber system (throughput, payloads, MACs, IPs, packet latencies, amongst others) simultaneously, it is possible to derive a unified perspective. By observing these two perspectives both independently and collectively, dynamics will be observed that encompass how these two perspectives interact. Figure 12.1 shows the overall process of this proposed future work. The four main steps for a high confident detection framework include the following: data aggregation, pattern and correlated pattern recognition, hybrid classification, and incident identification.

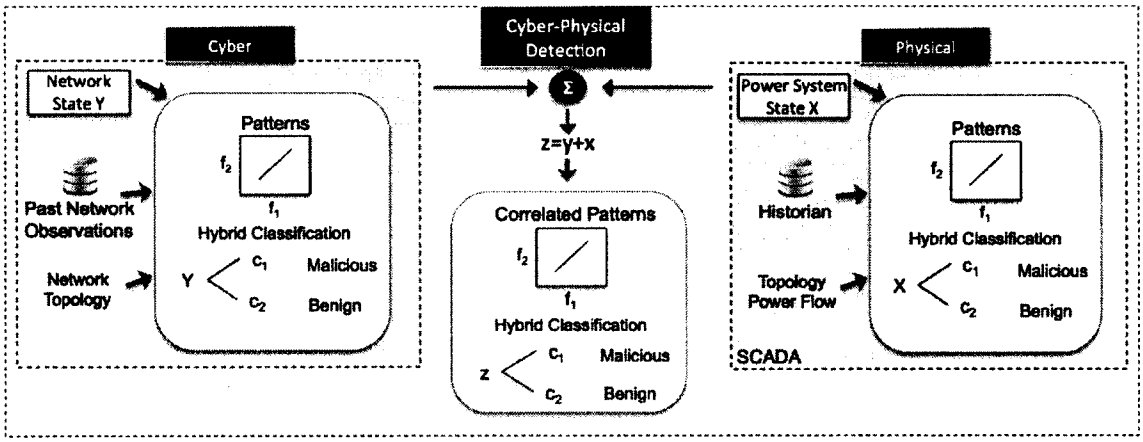

Figure 12.1: Suggested Future Approach for High Confident Intrusion Detection

1. **Data Aggregation**:

Data aggregation can be accomplished by bringing together both perspectives and all available information used to describe the cyber-physical system.

Aggregation of the cyber system perceptive can be derived by examining a) past observations and b) current observations of the cyber network controlling the physical power system. Observations are the result of strategically placed network observers which provide the following network attributes: throughput, payloads, MACs, IPs, packet latencies, amongst others. This information can be added to the information utilized by the detection scheme successfully developed by this dissertation.

2. **Pattern and Correlated Pattern Recognition**:

Pattern recognition is the result of information retrieval methodologies wherein patterns from large datasets are extracted across both perspectives. Such patterns can be extracted via the extensive analysis on the data aggregated, which contains a collection of power system states and cyber network states, independently. Dimensionality reduction and kernel transformations into different dimensional spaces provide a means for the extraction of information (patterns) provided by the decrease in redundant information. In a similar way, perspectives can be combined and correlated patterns are to be extracted, which express relationships between the cyber and physical perspectives. A potential correlated pattern includes while the physical power system is in an undesired state the energy management system (EMS) will send certain commands (network packets) to the controllers in the power system. By observing features from one perspective, inferences can be made describing the other, resulting in a derived unified perspective combining all available cyber-physical information. Promising feature extraction techniques have already been identified for both

the cyber perspective [59] and physical perspective by the work performed here in this dissertation.

3. **Hybrid Classification**:

Based on results described in this dissertation that describe a detection scheme using the physical perspective, it is suggested that the unified classification scheme developed will be hybrid in nature. A hybrid approach brings the benefits of multiple classification algorithms together into a single classification approach accomplishing more than just one algorithm can accomplish alone. Such techniques in the discipline of knowledge discovery is known as ensembles. As shown in Figure 12.1, classification is to occur at the cyber and physical perspectives independently while also occurring at the collectively derived perspective. This particular structure for classification produces an environment for a highly confident intrusion detection scheme with each perspective either validating or identifying the intrusion.

4. **Incident Identification**:

The classification of each state is based on the hybrid approaches and feature extraction methods to be developed. Incident identification is the result of examining the classification and attributes of each perspective both independently and collectively. By cross examining the classification performed by each perspective, the true result and method of the intrusion can be identified. For instance, if the cyber perspective successfully classifies and extracts a spoofed control packet and a change in the power system state is observed to be reflective

of that spoofed command, then it can be concluded within high confidence the method and target of the intrusion.

12.6 Conclusions

Though the work developed by this dissertation is promising, certain modifications and enchantments may increase the overall accuracy and efficiency of the developed approach. This chapter proposed several possible near term enhancements while also proposing an approach that would integrate the cyber perspective to the developed cyber-event detection framework. The approach developed by this dissertation uses power system variables to reach a physically derived conclusion while a cyber detection scheme uses network telemetry and packet payload data to reach conclusions. The integration of the two perspective will produce an intrusions detection system fundamentally tailored to protect the smart gird and other cyber-physical systems.

APPENDIX A

5-BUS POWER SYSTEM

A.1 System Details

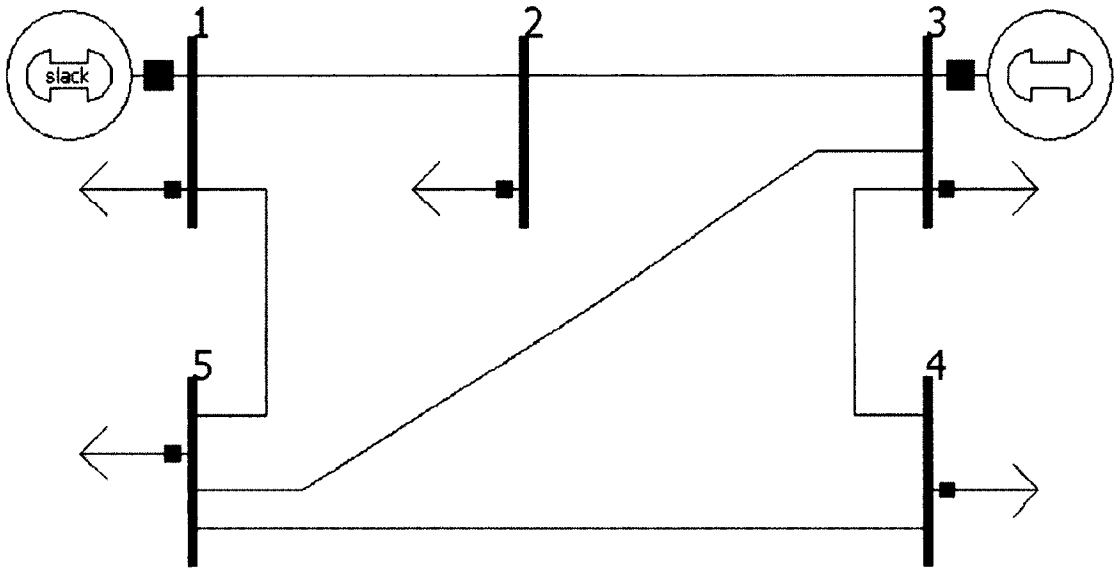

Figure A.1: 5-Bus One-line Diagram

Table A.1: 5-Bus Transmission Line Impedances [2]

Line #	Bus - Bus	R	X	B
1	1 - 2	0.042	0.168	0.041
2	2 - 5	0.031	0.126	0.031
3	2 - 3	0.031	0.126	0.031
4	3 - 4	0.084	0.336	0.082
5	3 - 5	0.053	0.210	0.051
6	4 - 5	0.063	0.252	0.061

A.2 Power Flow Simulation Snapshots

Table A.2: 5-Bus Input Snapshot

Bus #	Type	V	Delta	PG	QG	PL	QL
1	0	1.040	0	-	-	0.65	0.3
2	1	-	-	0	0	1.150	0.6
3	2	1.020	-	1.8	-	0.7	0.4
4	1	-	-	0	0	0.7	0.3
5	1	-	-	0	0	0.850	0.4

Table A.3: 5-Bus Output (**Bold**) Snapshot

Bus #	Type	V	Delta	PG	QG	PL	QL
1	0	1.040	0	**2.347**	**1.001**	0.65	0.3
2	1	**0.9614**	**-6.322**	0	0	1.150	0.6
3	2	1.020	**-3.713**	1.8	**1.103**	0.7	0.4
4	1	**0.9204**	**-10.88**	0	0	0.7	0.3
5	1	**0.9683**	**-6.162**	0	0	0.850	0.4

A.3 State Parameter Variances from Monte Carlo Simulations

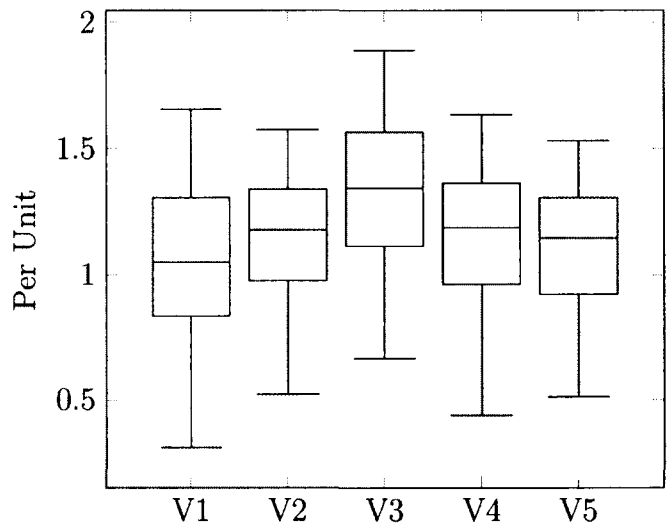

Figure A.2: Boxplot 5-Bus Voltages, 500 Instances

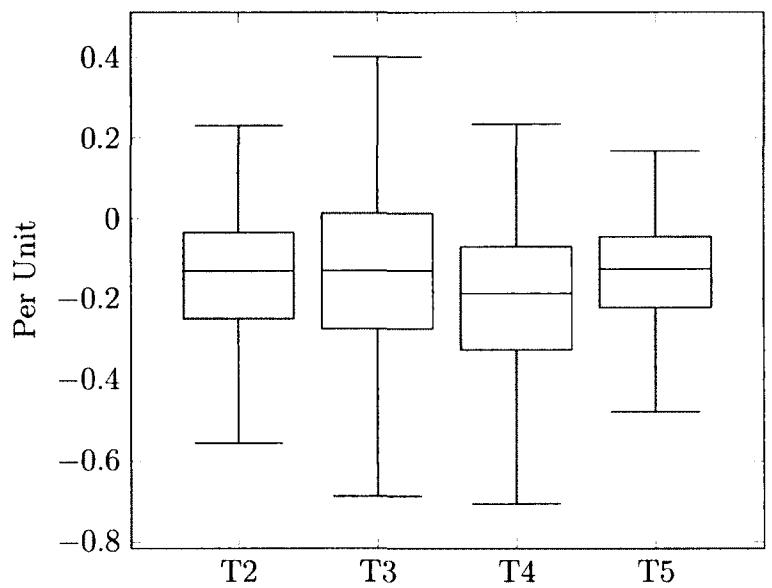

Figure A.3: Boxplot 5-Bus Angles, 500 Instances

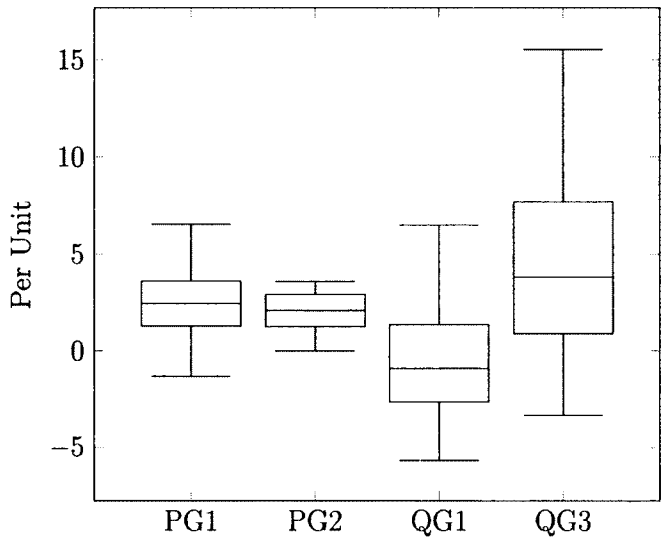

Figure A.4: Boxplot 5-Bus Real and Reactive Powers Generated, 500 Instances

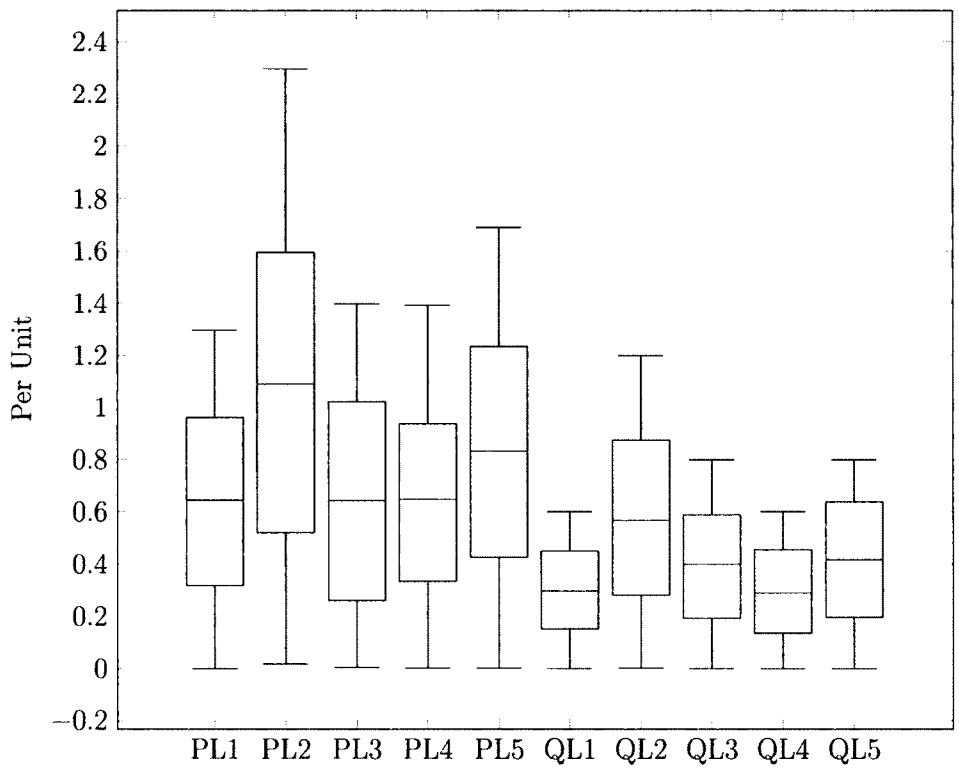

Figure A.5: Boxplot 5-Bus Real and Reactive Powers Consumed, 500 Instances

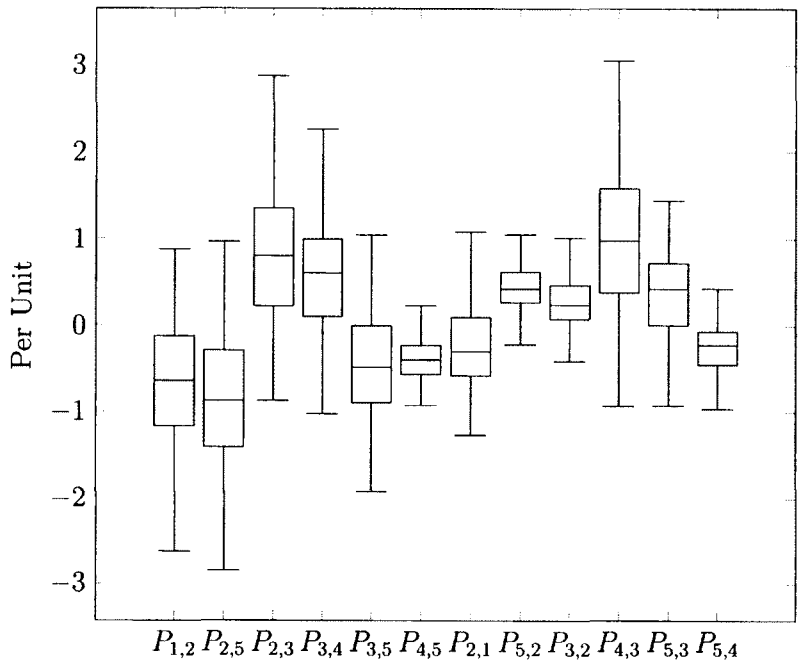

Figure A.6: Boxplot 5-Bus Real Powers Injected, 500 Instances

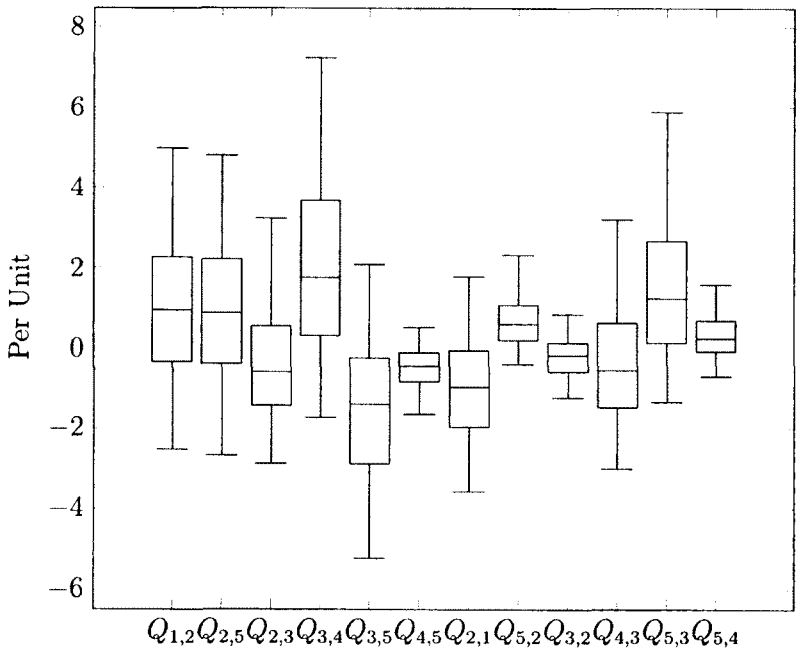

Figure A.7: Boxplot 5-Bus Reactive Powers Injected, 500 Instances

APPENDIX B

14-BUS POWER SYSTEM

B.1 System Details

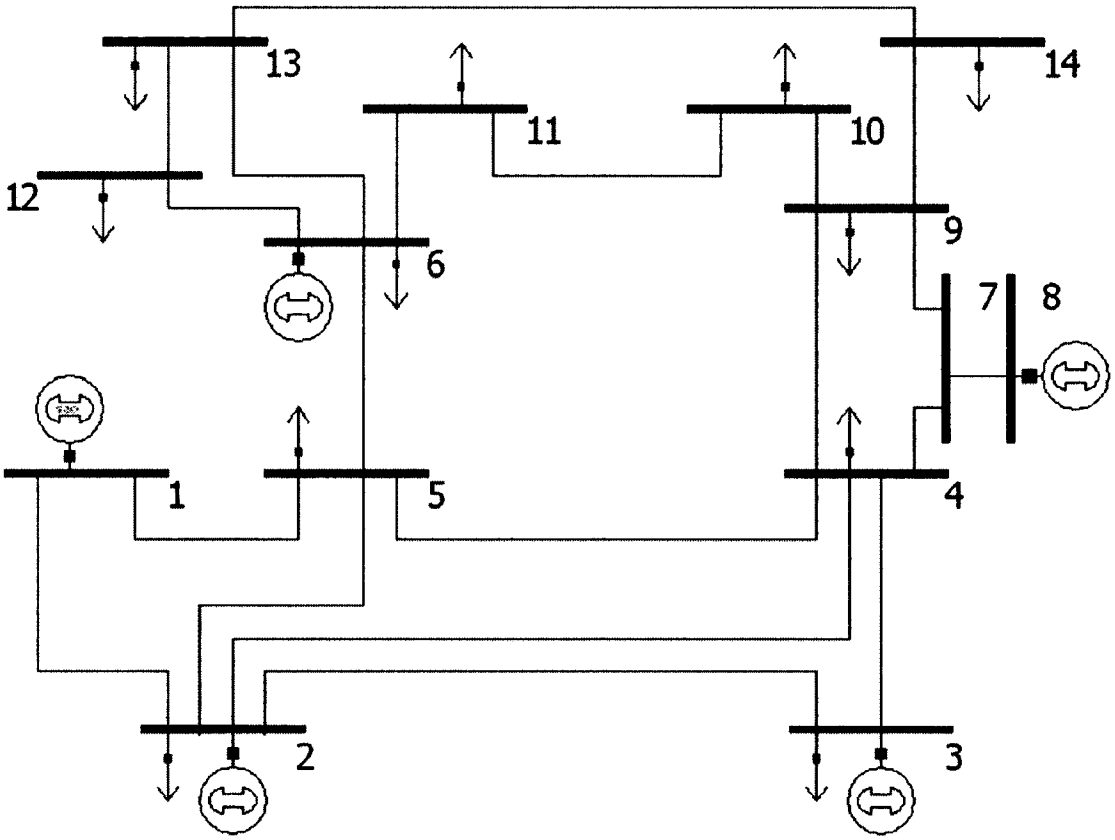

Figure B.1: 14-Bus One-line Diagram

Table B.1: 14-Bus Transmission Line Impedances

Line #	Bus - Bus	R	X	B
1	1 - 2	0.01938	0.05917	0.0528
2	1 - 5	0.05403	0.22304	0.0492
3	2 - 3	0.04699	0.19797	0.0438
4	2 - 4	0.05811	0.17632	0.0374
5	2 - 5	0.05695	0.17388	0.034
6	3 - 4	0.06701	0.17103	0.0346
7	4 - 5	0.01335	0.04211	0.0128
8	4 - 7	0	0.20912	0
9	4 - 9	0	0.55618	0
10	5 - 6	0	0.25202	0
11	6 - 11	0.09498	0.1989	0
12	6 - 12	0.12291	0.25581	0
13	6 - 13	0.06615	0.13027	0
14	7 - 8	0	0.17615	0
15	7 - 9	0	0.11001	0
16	9 - 10	0.03181	0.08450	0
17	9 - 14	0.12711	0.27038	0
18	10 - 11	0.08205	0.19207	0
19	12 - 13	0.22092	0.19988	0
20	13 - 14	0.17093	0.34802	0

B.2 Power Flow Simulation Snapshots

Table B.2: 14-Bus Input Snapshot

Bus #	Type	V	Delta	PG	QG	PL	QL
1	0	1.06	0	-	-	0	0
2	2	1.045	-	0.4	-	.217	0.127
3	2	1.01	-	0	.0234	.942	0.190
4	1	-	-	0	0	.478	-0.039
5	1	-	-	0	0	.076	0.016
6	2	1.07	-	0	.0122	.112	0.0750
7	1	-	-	0	0	0	0
8	2	1.09	-	0	0	0	0
9	1	-	-	0	.0174	0.2950	0.1660
10	1	-	-	0	0	0.0900	0.0580
11	1	-	-	0	0	0.0350	0.0180
12	1	-	-	0	0	0.0610	0.0160
13	1	-	-	0	0	0.1350	0.0580
14	1	-	-	0	0	0.1490	0.0500

Table B.3: 14-Bus Output (**Bold**) Snapshot

Bus #	Type	V	Delta	PG	QG	PL	QL
1	0	1.06	0	**2.324**	**-0.236**	0	0
2	2	1.045	**-4.951**	0.4	**-0.270**	.217	0.127
3	2	1.01	**-12.61**	0	.0234	.942	0.190
4	1	**1.0296**	**-10.41**	0	0	.478	-0.039
5	1	**1.0351**	**-8.963**	0	0	.076	0.016
6	2	1.07	**-14.72**	0	.0122	.112	0.0750
7	1	**1.0536**	**-13.54**	0	0	0	0
8	2	1.09	**-13.54**	0	0	0	0
9	1	**1.0447**	**-15.15**	0	.0174	0.2950	0.1660
10	1	**1.0417**	**-15.36**	0	0	0.0900	0.0580
11	1	**1.0522**	**-15.17**	0	0	0.0350	0.0180
12	1	**1.0543**	**-15.57**	0	0	0.0610	0.0160
13	1	**1.0487**	**-15.62**	0	0	0.1350	0.0580
14	1	**1.0283**	**-16.37**	0	0	0.1490	0.0500

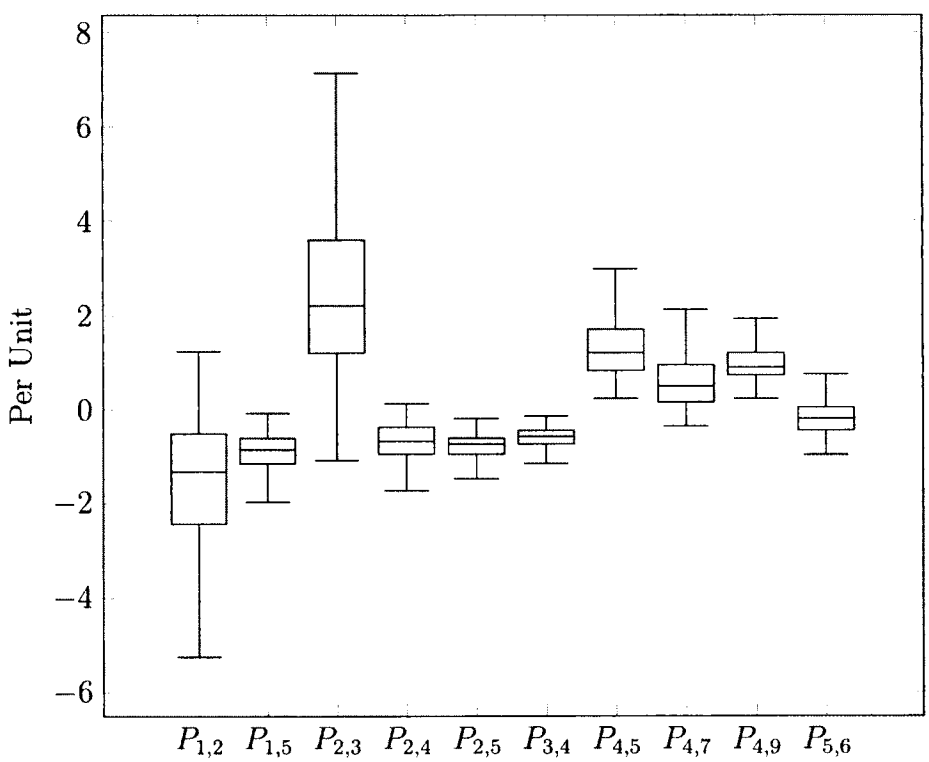

Figure B.7: 14-Bus Real Powers Injected, 500 Instances

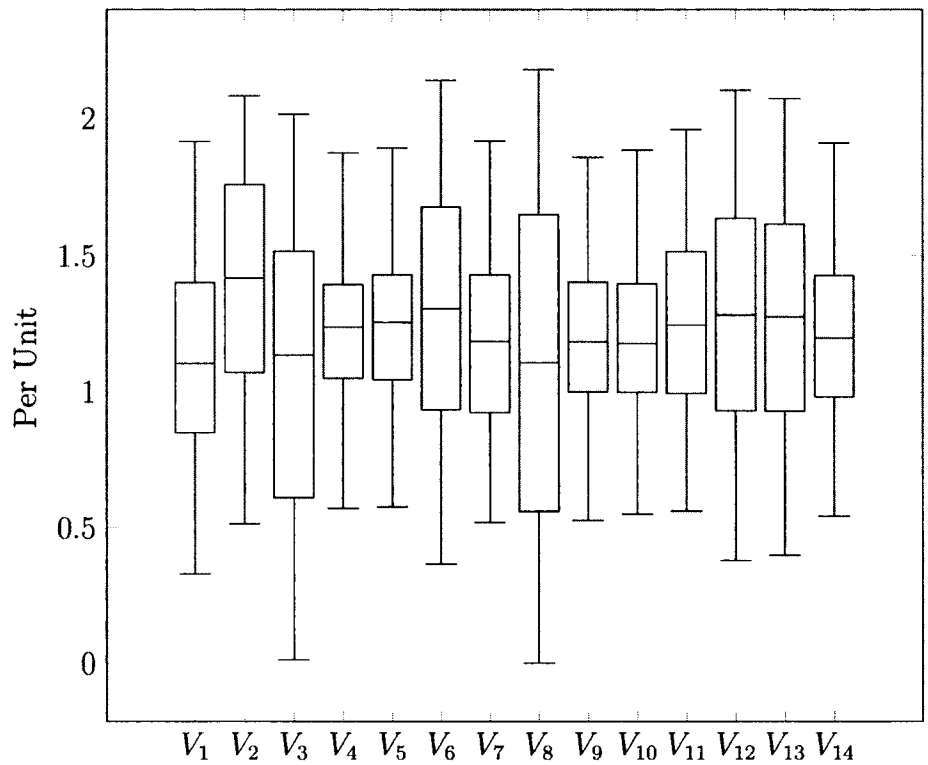

Figure B.2: Boxplot 14-Bus Voltages, 500 Instances

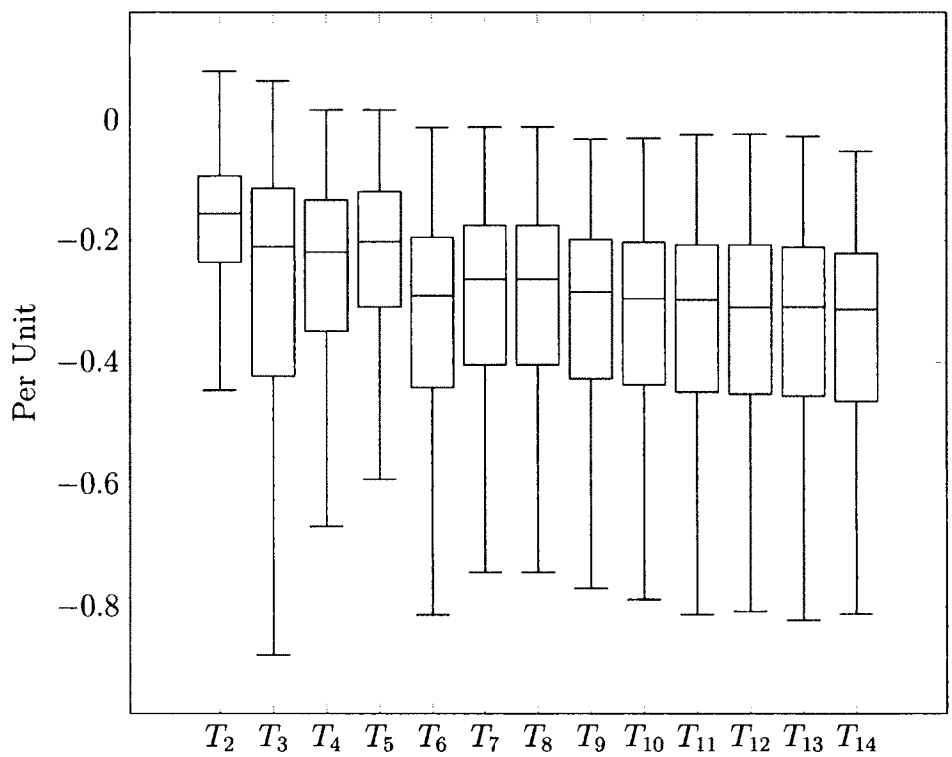

Figure B.3: Boxplot 14-Bus Angles, 500 Instances

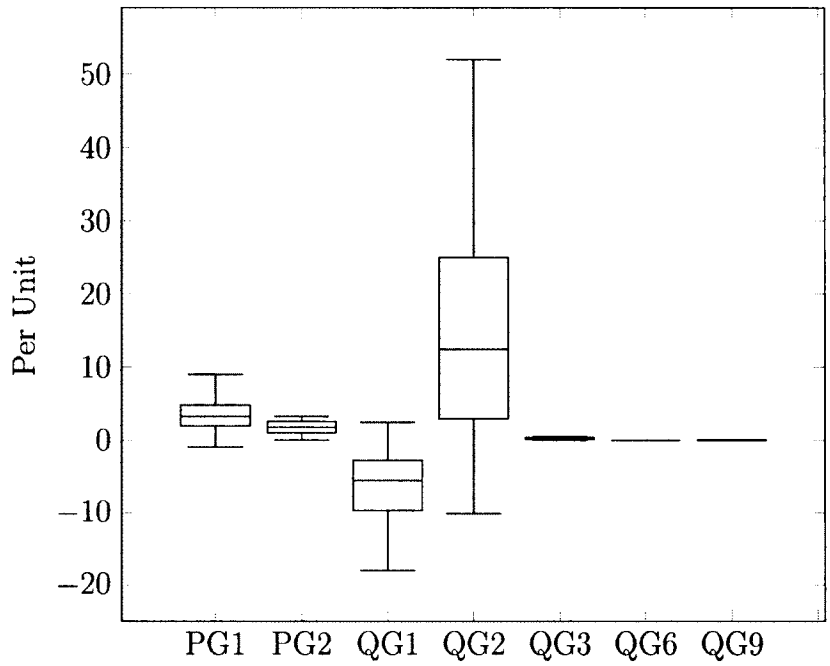

Figure B.4: Boxplot 14-Bus Real and Reactive Powers Generated, 500 Instances

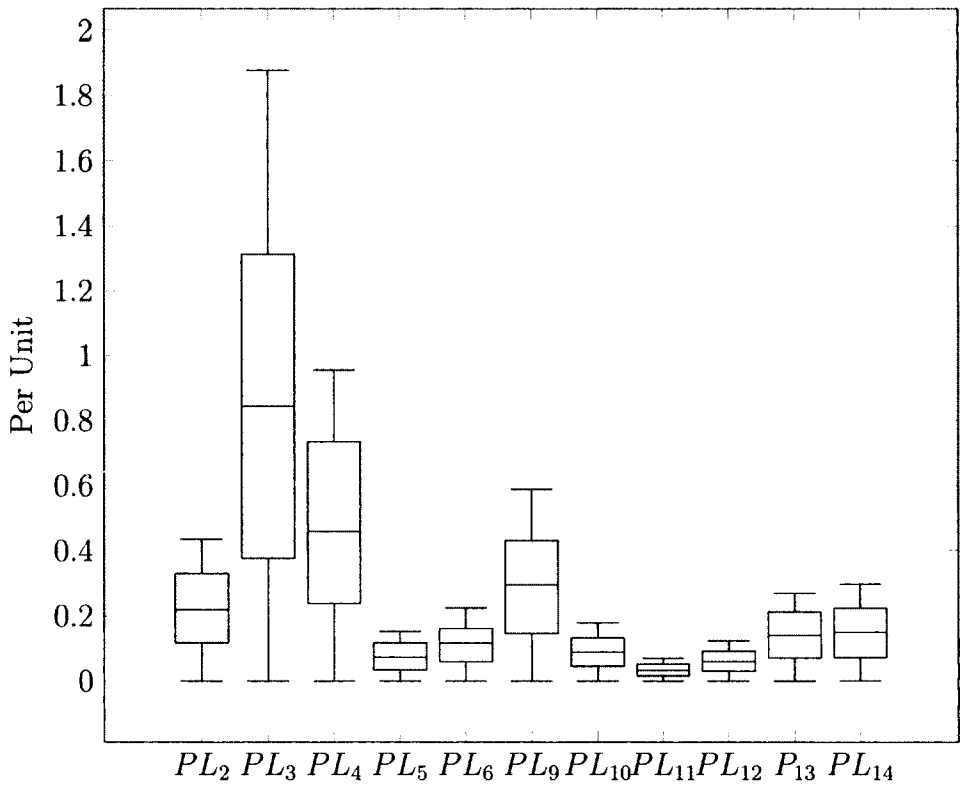

Figure B.5: Boxplot 14-Bus Real Power Consumed, 500 Instances

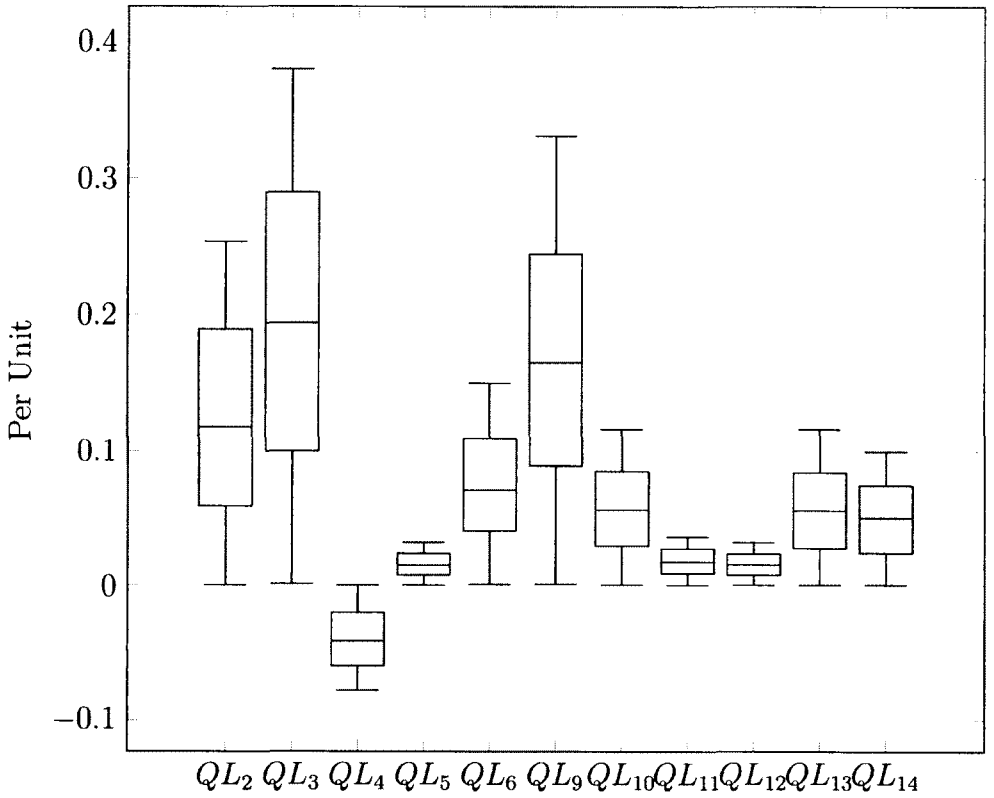

Figure B.6: Boxplot 14-Bus Reactive Powers Consumed, 500 Instances

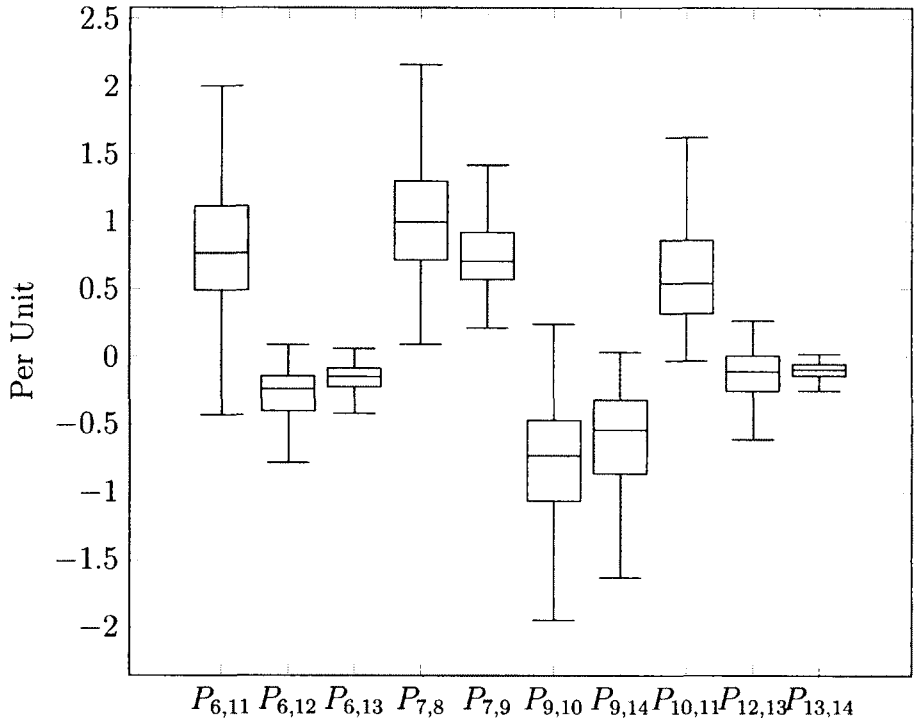

Figure B.8: 14-Bus Real Powers Injected, 500 Instances

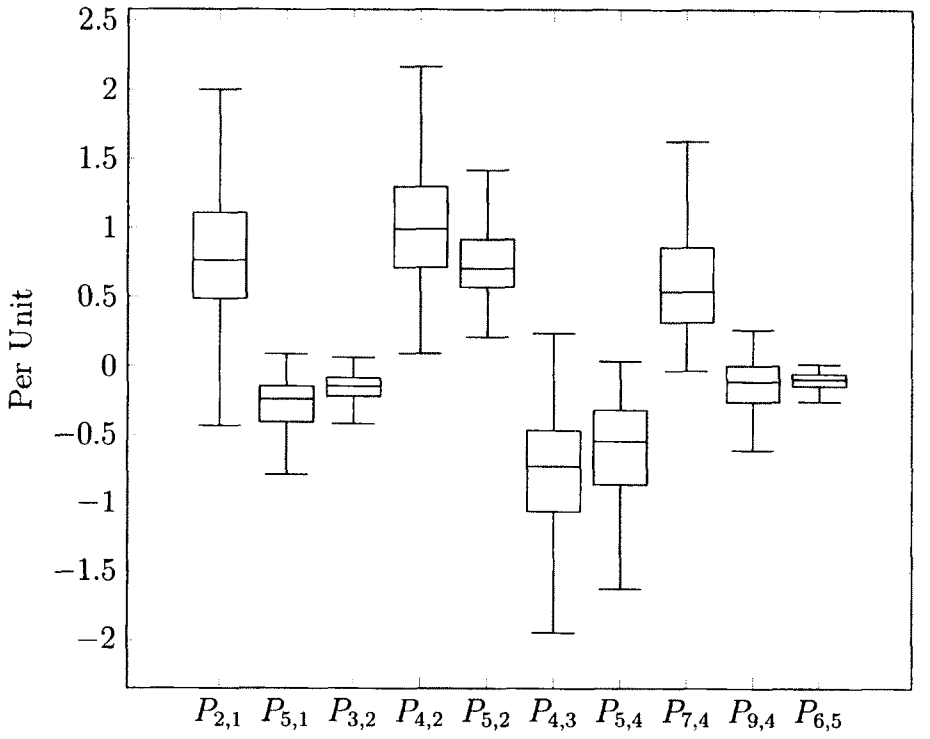

Figure B.9: 14-Bus Real Powers Injected, 500 Instances

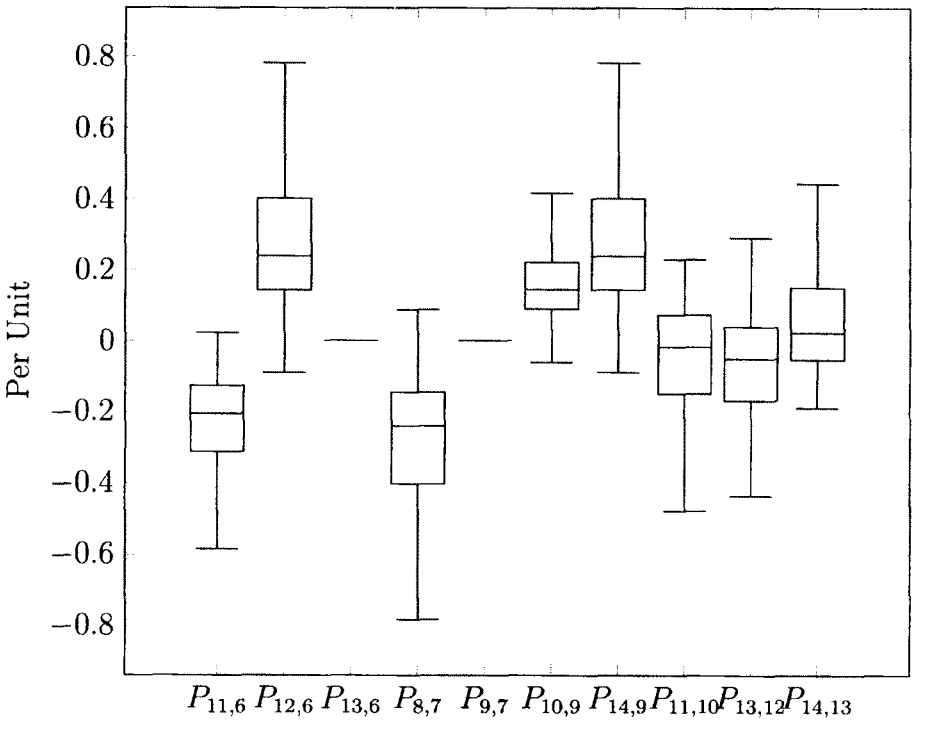

Figure B.10: 14-Bus Real Powers Injected, 500 Instances

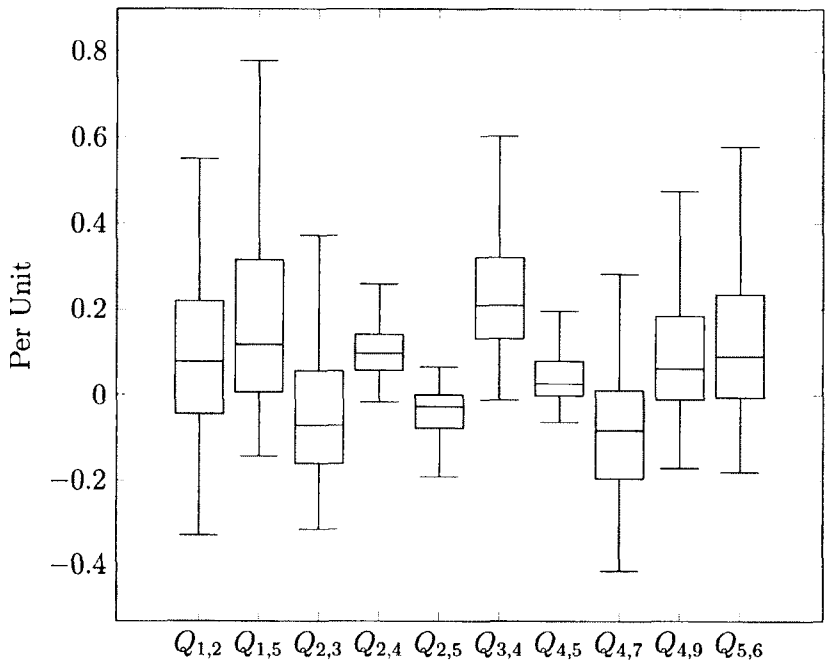

Figure B.11: 14-Bus Reactive Powers Injected, 500 Instances

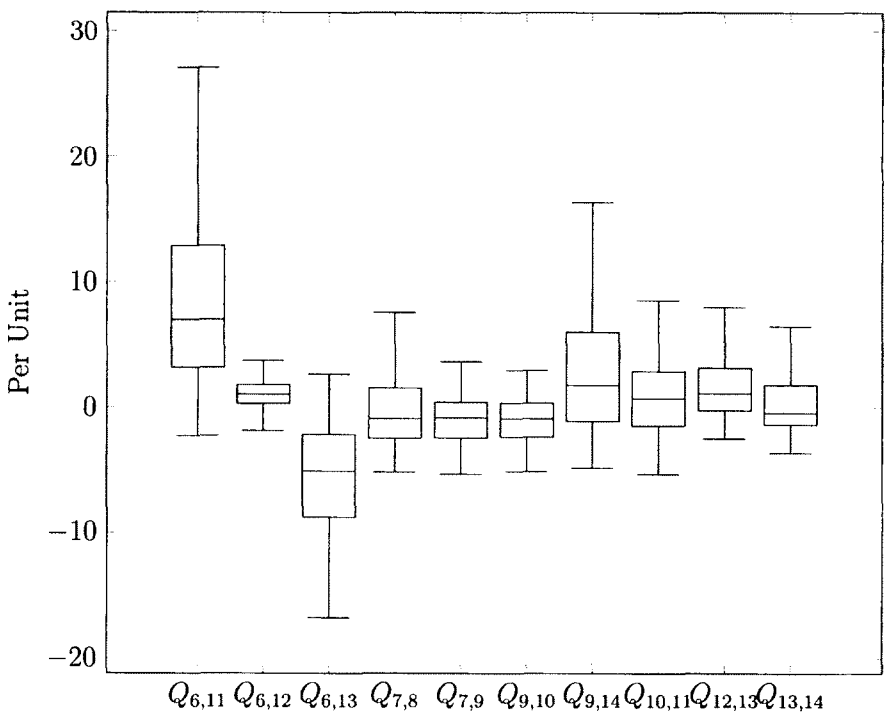

Figure B.12: 14-Bus Reactive Powers Injected, 500 Instances

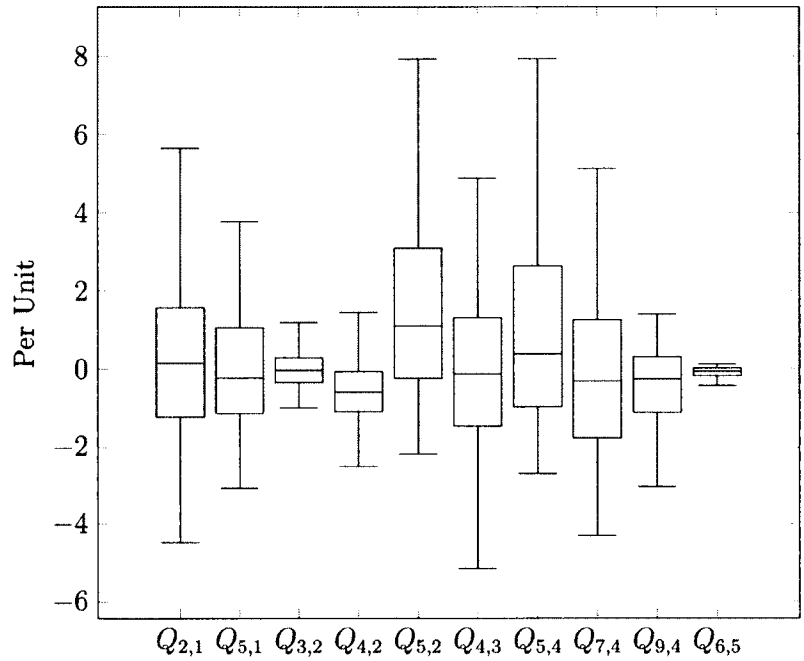

Figure B.13: 14-Bus Reactive Powers Injected, 500 Instances

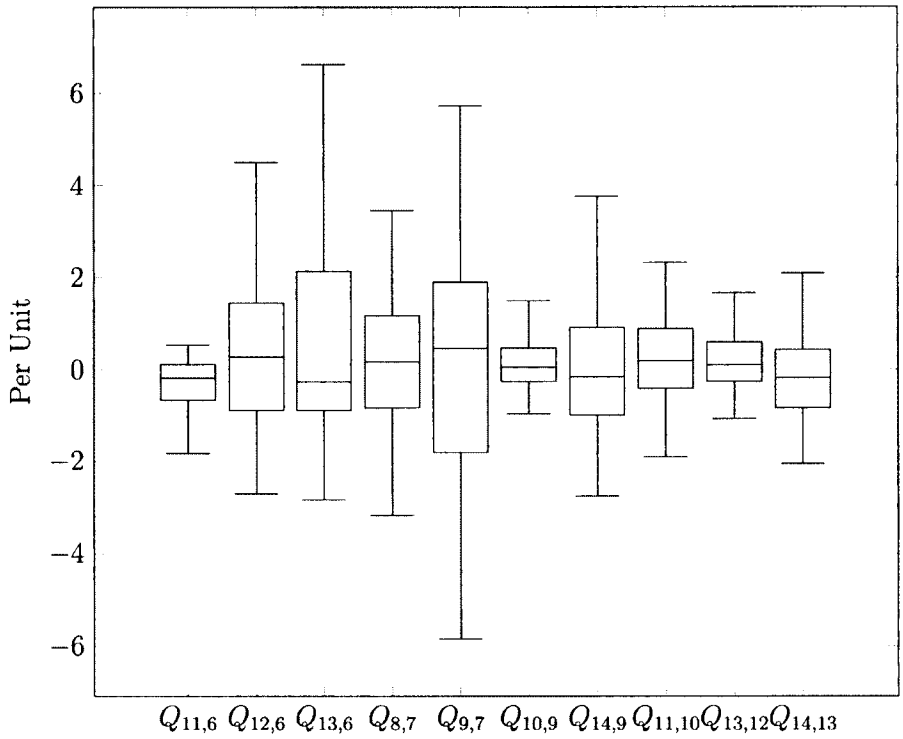

Figure B.14: 14-Bus Reactive Powers Injected, 500 Instances

APPENDIX C

PRINCIPAL COMPONENT ANALYSIS DIMENSIONAL TRANSFORMATIONS

C.1 5-Bus Transformation

C.1.1 Without Line Flows

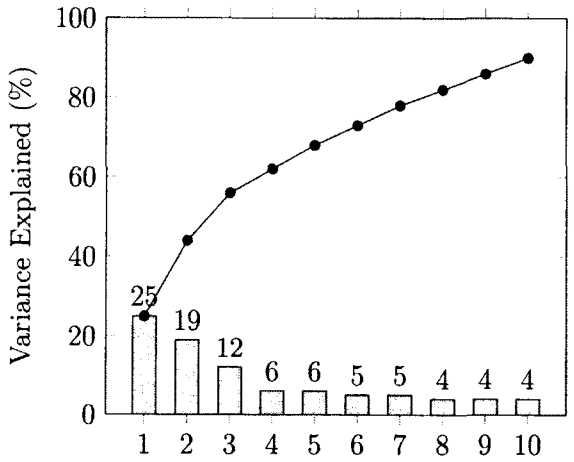

Figure C.1: PCA Scree Plot of 500 5-Bus Instances Without Line Flows

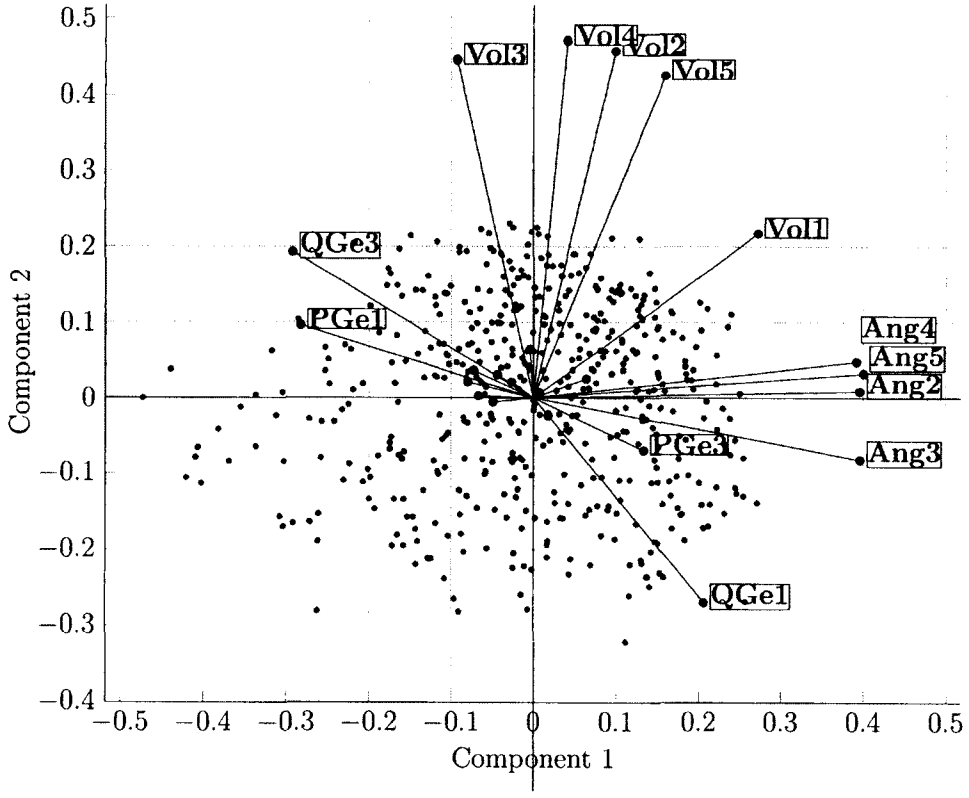

Figure C.2: 500 5-Bus Scores and Feature Vectors Transformed

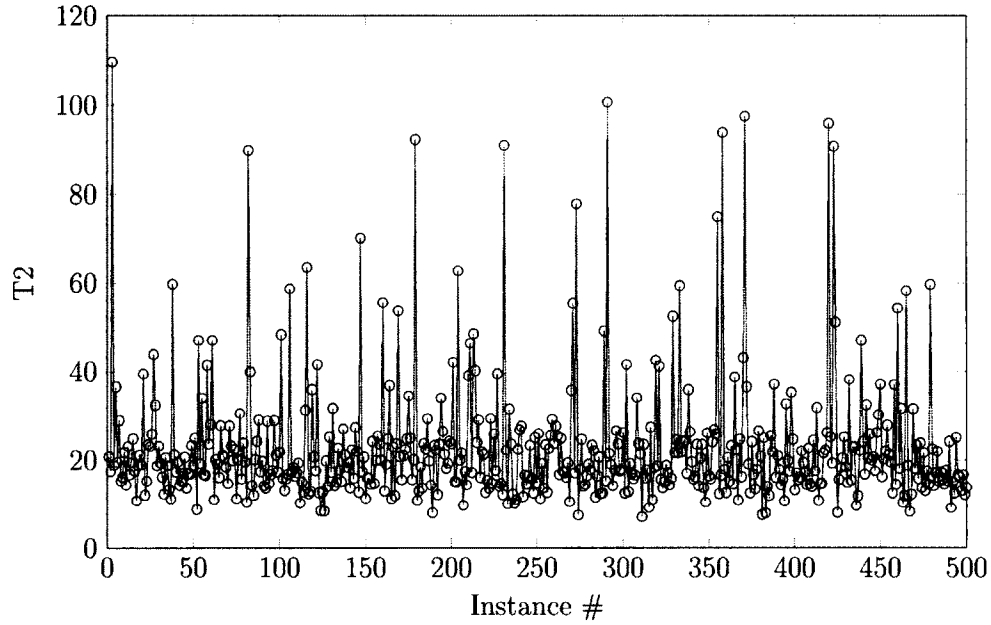

Figure C.3: Hotelling T^2 of 500 5-Bus Instances Without Line Flows

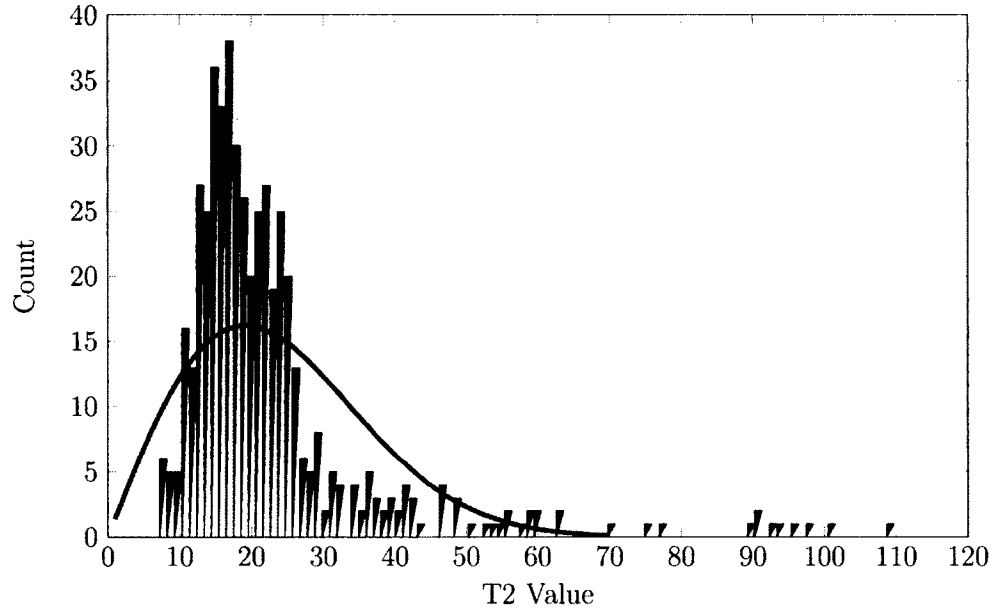

Figure C.4: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows

C.1.2 With Line Flows

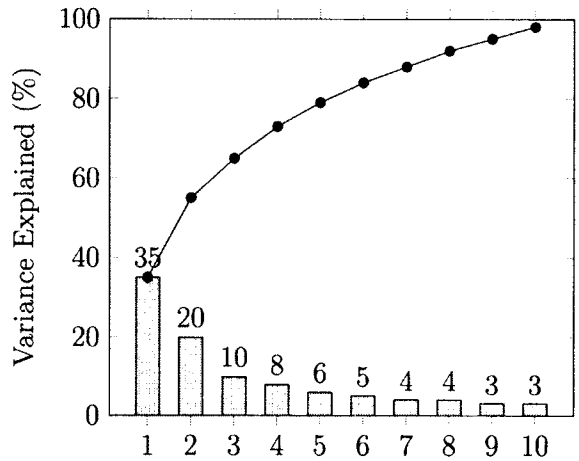

Figure C.5: PCA Scree Plot

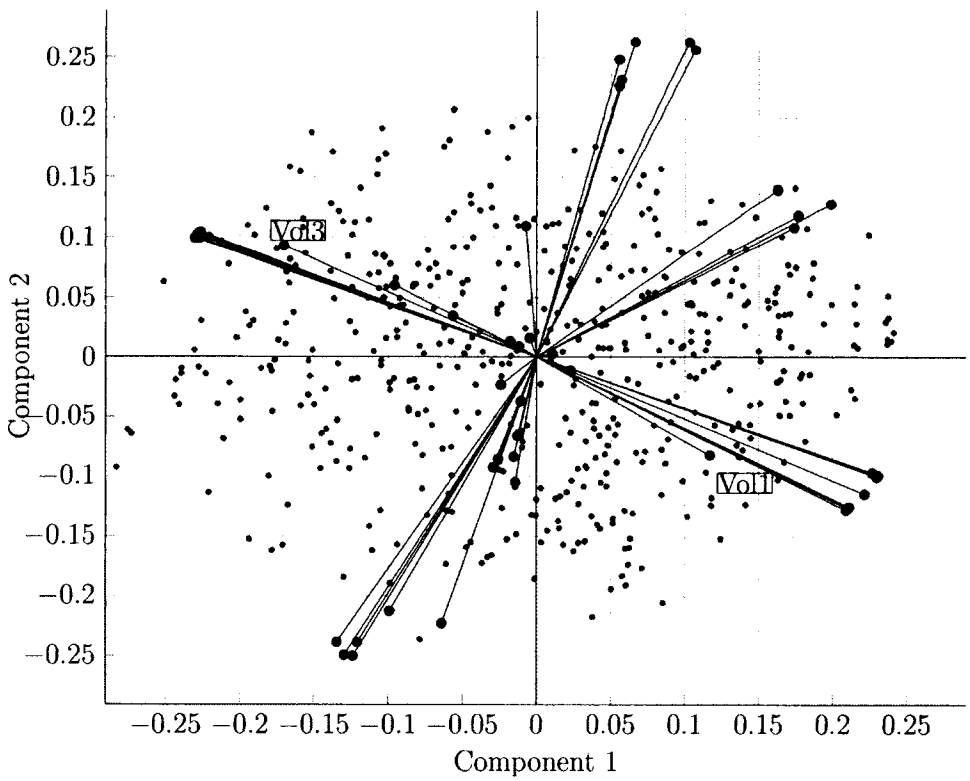

Figure C.6: Scores and Feature Vectors Transformed

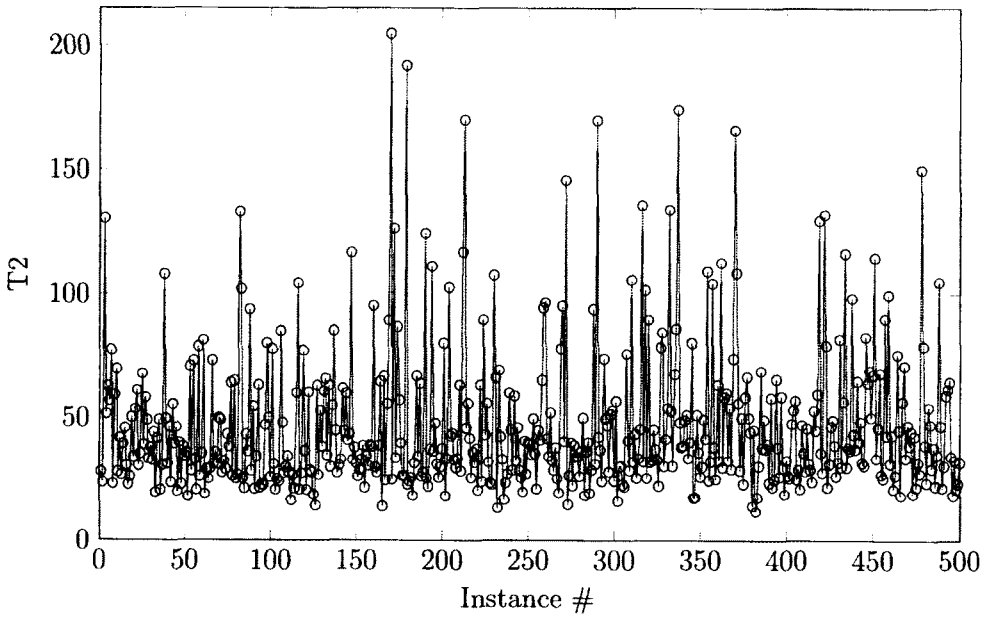

Figure C.7: Hotelling T^2 of 500 5-Bus Instances With Line Flows

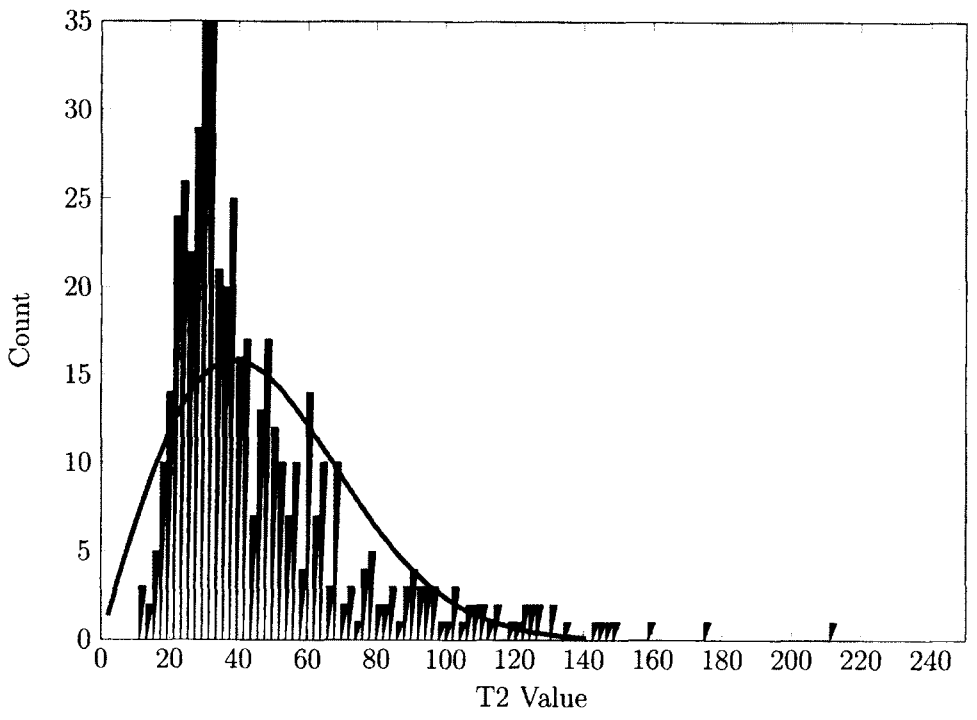

Figure C.8: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances With Line Flows

C.2 IEEE 14-Bus Transformation

C.2.1 Without Line Flows

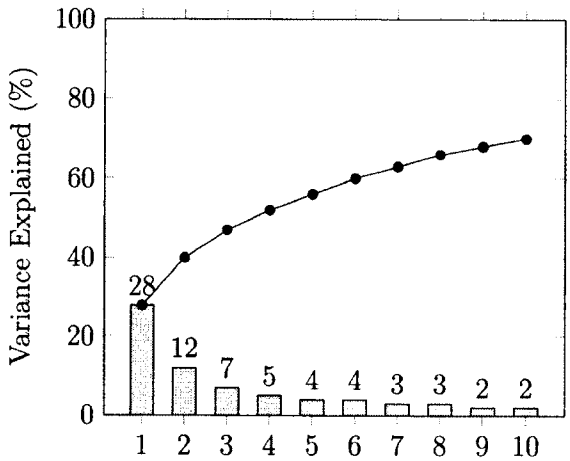

Figure C.9: PCA Scree Plot of 500 14-Bus Instances Without Line Flows

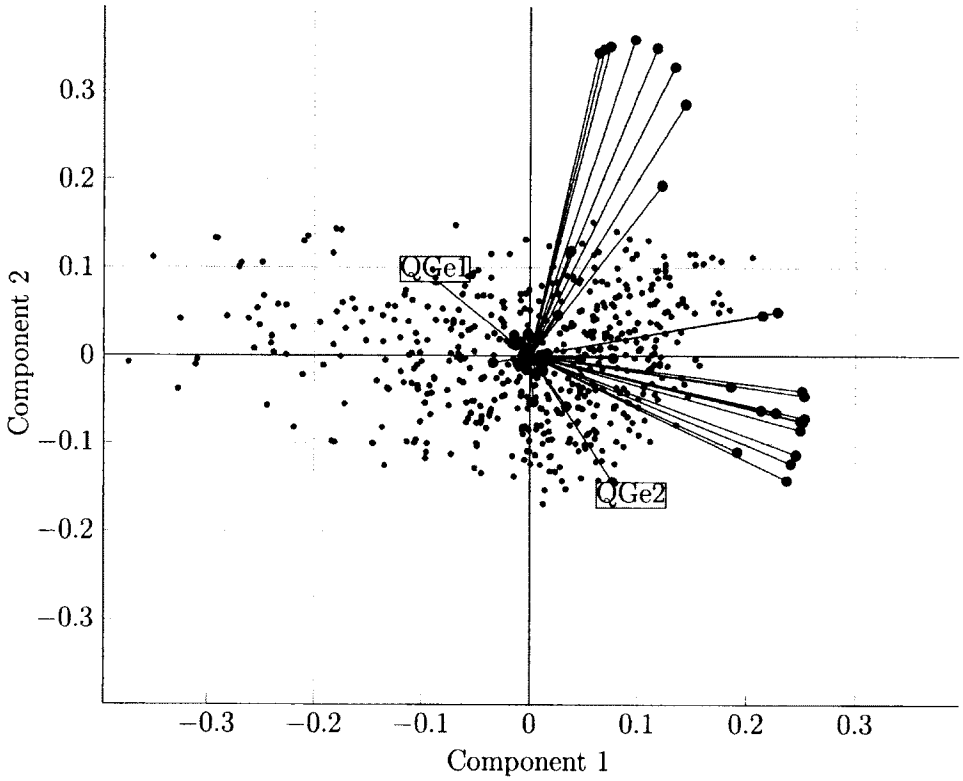

Figure C.10: 500 14-Bus Scores and Feature Vectors Transformed

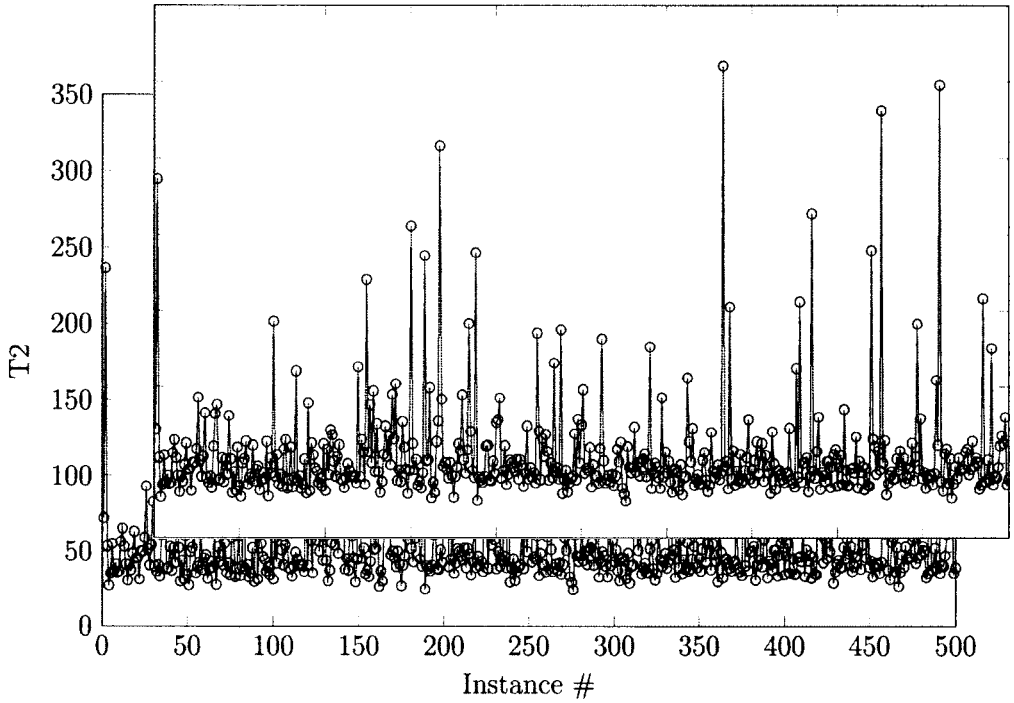

Figure C.11: Hotelling T^2 of 500 14-Bus Instances Without Line Flows

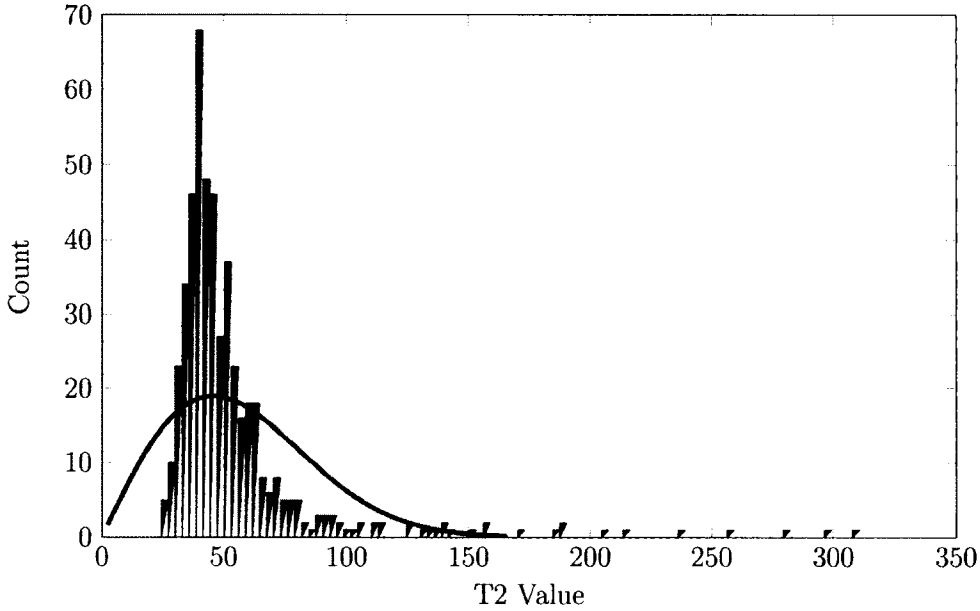

Figure C.12: Histogram and Rayleigh Curve Fit of T^2 values for 500 5-Bus Instances Without Line Flows

C.2.2 With Line Flows

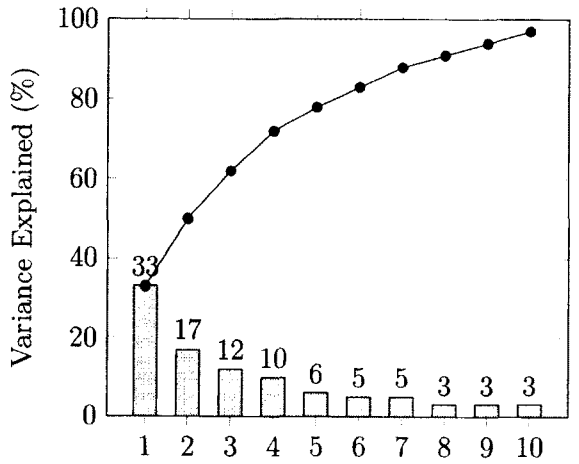

Figure C.13: PCA Scree Plot of 500 14-Bus Instances With Line Flows

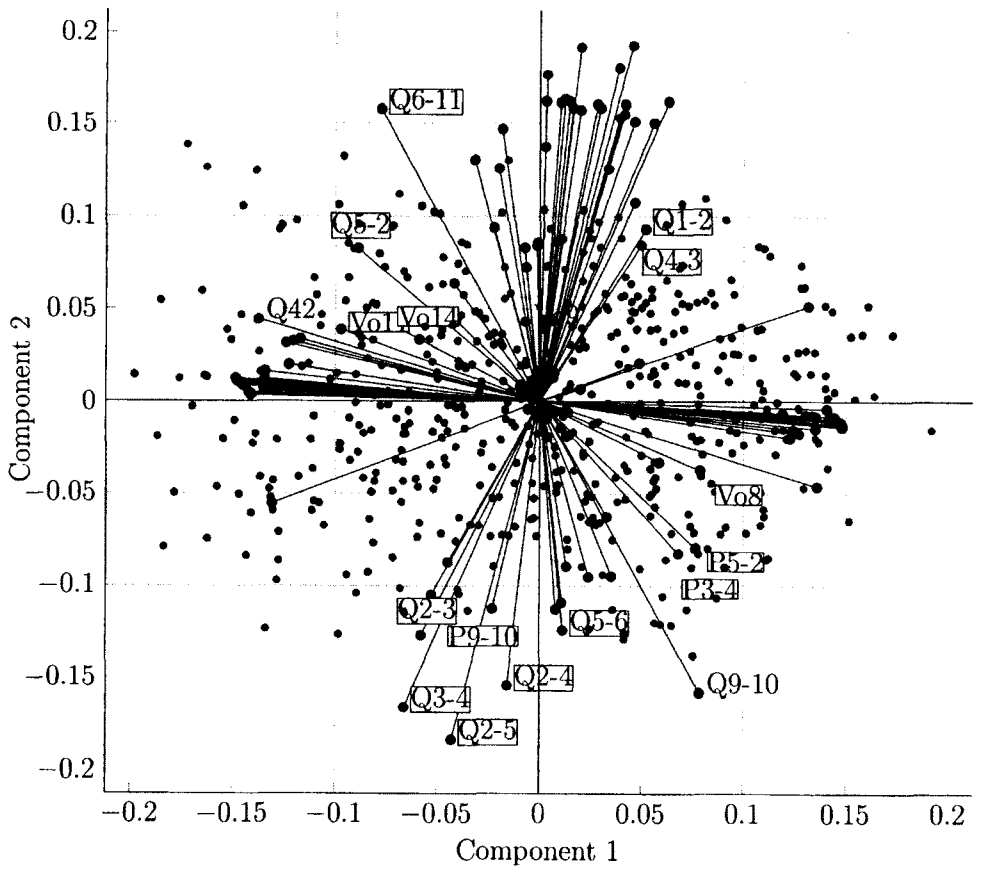

Figure C.14: 500 14-Bus Scores and Feature Vectors Transformed

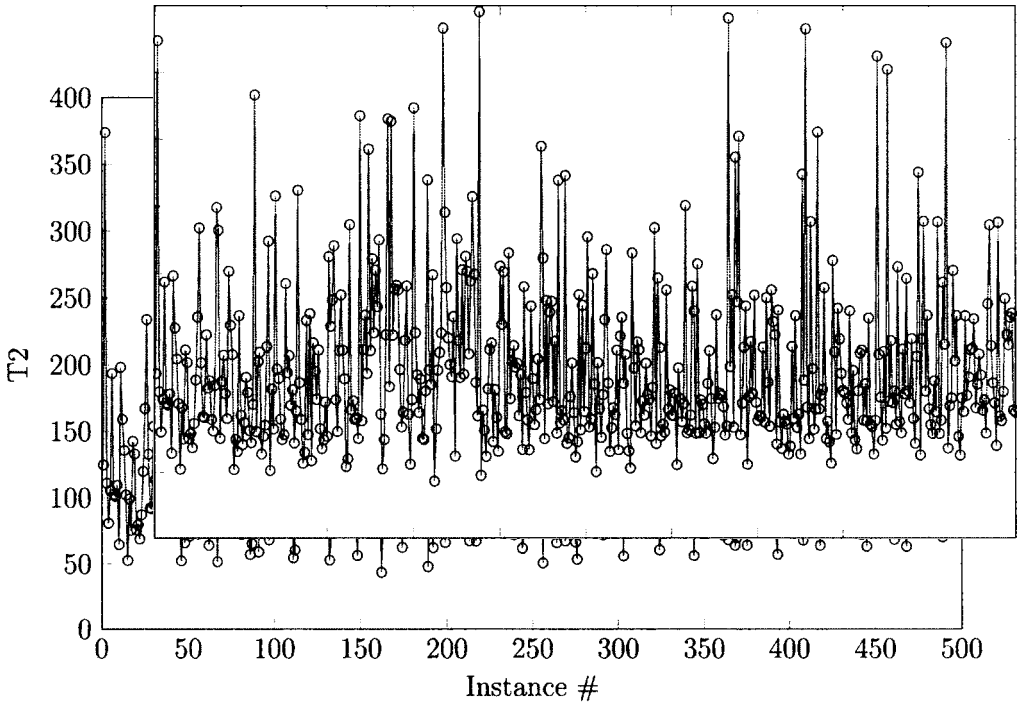

Figure C.15: Hotelling T^2 of 500 14-Bus Instances With Line Flows

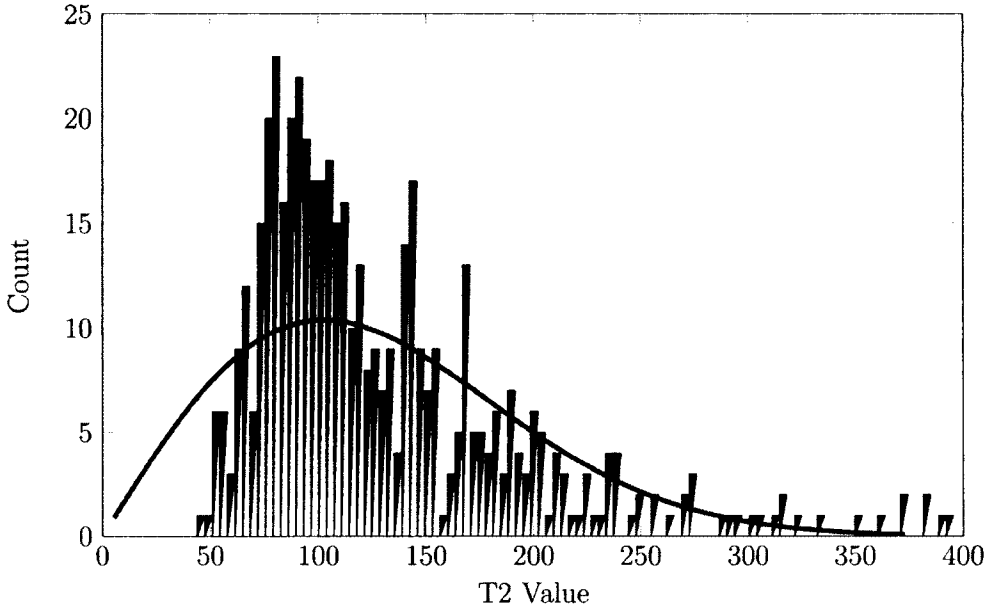

Figure C.16: Histogram and Rayleigh Curve Fit of T^2 values for 500 IEEE 14-Bus Instances With Line Flows

APPENDIX D

CYBER-EVENT IDENTIFICATION PLOTS AND TABLES

D.1 5-Bus Identification

D.1.1 Without Line Flows

Single variate Type I Attack (SI)

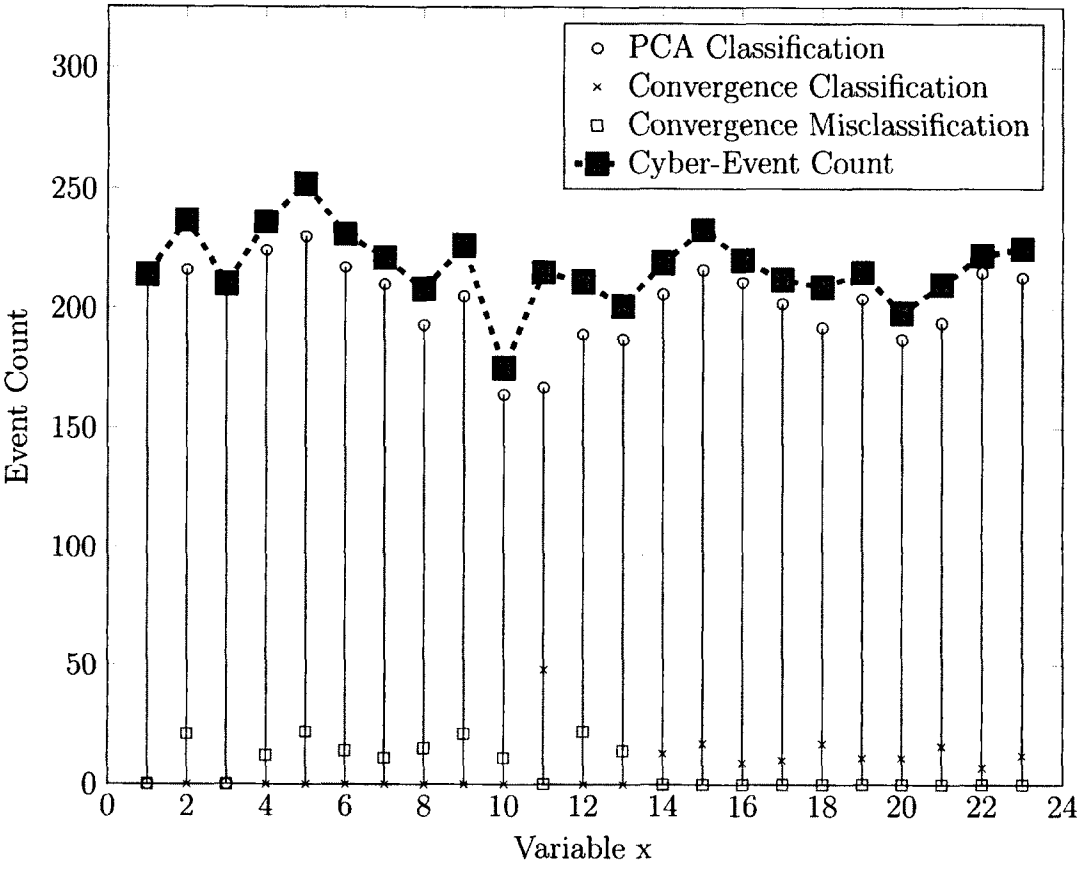

Figure D.1: 5-Bus Without Line Flows SI Classification Results

Table D.1: 5-Bus Without Line Flows SI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
163	595	0	4242
Total Number of Simulated Malicious Instances = 5,000			
Total Number of Simulated Cyber-Events = 5,000			

Single variate Type II Attack (SII)

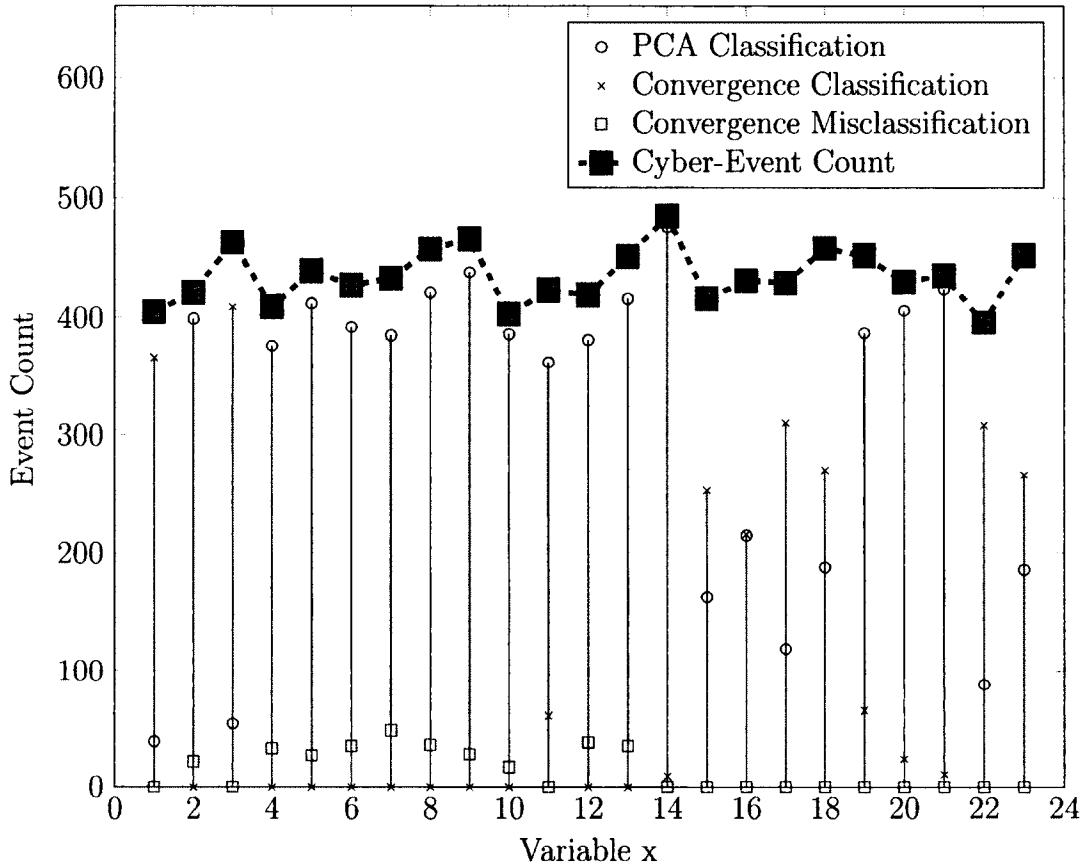

Figure D.2: 5-Bus Without Line Flows SII Classification Results

Table D.2: 5-Bus Without Line Flows SII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
319	2568	0	7113
Total Number of Simulated Malicious Instances = 10,000			
Total Number of Simulated Cyber-Events = 10,000			

Multivariate Type I Attack (MI)

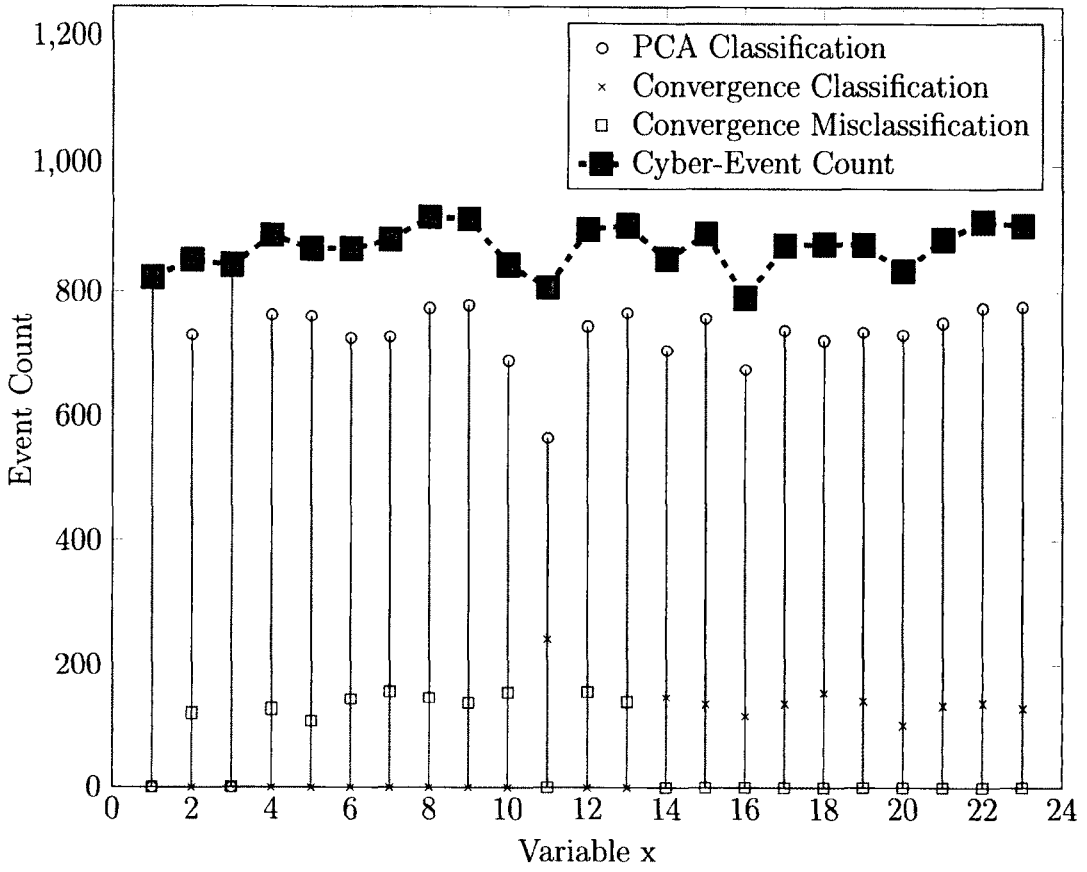

Figure D.3: 5-Bus Without Line Flows MI Classification Results

Table D.3: 5-Bus Without Line Flows MI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
1373	3225	0	15402
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

Multivariate Type II Attack (MII)

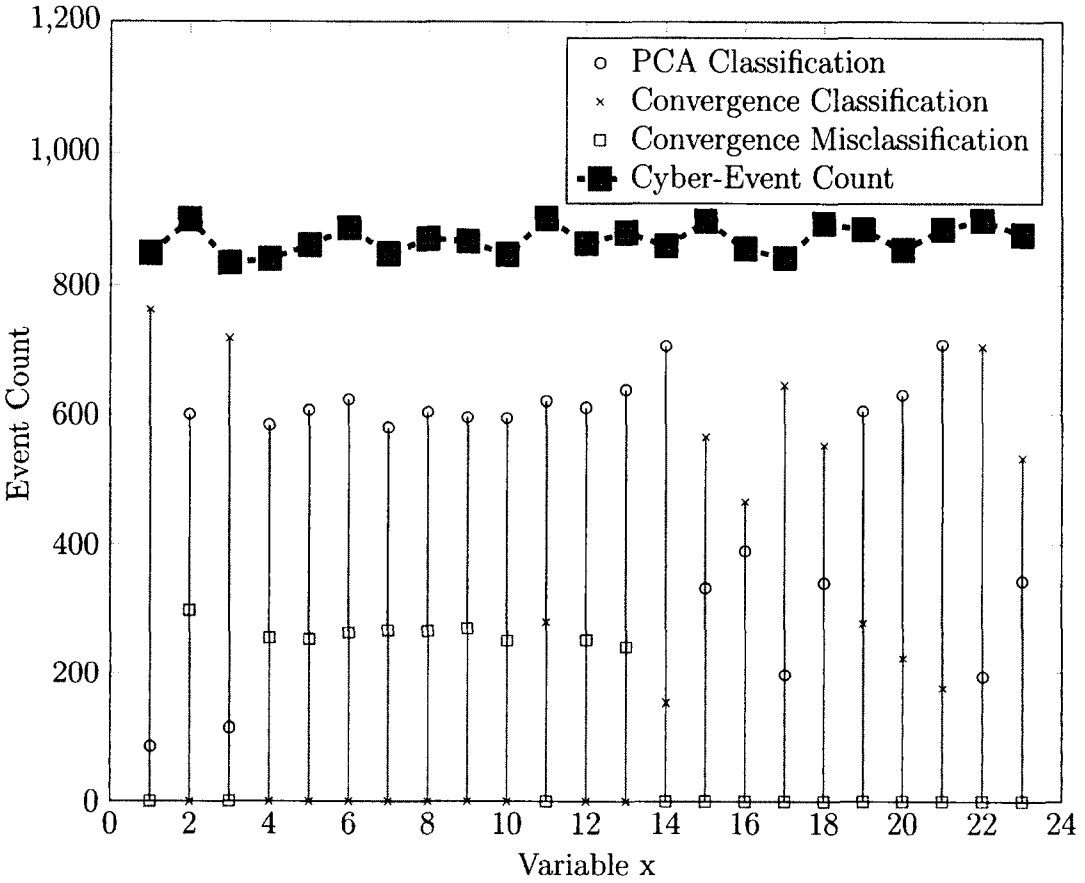

Figure D.4: 5-Bus Without Line Flows MII Classification Results

Table D.4: 5-Bus Without Line Flows MII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
2626	6062	0	11312
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

D.1.2 With Line Flows

Single variate Type I Attack (SI)

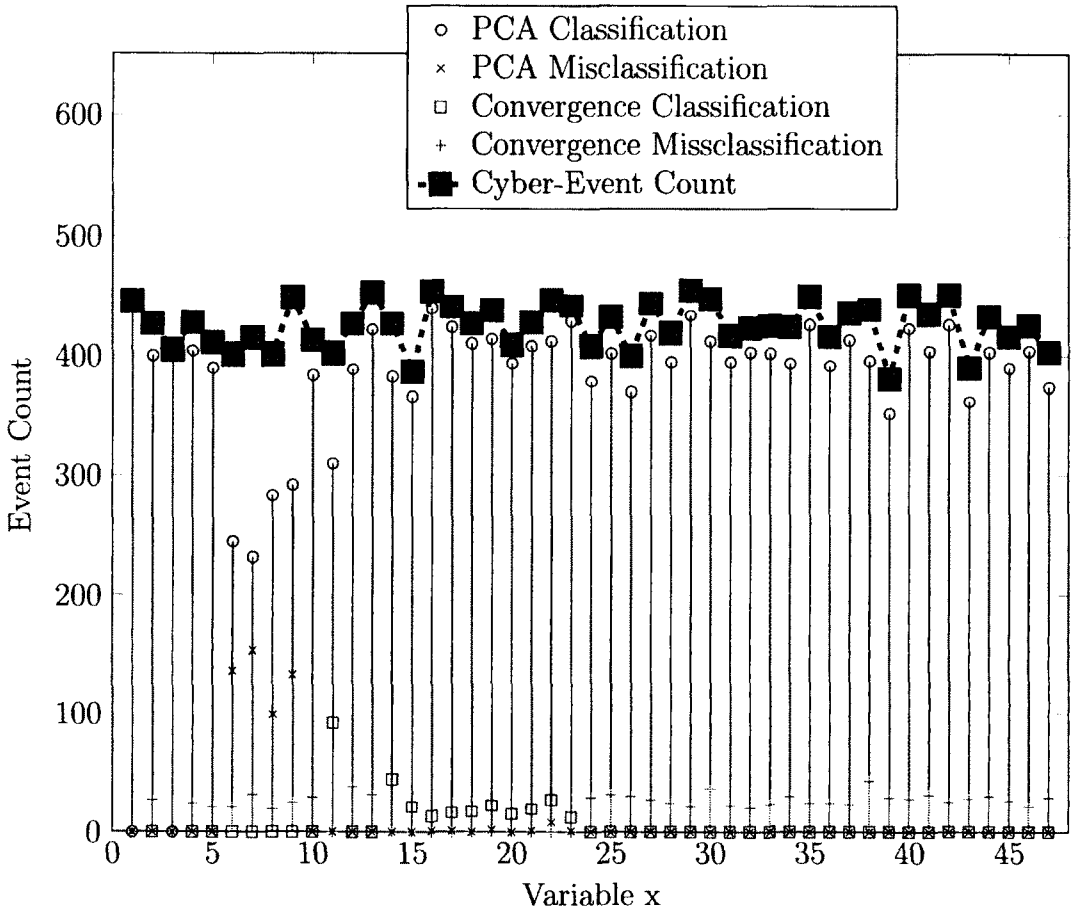

Figure D.5: 5-Bus With Line Flows SI Classification Results

Table D.5: 5-Bus With Line Flows SI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
920	1149	532	17399
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Single variate Type II Attack (SII)

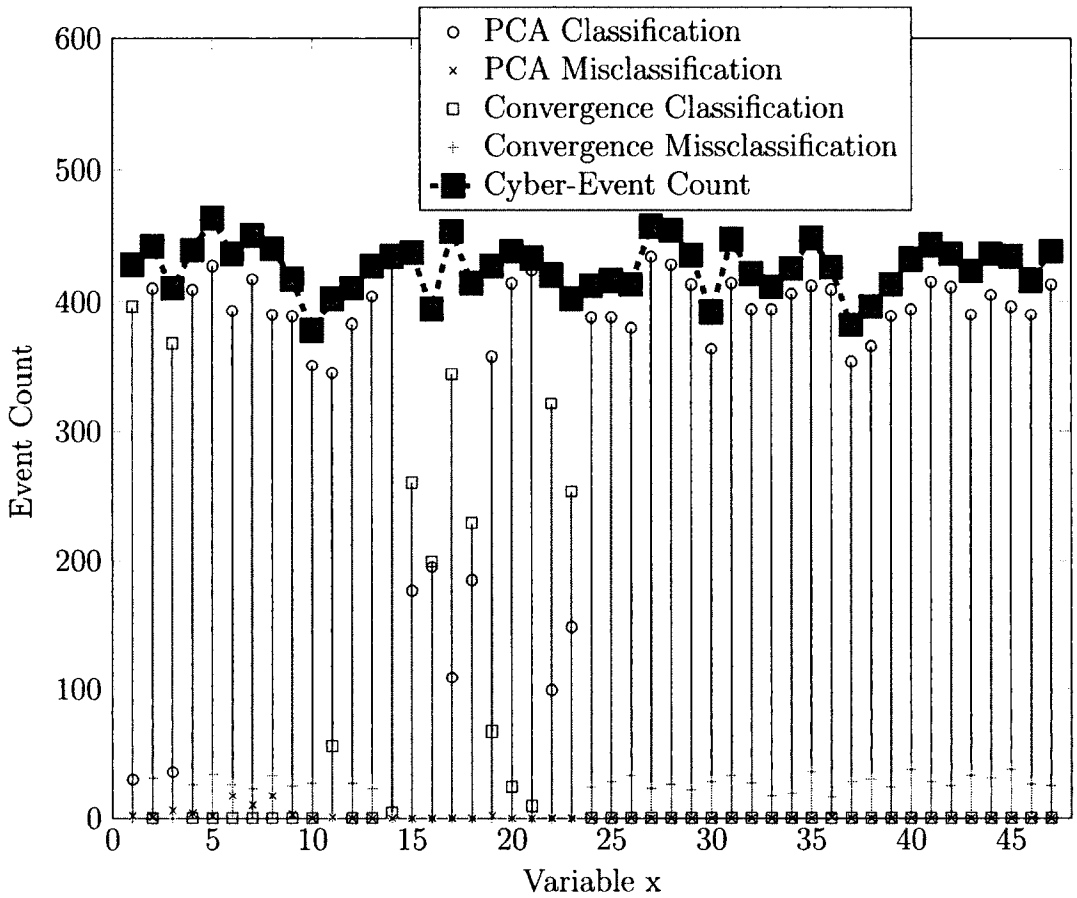

Figure D.6: 5-Bus With Line Flows SII Classification Results

Table D.6: 5-Bus With Line Flows SII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
933	2530	66	16471
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Multivariate Type I Attack (MI)

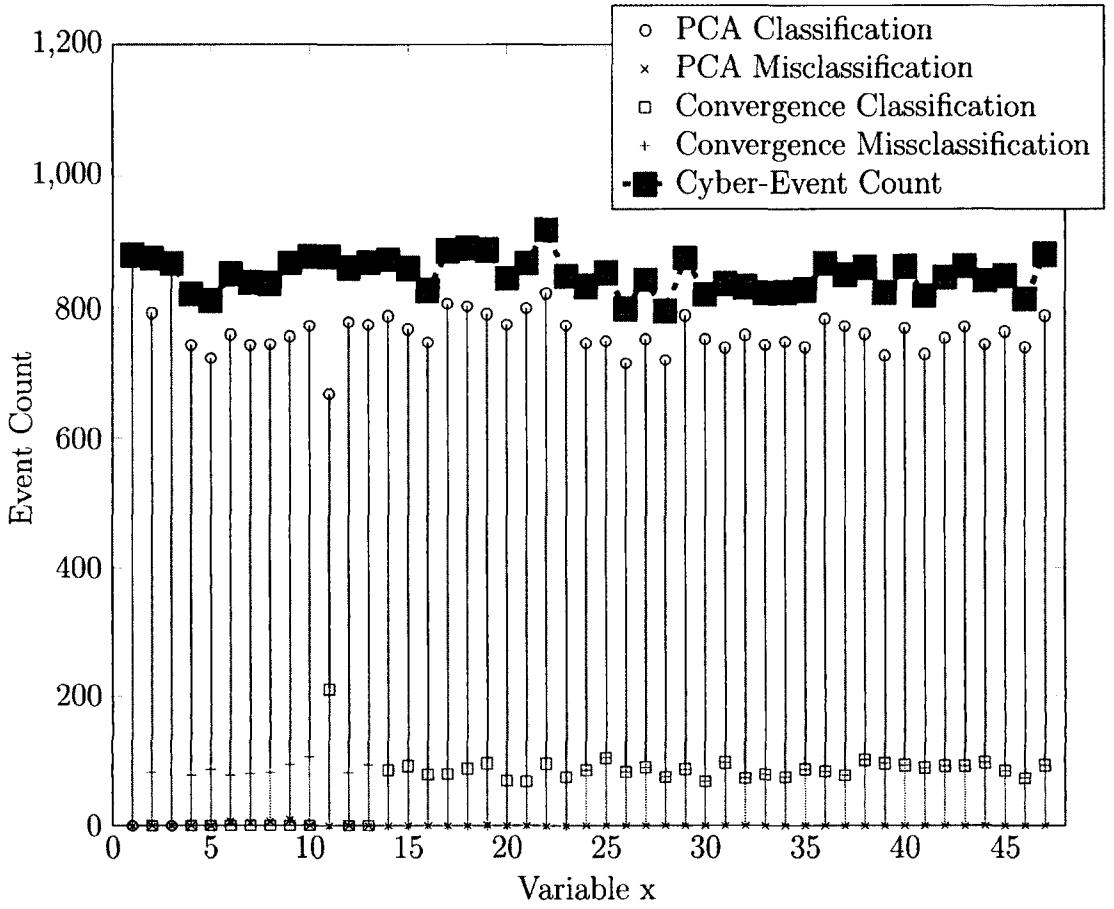

Figure D.7: 5-Bus With Line Flows MI Classification Results

Table D.7: 5-Bus With Line Flows MI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
1509	1355	29	34214
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

Multivariate Type II Attack (MII)

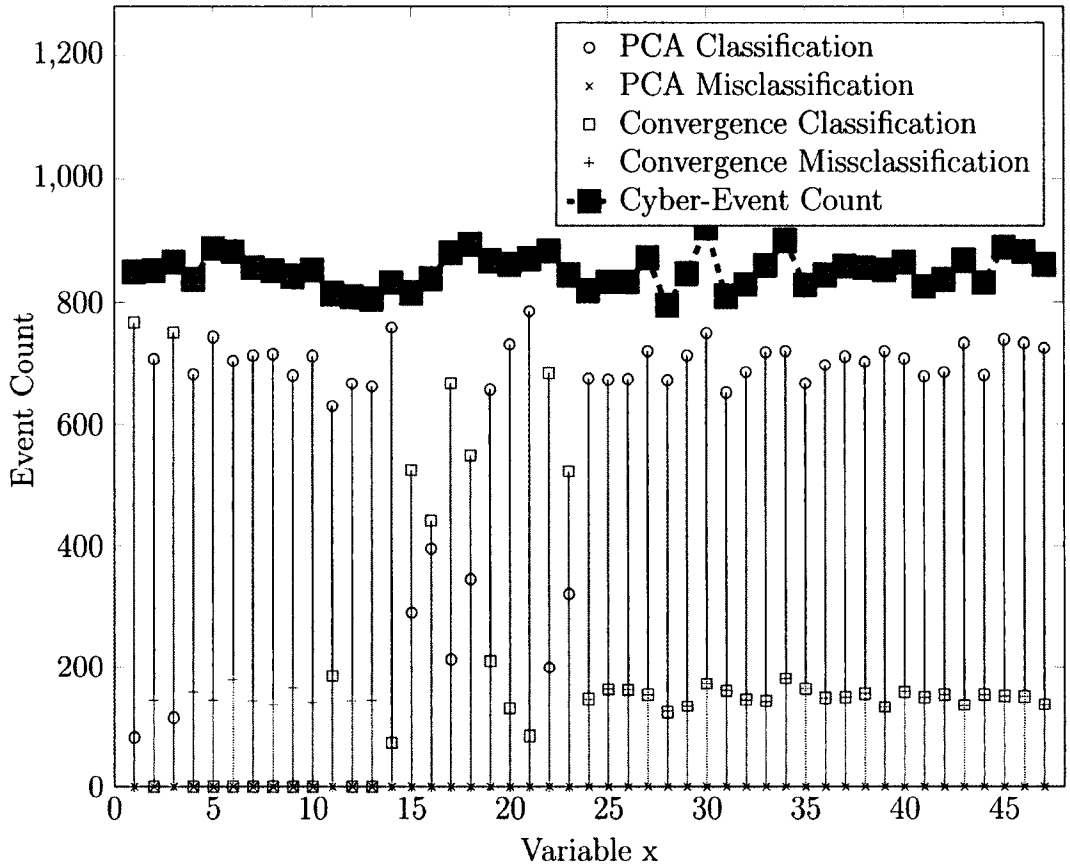

Figure D.8: 5-Bus With Line Flows MII Classification Results

Table D.8: 5-Bus With Line Flows MII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
5050	9157	0	29,362
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

D.2 IEEE 14-Bus Identification

D.2.1 Without Line Flows

Single variate Type I Attack (SI)

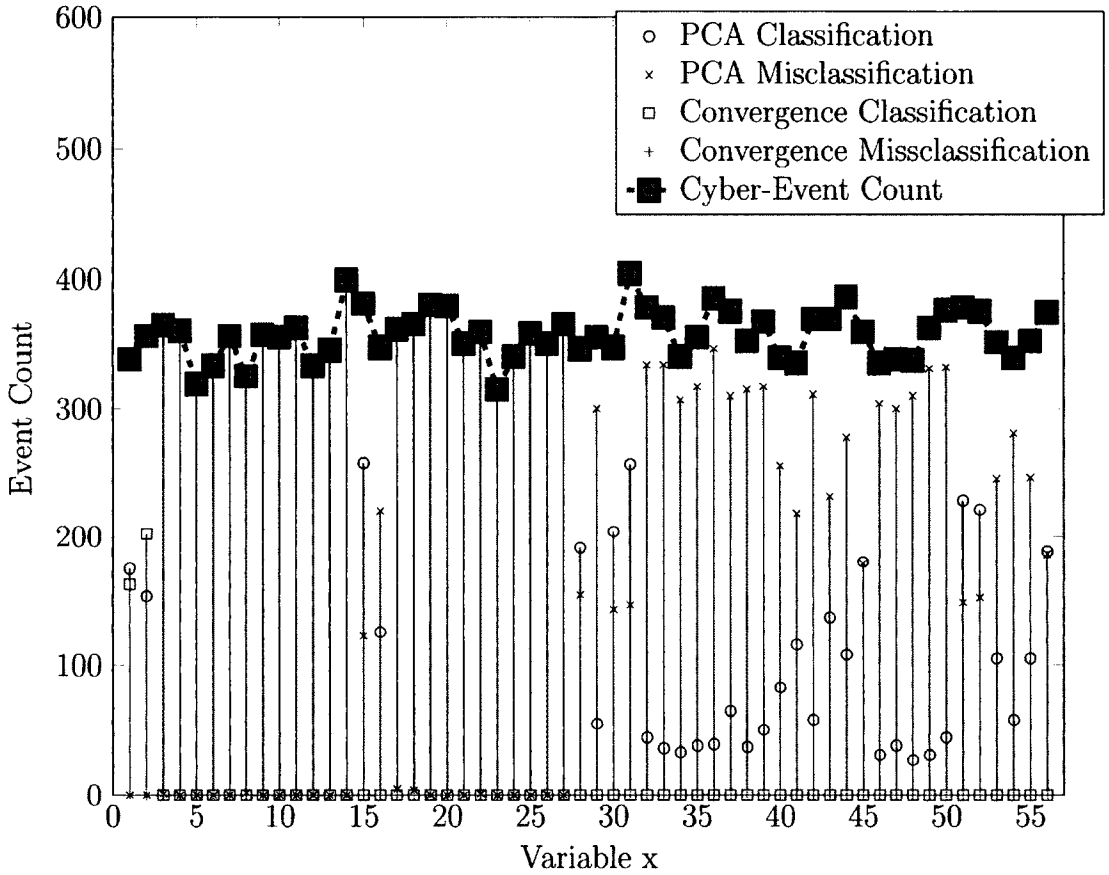

Figure D.9: IEEE 14-Bus Without Line Flows SI Classification Results

Table D.9: IEEE 14-Bus Without Line Flows SI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
0	365	7996	11639
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Single variate Type II Attack (SII)

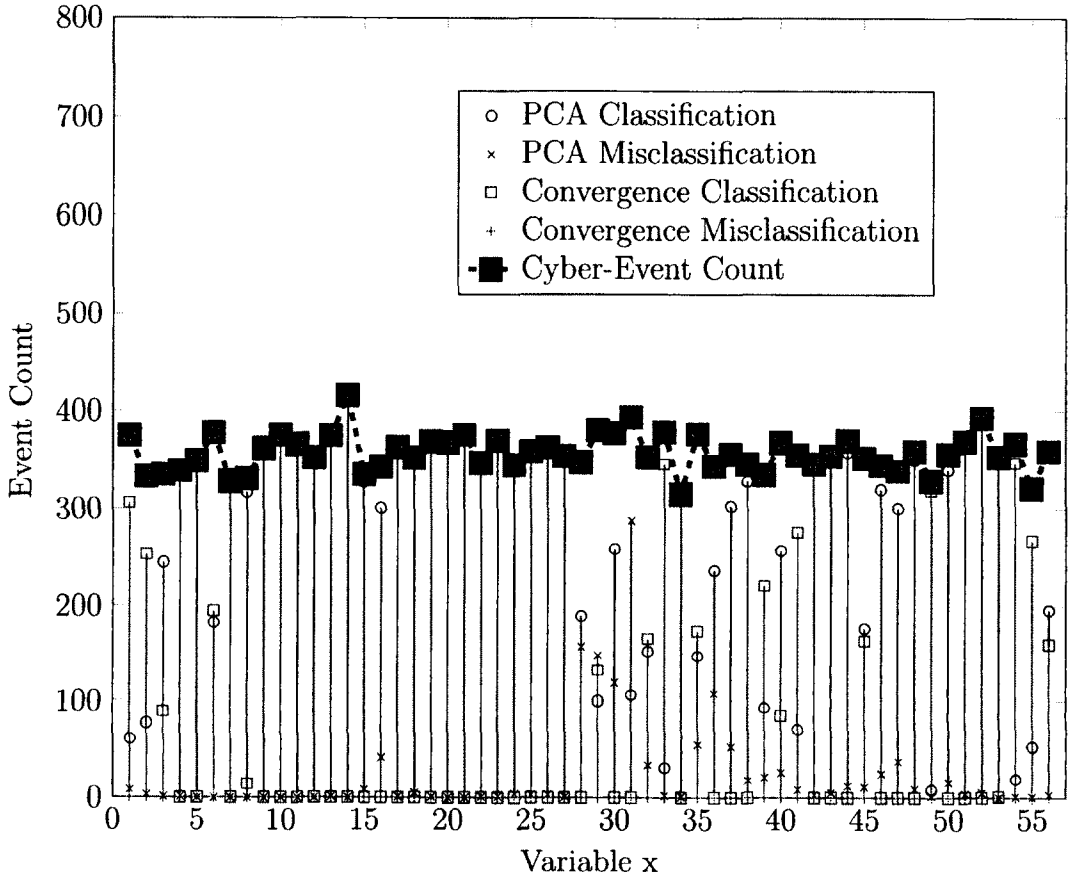

Figure D.10: IEEE 14-Bus Without Line Flows SII Classification Results

Table D.10: IEEE 14-Bus Without Line Flows SII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
0	365	7996	11639
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Multivariate Type I Attack (MI)

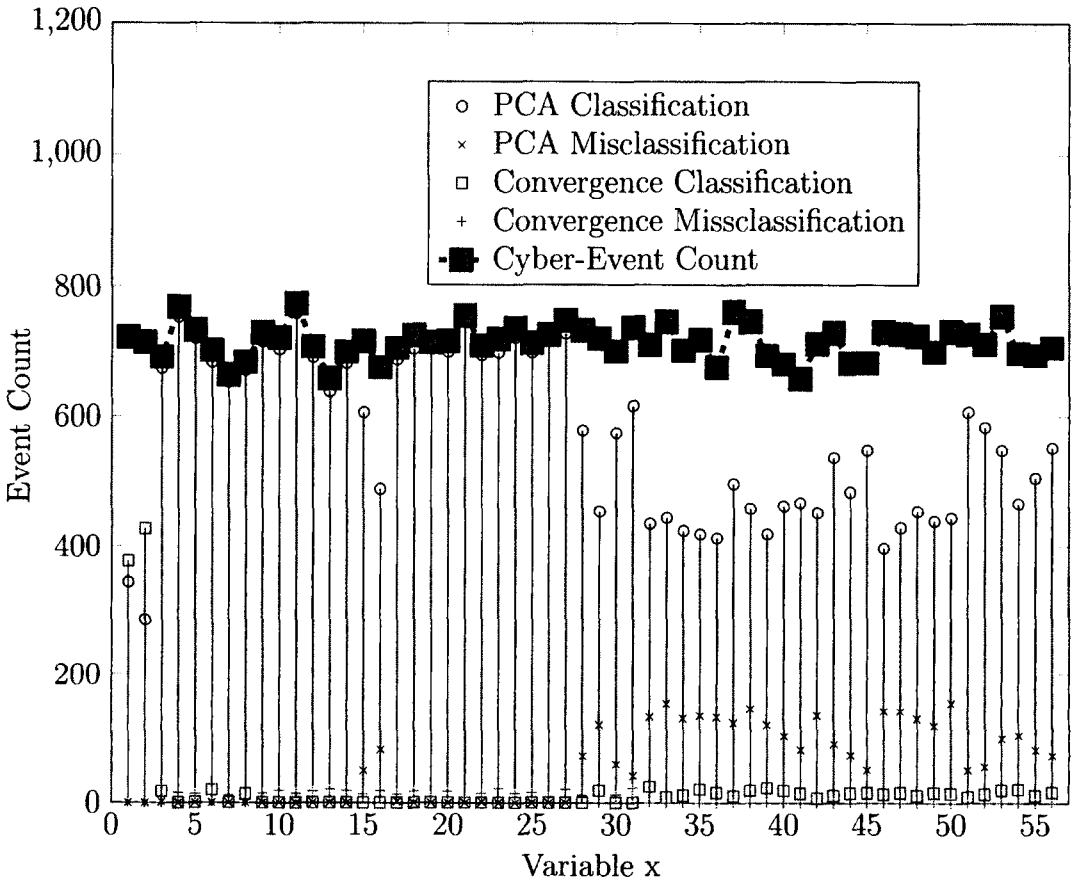

Figure D.11: IEEE 14-Bus Without Line Flows MI Classification Results

Table D.11: IEEE 14-Bus Without Line Flows MI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
373	1235	3214	31964
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

Multivariate Type II Attack (MII)

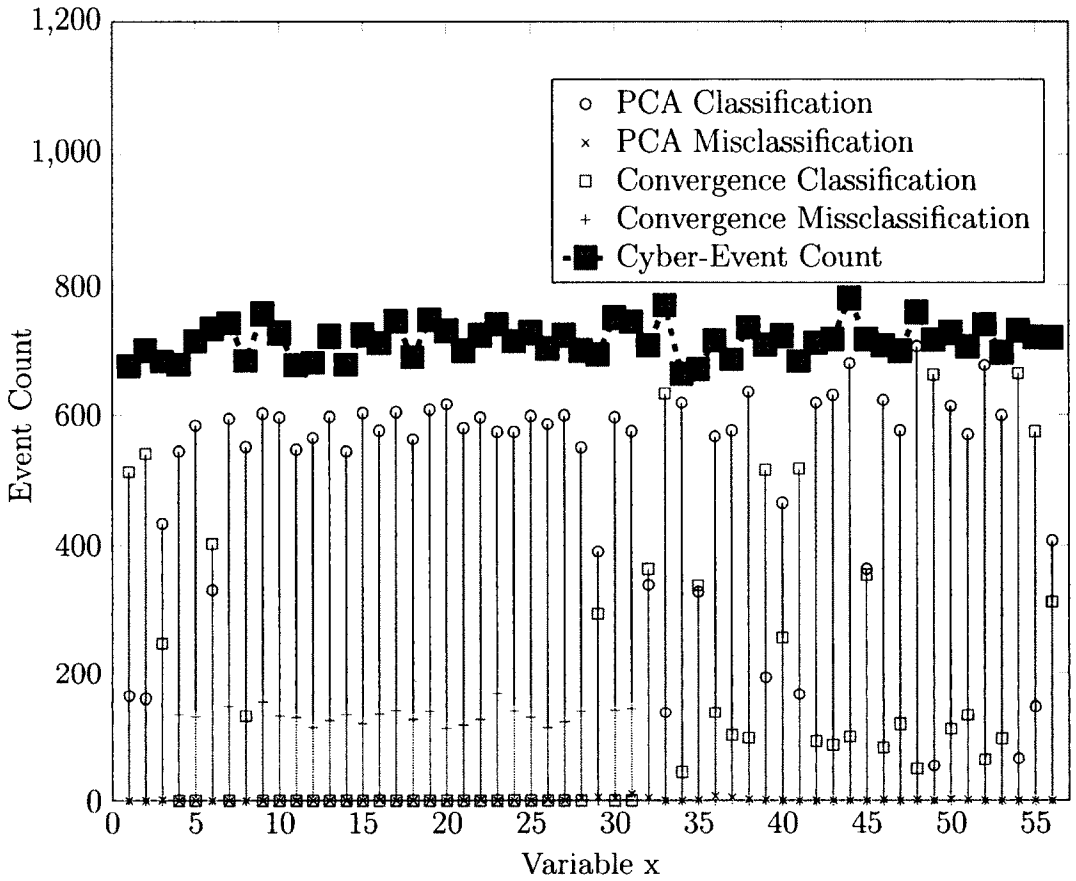

Figure D.12: IEEE 14-Bus Without Line Flows MII Classification Results

Table D.12: IEEE 14-Bus Without Line Flows MII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
3315	8635	52	27964
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 40,000			

D.2.2 With Line Flows

Single variate Type I Attack (SI)

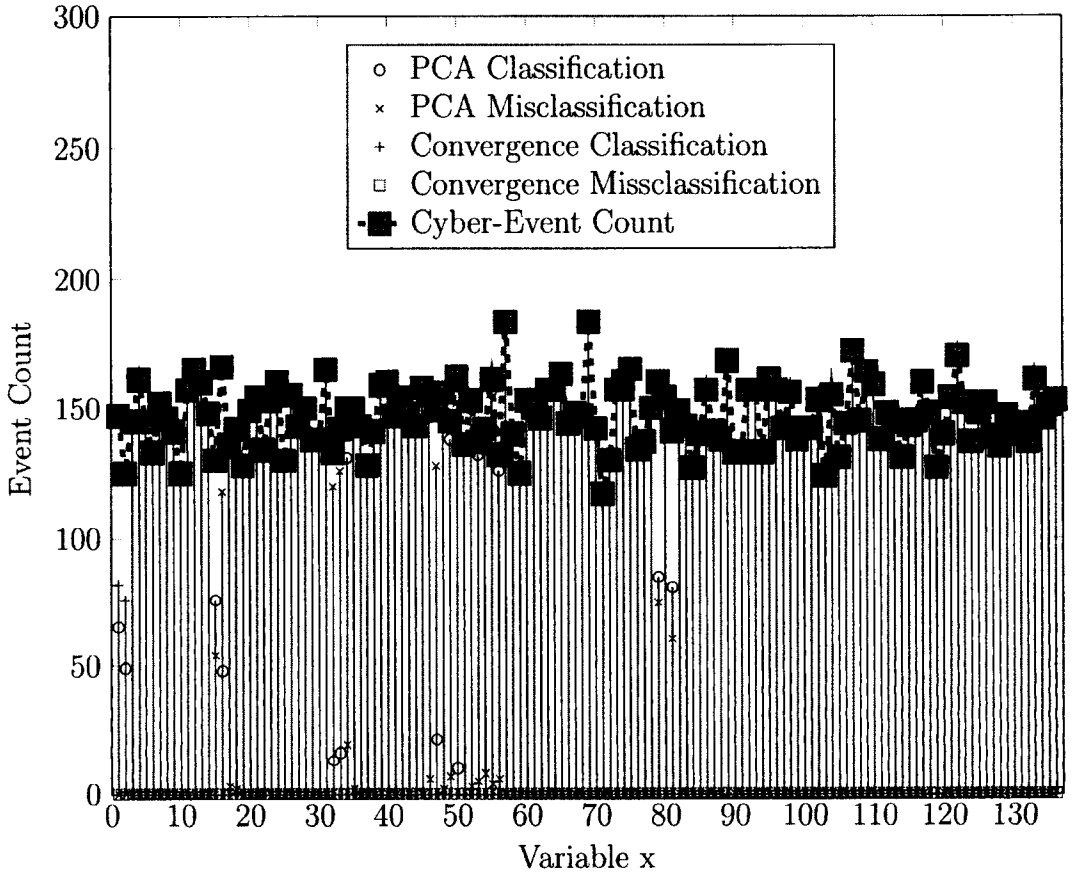

Figure D.13: IEEE 14-Bus With Line Flows SI Classification Results

Table D.13: IEEE 14-Bus With Line Flows SI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
0	158	910	18392
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Single variate Type II Attack (SII)

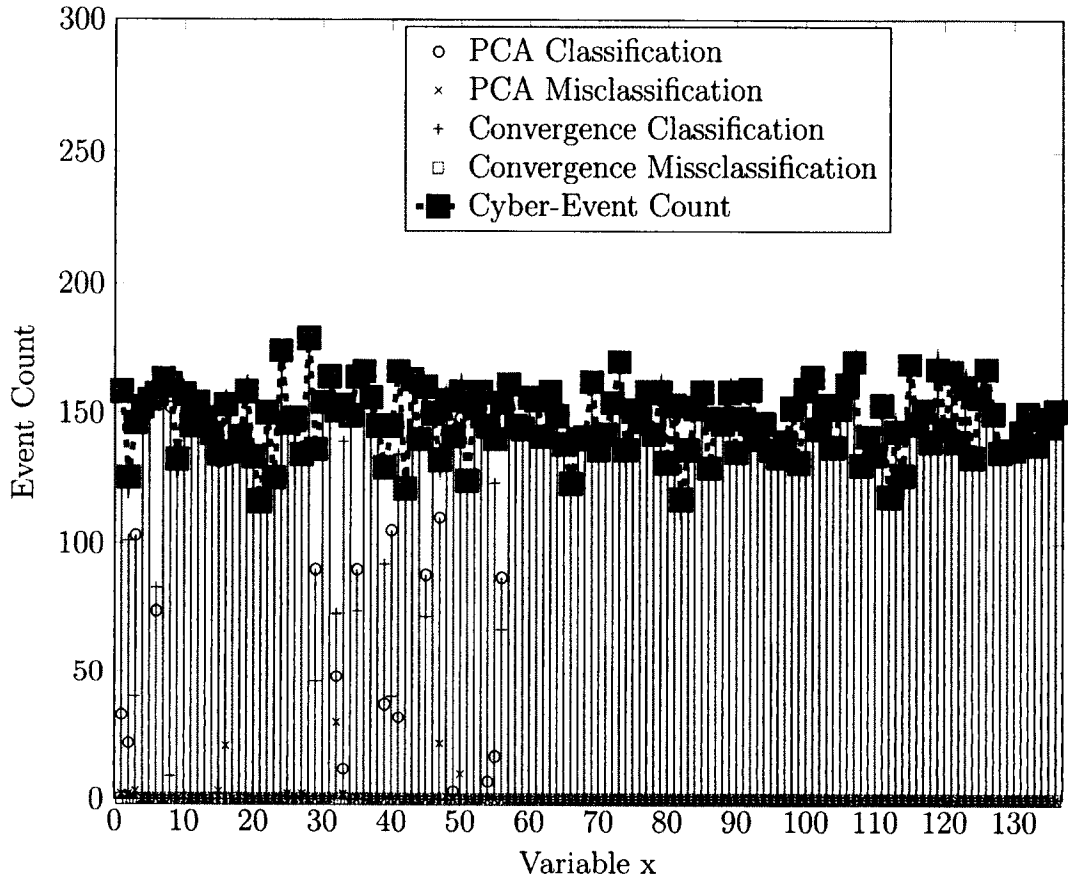

Figure D.14: IEEE 14-Bus With Line Flows SII Classification Results

Table D.14: IEEE 14-Bus With Line Flows SII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
0	1492	107	18393
Total Number of Simulated Malicious Instances = 20,000			
Total Number of Simulated Cyber-Events = 20,000			

Multivariate Type I Attack (MI)

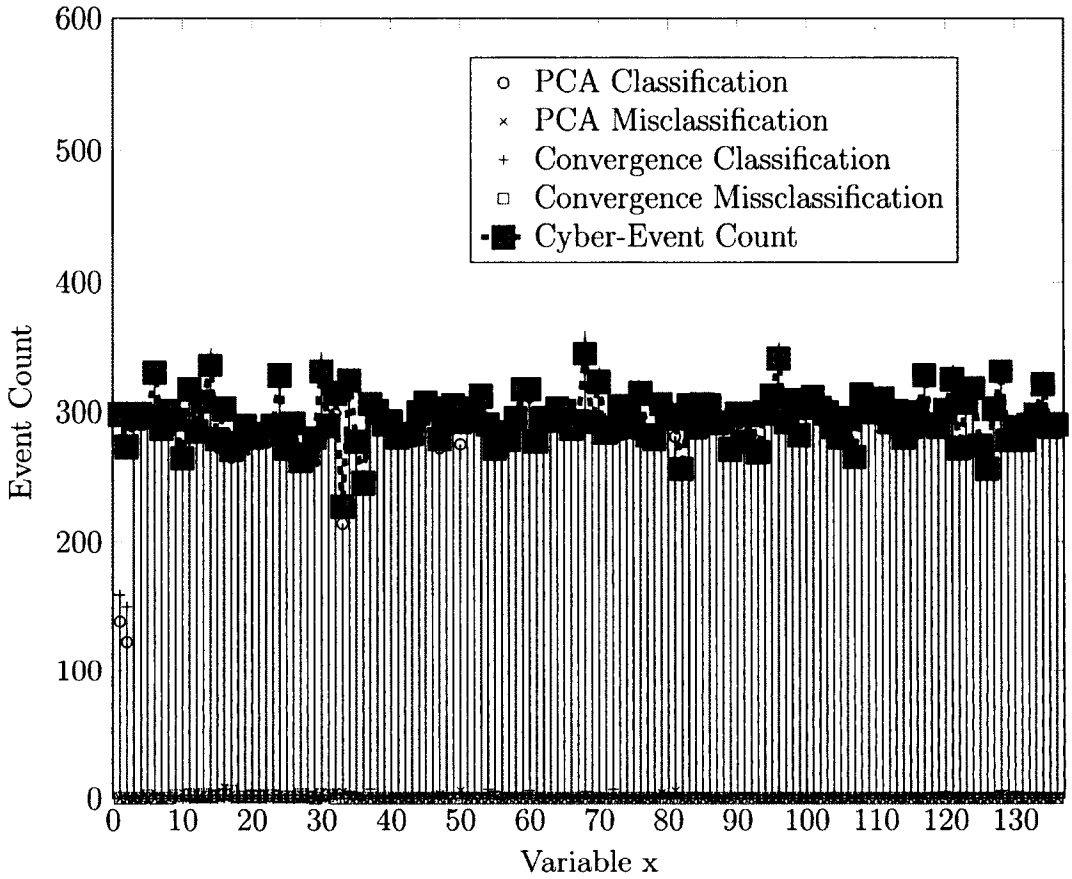

Figure D.15: IEEE 14-Bus With Line Flows MI Classification Results

Table D.15: IEEE 14-Bus With Line Flows MI Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
46	572	86	39296
Total Number of Simulated Malicious Instances = 40,000			
Total Number of Simulated Cyber-Events = 40,000			

Multivariate Type II Attack (MII)

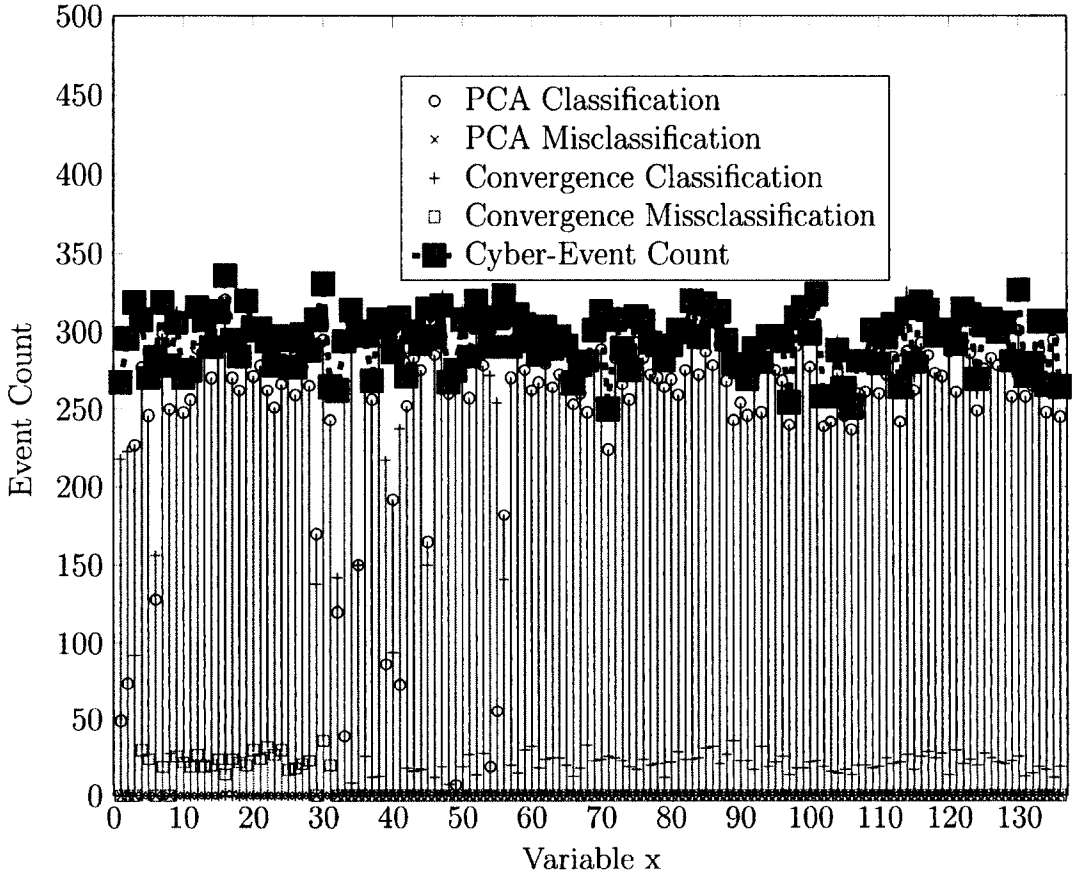

Figure D.16: IEEE 14-Bus With Line Flows MII Classification Results

Table D.16: IEEE 14-Bus With Line Flows MII Classification Results

Convergence Misclassification	Convergence Classification	PCA Misclassification	PCA Classification
588	5032	2	34340
Total Number of Simulated Malicious Instances = 40,000			
Total Number of Simulated Cyber-Events = 40,000			

APPENDIX E

CYBER-EVENT LOCALIZATION PLOTS AND TABLES

E.1 5-Bus Localization

E.1.1 Without Line Flows

Single variate Type I Attack (SI)

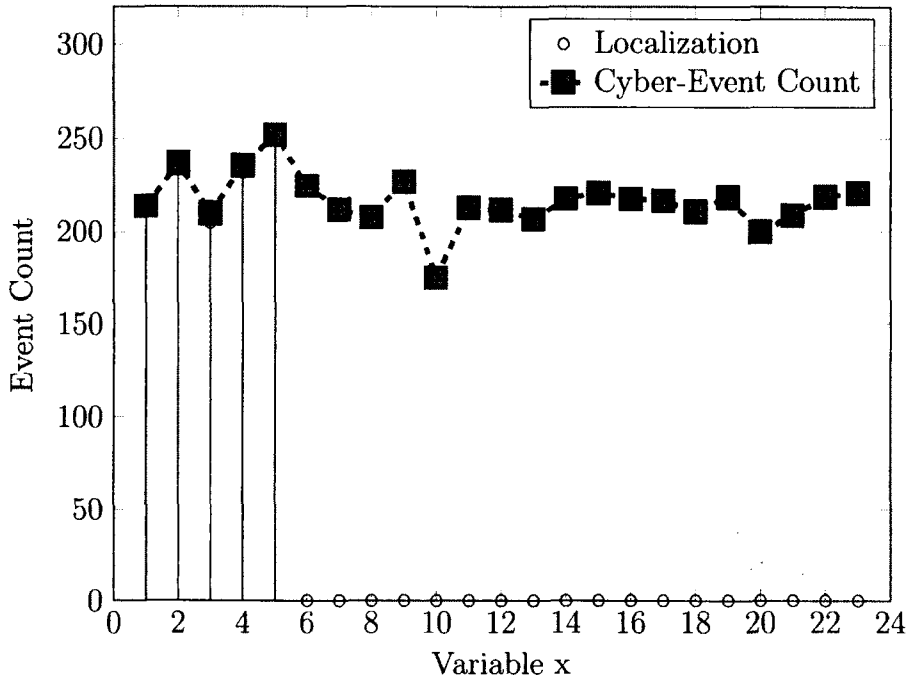

Figure E.1: 5-Bus Without Line Flows SI Localization Results

Table E.1: 5-Bus Without Line Flows SI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	214	213	99.5
x_2	237	235	99.2
x_3	210	205	97.6
x_4	236	232	98.3
x_5	252	249	98.8

Single variate Type II Attack (SII)

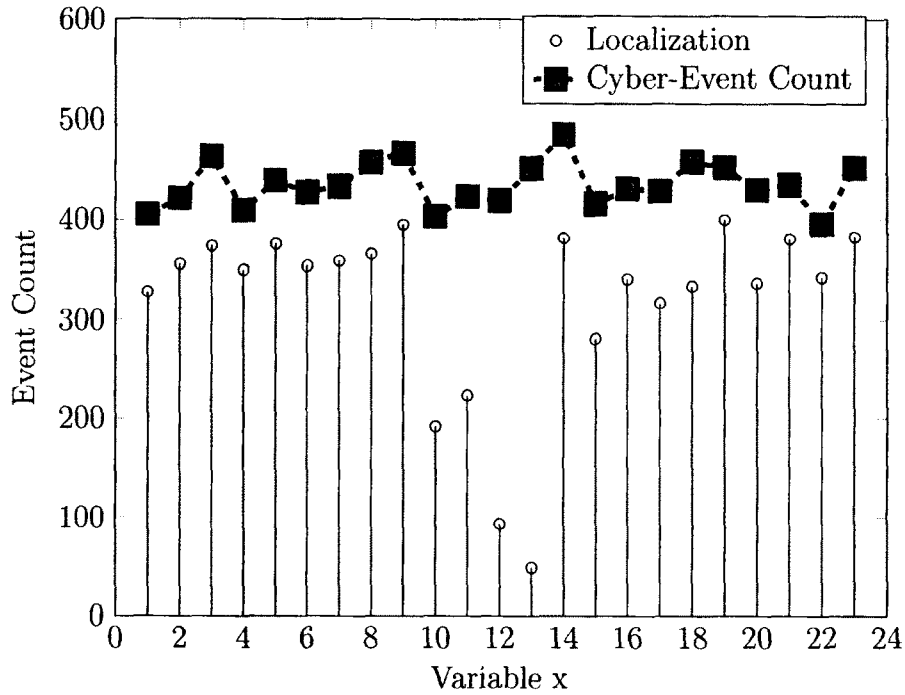

Figure E.2: 5-Bus Without Line Flows SII Localization Results

Table E.2: 5-Bus Without Line Flows SII Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	405	328	81.0
x_2	421	356	84.7
x_3	463	374	80.8
x_4	409	350	85.6
x_5	439	376	85.7
x_6	427	354	82.9
x_7	433	359	82.9
x_8	457	366	80.0
x_9	466	395	84.8
x_{10}	403	192	47.6
x_{11}	423	223	52.7
x_{12}	419	93	22.2
x_{13}	451	49	10.9
x_{14}	485	382	78.8
x_{15}	416	281	67.6
x_{16}	431	341	79.1
x_{17}	429	317	73.9
x_{18}	458	334	72.9
x_{19}	452	400	88.5
x_{20}	430	337	78.4
x_{21}	435	381	87.6
x_{22}	396	343	86.6
x_{23}	452	383	84.7

Multivariate Type I Attack (MI)

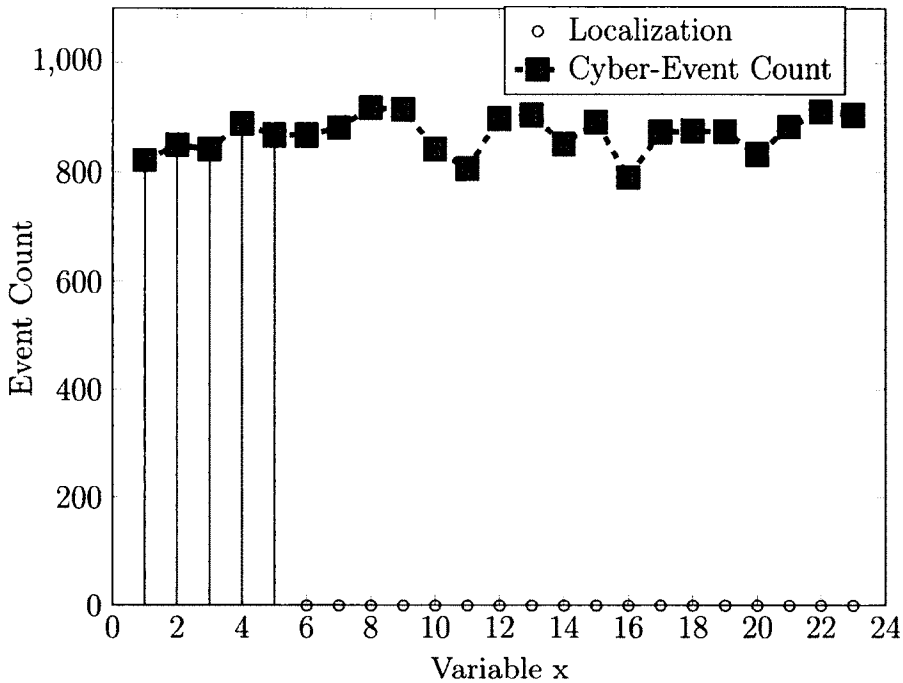

Figure E.3: 5-Bus Without Line Flows MI Localization Results

Table E.3: 5-Bus Without Line Flows MI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	822	822	100
x_2	850	850	100
x_3	842	842	100
x_4	889	887	99.8
x_5	868	865	99.6

Multivariate Type II Attack (MII)

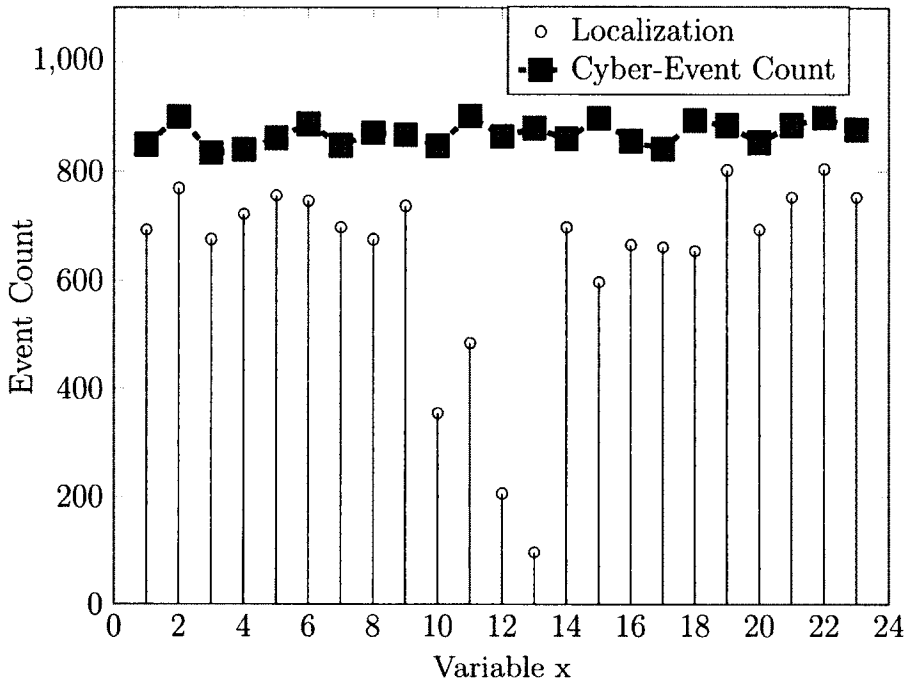

Figure E.4: 5-Bus Without Line Flows MII Localization Results

Table E.4: 5-Bus Without Line Flows MII Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	849	693	81.6
x_2	900	769	85.4
x_3	834	676	81.1
x_4	840	722	86.0
x_5	861	756	87.8
x_6	887	746	84.1
x_7	848	698	82.3
x_8	871	676	77.6
x_9	867	737	85.0
x_{10}	847	355	41.9
x_{11}	902	486	53.9
x_{12}	864	206	23.8
x_{13}	880	97	11.0
x_{14}	860	698	81.2
x_{15}	898	598	66.6
x_{16}	856	666	77.8
x_{17}	842	662	78.6
x_{18}	894	655	73.2
x_{19}	885	803	90.7
x_{20}	854	694	81.3
x_{21}	885	753	85.1
x_{22}	899	805	89.5
x_{23}	877	753	85.9

E.1.2 With Line Flows

Single variate Type I Attack (SI)

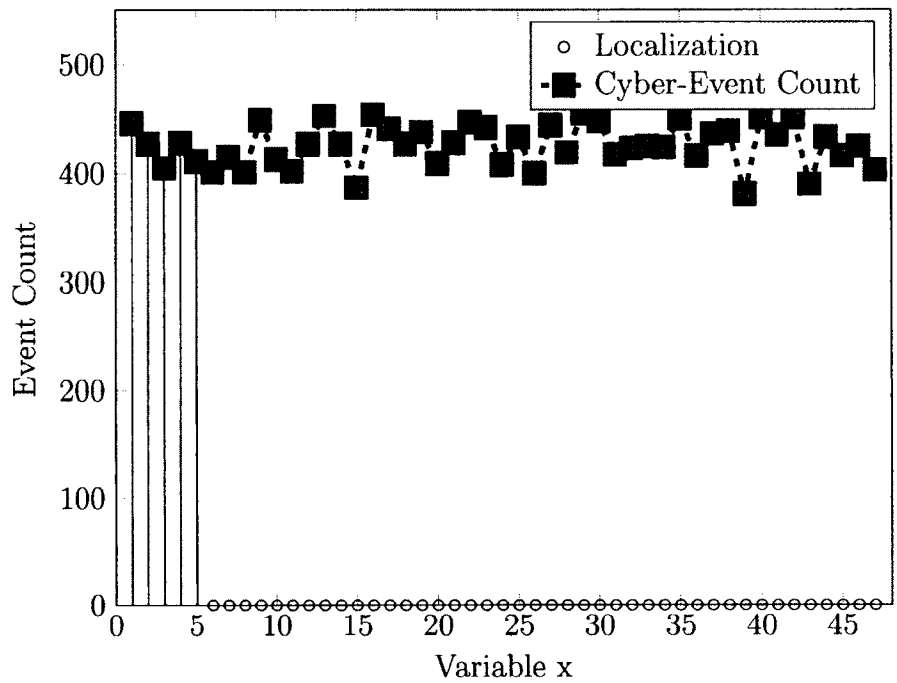

Figure E.5: 5-Bus With Line Flows SI Localization Results

Table E.5: 5-Bus With Line Flows SI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	849	693	81.6
x_2	900	769	85.4
x_3	834	676	81.1
x_4	840	722	86.0
x_5	861	756	87.8
x_6	887	746	84.1
x_7	848	698	82.3
x_8	871	676	77.6
x_9	867	737	85.0

Single variate Type II Attack (SII)

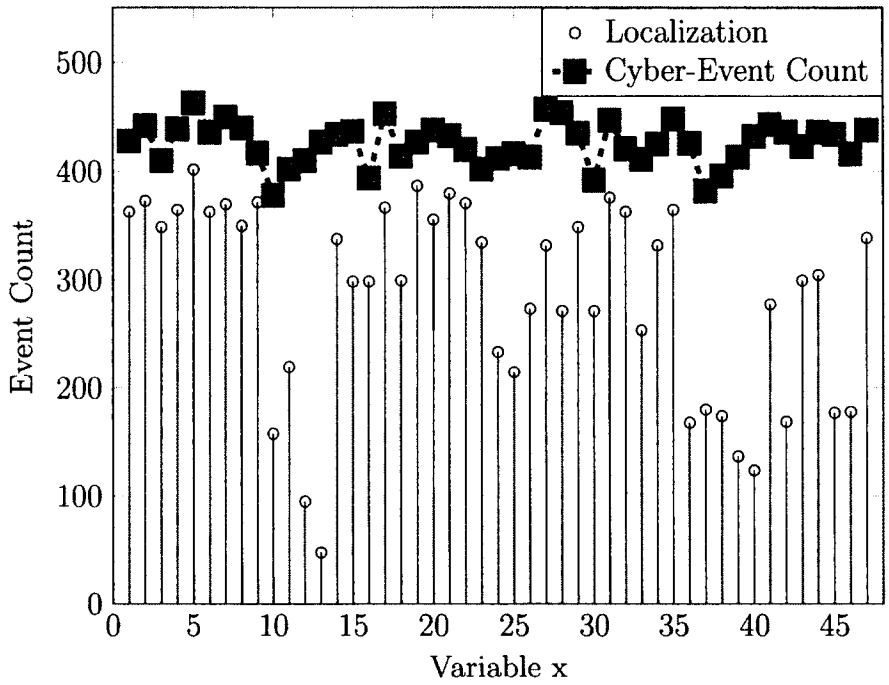

Figure E.6: 5-Bus With Line Flows SII Localization Results

Table E.6: 5-Bus With Line Flows SII Localization Results

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	428	363	84.8	x_{25}	416	215	51.7
x_2	442	373	84.4	x_{26}	413	274	66.3
x_3	410	349	85.1	x_{27}	457	332	72.6
x_4	439	365	83.1	x_{28}	454	272	60.0
x_5	463	402	86.8	x_{29}	435	349	80.2
x_6	436	363	83.3	x_{30}	392	272	69.4
x_7	450	370	82.2	x_{31}	447	376	84.1
x_8	440	350	79.5	x_{32}	421	363	86.2
x_9	417	372	89.2	x_{33}	411	254	61.8
x_{10}	378	158	41.8	x_{34}	425	332	78.1
x_{11}	402	220	54.7	x_{35}	448	365	81.5
x_{12}	410	95	23.2	x_{36}	426	168	39.4
x_{13}	427	48	11.2	x_{37}	382	180	47.1
x_{14}	434	338	77.9	x_{38}	396	174	43.9
x_{15}	437	299	68.4	x_{39}	413	137	33.2
x_{16}	394	299	75.9	x_{40}	432	124	28.7
x_{17}	453	367	81.0	x_{41}	443	278	62.8
x_{18}	414	300	72.5	x_{42}	436	169	38.8
x_{19}	427	387	90.6	x_{43}	423	300	70.9
x_{20}	438	356	81.3	x_{44}	436	305	70.0
x_{21}	433	380	87.8	x_{45}	434	177	40.8
x_{22}	420	371	88.3	x_{46}	416	178	42.8
x_{23}	402	335	83.3	x_{47}	438	339	77.4
x_{24}	412	234	56.8	–	–	–	–

Multivariate Type I Attack (MI)

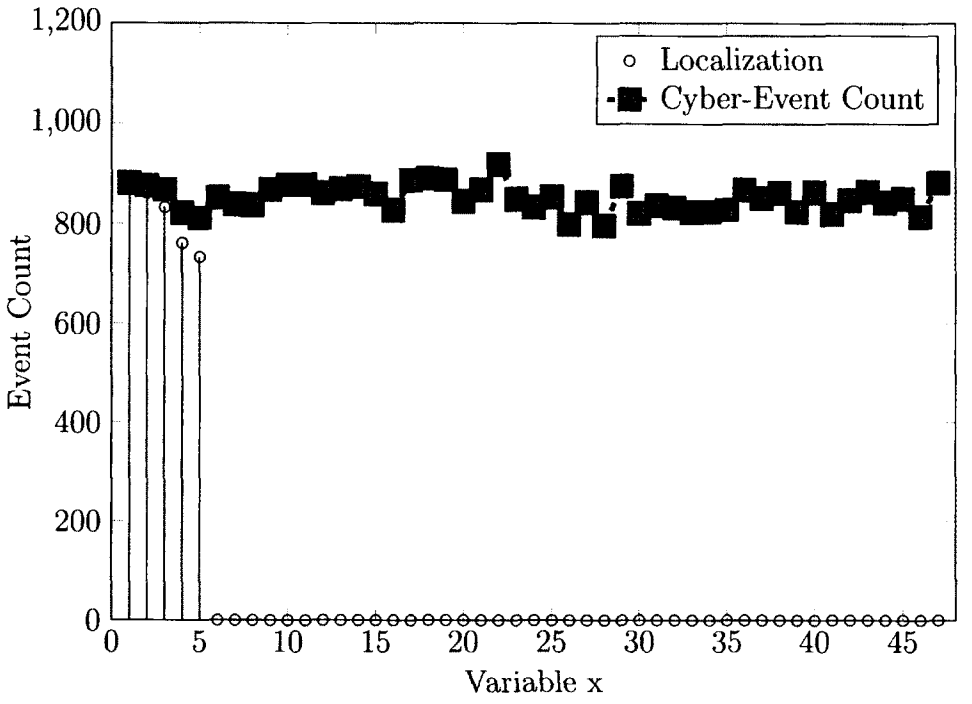

Figure E.7: 5-Bus With Line Flows MI Localization Results

Table E.7: 5-Bus With Line Flows MI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_1	881	881	100
x_2	876	861	98.3
x_3	868	833	96.0
x_4	822	761	92.6
x_5	811	733	90.4

Multivariate Type II Attack (MII)

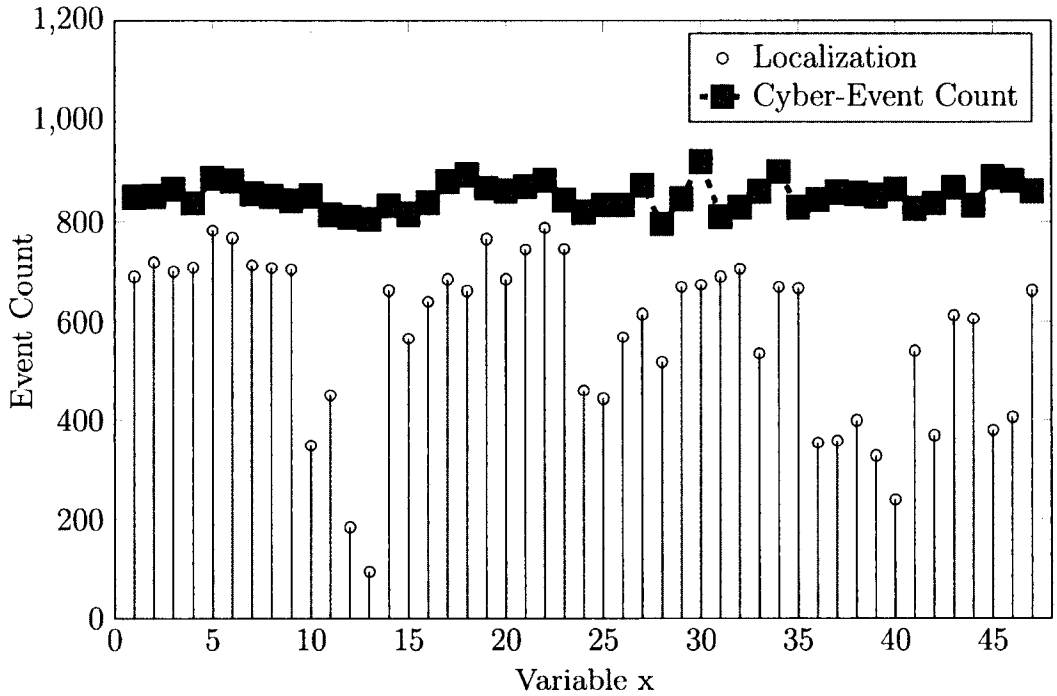

Figure E.8: 5-Bus With Line Flows MII Localization Results

Table E.8: 5-Bus With Line Flows MII Localization Results

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	849	691	81.4	x_{25}	833	443	53.2
x_2	851	719	84.5	x_{26}	833	569	68.3
x_3	865	701	81.0	x_{27}	872	615	70.5
x_4	837	709	84.7	x_{28}	795	518	65.2
x_5	887	783	88.3	x_{29}	846	670	79.2
x_6	882	768	87.1	x_{30}	920	674	73.3
x_7	856	713	83.3	x_{31}	810	690	85.2
x_8	851	708	83.2	x_{32}	828	706	85.2
x_9	842	705	83.7	x_{33}	860	536	62.3
x_{10}	852	349	41.0	x_{34}	900	670	74.4
x_{11}	814	450	55.3	x_{35}	828	667	80.6
x_{12}	809	184	22.7	x_{36}	844	354	41.9
x_{13}	805	94	11.7	x_{37}	859	358	41.7
x_{14}	832	663	80.0	x_{38}	856	399	46.6
x_{15}	815	566	69.5	x_{39}	852	328	38.5
x_{16}	838	640	76.4	x_{40}	865	239	27.6
x_{17}	880	685	77.8	x_{41}	826	541	65.5
x_{18}	894	662	74.1	x_{42}	837	369	44.1
x_{19}	867	766	88.4	x_{43}	868	613	70.6
x_{20}	861	685	79.6	x_{44}	832	606	72.8
x_{21}	870	745	85.6	x_{45}	889	380	42.7
x_{22}	883	788	89.2	x_{46}	882	406	46.0
x_{23}	844	746	88.4	x_{47}	861	663	77.0
x_{24}	819	459	56.0	–	–	–	–

E.2 IEEE 14-Bus Localization

E.2.1 Without Line Flows

Single variate Type I Attack (SI)

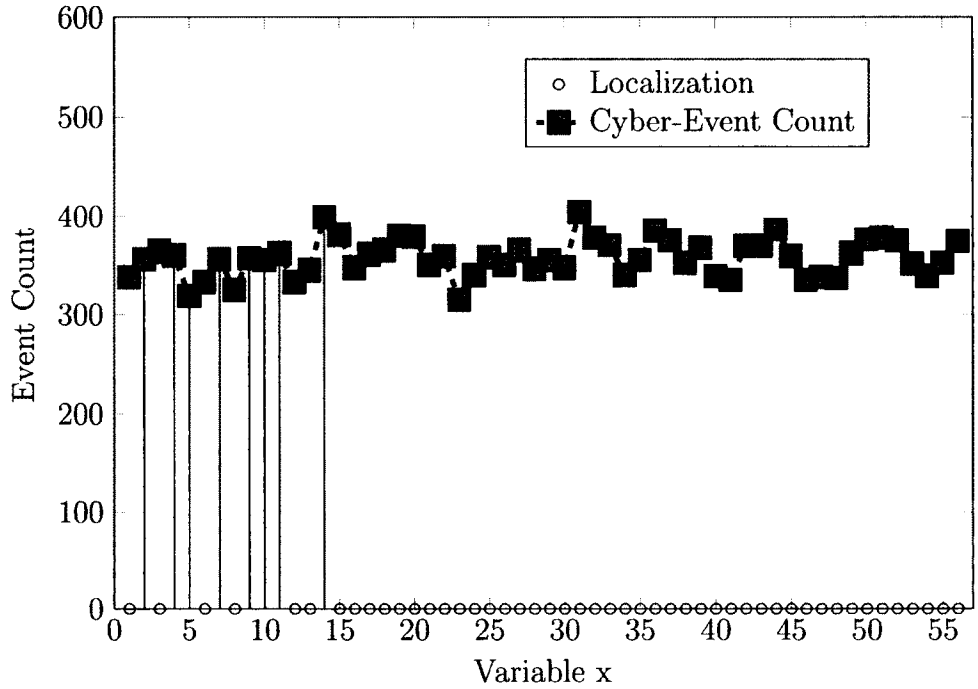

Figure E.9: IEEE 14-Bus Without Line Flows SI Localization Results

Table E.9: IEEE 14-Bus Without Line Flows SI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_2	356	356	100
x_4	360	360	100
x_5	319	319	100
x_7	356	356	100
x_9	357	357	100
x_10	355	355	100
x_11	363	362	100
x_14	399	399	100

Single variate Type II Attack (SII)

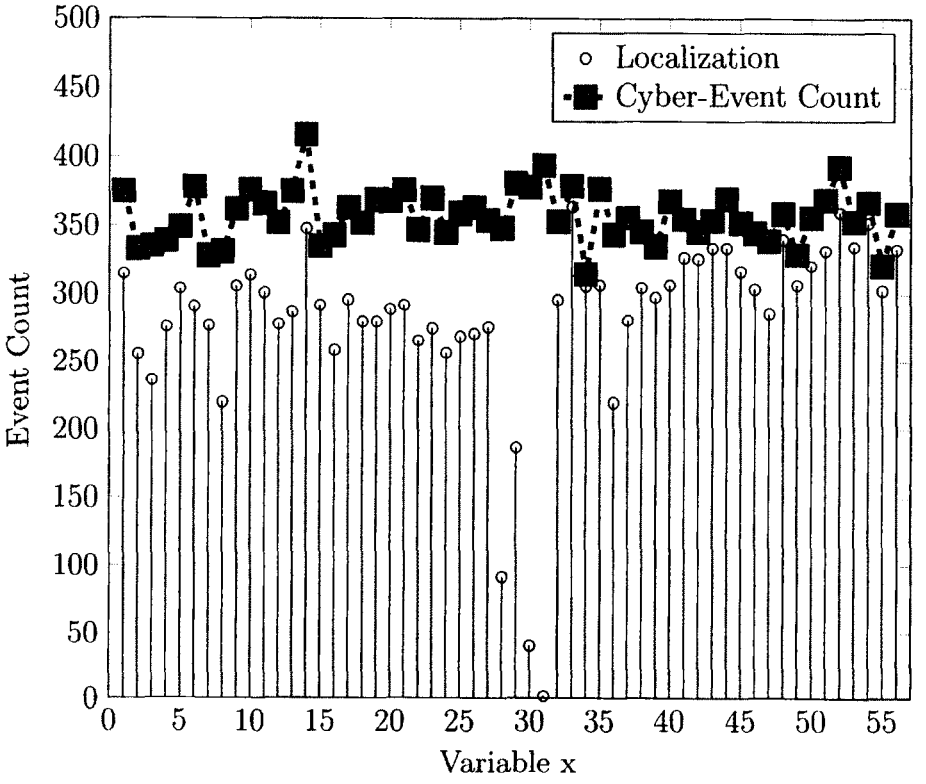

Figure E.10: IEEE 14-Bus Without Line Flows SII Localization Results

Table E.10: IEEE 14-Bus Without Line Flows SII Localization Results

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	375	315	84.0	x_{29}	381	187	49.1
x_2	333	256	76.9	x_{30}	378	41	10.9
x_3	335	236	70.5	x_{31}	394	2	0.51
x_4	339	276	81.4	x_{32}	353	296	83.9
x_5	349	304	87.1	x_{33}	379	364	96.0
x_6	378	291	77.0	x_{34}	315	306	97.1
x_7	328	277	84.5	x_{35}	377	307	81.5
x_8	331	220	66.5	x_{36}	344	220	64.0
x_9	362	306	84.5	x_{37}	356	281	79.0
x_{10}	376	314	83.5	x_{38}	346	305	88.2
x_{11}	366	301	82.2	x_{39}	335	298	89.0
x_{12}	352	278	79.0	x_{40}	368	307	83.4
x_{13}	375	287	76.5	x_{41}	355	327	92.1
x_{14}	416	348	83.7	x_{42}	346	326	94.2
x_{15}	335	292	87.2	x_{43}	354	334	94.4
x_{16}	343	259	75.5	x_{44}	370	334	90.3
x_{17}	363	296	81.5	x_{45}	352	317	90.1
x_{18}	352	280	79.6	x_{46}	345	304	88.1
x_{19}	369	280	75.9	x_{47}	339	286	84.4
x_{20}	368	289	78.5	x_{48}	359	340	94.7
x_{21}	376	292	77.7	x_{49}	329	307	93.3
x_{22}	347	266	76.7	x_{50}	356	321	90.2
x_{23}	370	275	74.3	x_{51}	369	332	90.0
x_{24}	345	257	74.5	x_{52}	393	360	91.6
x_{25}	359	269	74.9	x_{53}	353	335	94.9
x_{26}	363	271	74.7	x_{54}	367	352	95.9
x_{27}	354	276	78.0	x_{55}	321	303	94.4
x_{28}	348	92	26.4	x_{56}	359	333	92.8

Multivariate Type I Attack (MI)

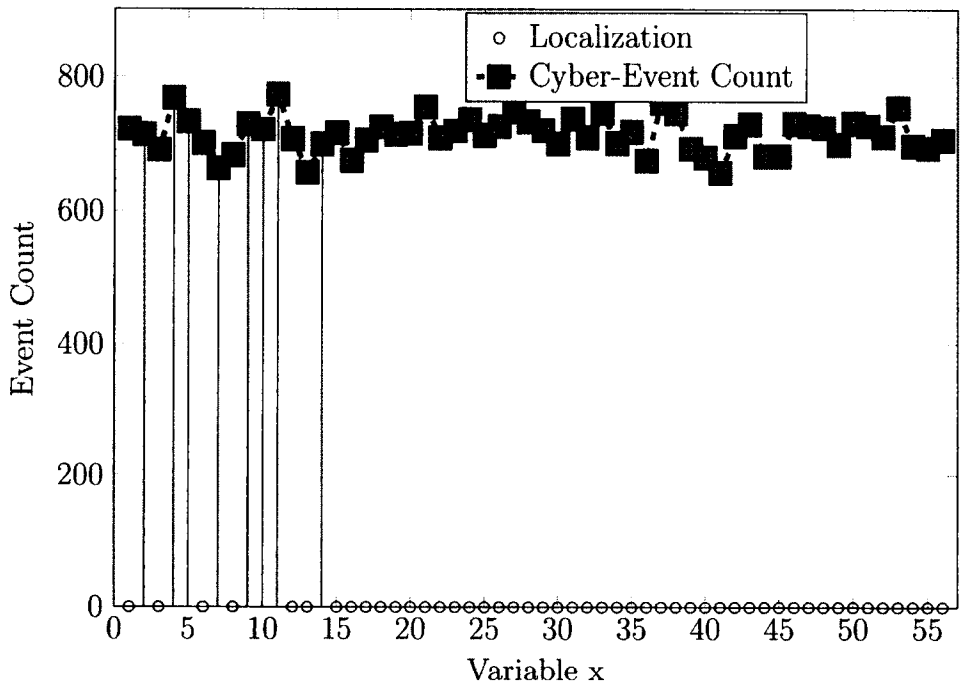

Figure E.11: IEEE 14-Bus Without Line Flows MI Localization Results

Table E.11: IEEE 14-Bus Without Line Flows MI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_2	714	714	100
x_4	768	767	99.9
x_5	733	732	99.9
x_7	663	662	99.9
x_9	729	726	99.6
x_10	721	718	99.6
x_11	773	766	99.1
x_14	699	693	99.1

Multivariate Type II Attack (MII)

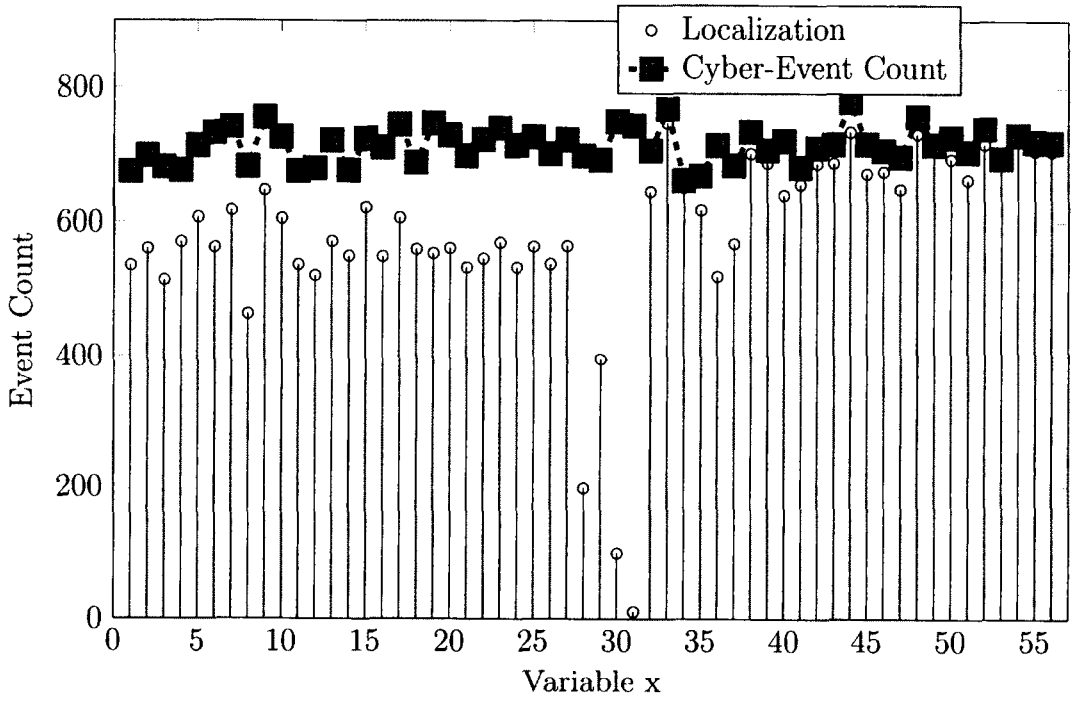

Figure E.12: IEEE 14-Bus Without Line Flows MII Localization Results

Table E.12: IEEE 14-Bus Without Line Flows MII Localization Results

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	675	536	79.4	x_{29}	693	396	57.1
x_2	699	561	80.3	x_{30}	750	100	13.3
x_3	682	514	75.4	x_{31}	744	11	1.48
x_4	677	571	84.3	x_{32}	707	646	91.4
x_5	714	608	85.2	x_{33}	769	748	97.3
x_6	733	563	76.8	x_{34}	663	652	98.3
x_7	742	618	83.3	x_{35}	670	619	92.4
x_8	683	464	67.9	x_{36}	715	520	72.7
x_9	756	648	85.7	x_{37}	685	569	83.1
x_{10}	727	606	83.4	x_{38}	735	703	95.7
x_{11}	676	537	79.4	x_{39}	708	689	97.3
x_{12}	680	521	76.6	x_{40}	722	641	88.8
x_{13}	722	572	79.2	x_{41}	682	657	96.3
x_{14}	677	550	81.2	x_{42}	711	688	96.8
x_{15}	724	622	85.9	x_{43}	717	689	96.1
x_{16}	711	549	77.2	x_{44}	780	735	94.2
x_{17}	745	607	81.5	x_{45}	717	673	93.9
x_{18}	689	560	81.3	x_{46}	707	676	95.6
x_{19}	747	554	74.2	x_{47}	698	650	93.1
x_{20}	730	562	77.0	x_{48}	758	732	96.6
x_{21}	699	533	76.3	x_{49}	716	710	99.2
x_{22}	723	546	75.5	x_{50}	727	695	95.6
x_{23}	740	570	77.0	x_{51}	705	664	94.2
x_{24}	714	533	74.7	x_{52}	740	717	96.9
x_{25}	727	564	77.6	x_{53}	696	692	99.4
x_{26}	702	538	76.6	x_{54}	730	729	99.9
x_{27}	723	565	78.2	x_{55}	720	707	98.2
x_{28}	699	198	28.3	x_{56}	719	706	98.2

E.2.2 With Line Flows

Single variate Type I Attack (SI)

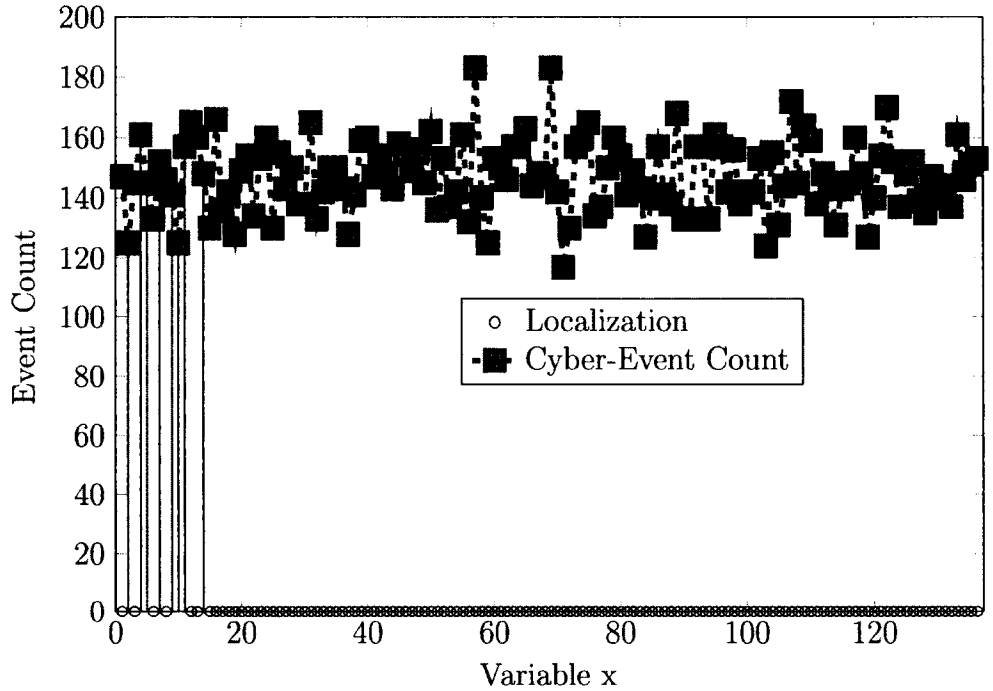

Figure E.13: IEEE 14-Bus With Line Flows SI Localization Results

Table E.13: IEEE 14-Bus With Line Flows SI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_2	125	125	100
x_4	161	161	100
x_5	145	145	100
x_7	152	152	100
x_9	141	141	100
x_{10}	125	125	100
x_{11}	157	157	100
x_{14}	148	148	100

Single variate Type II Attack (SII)

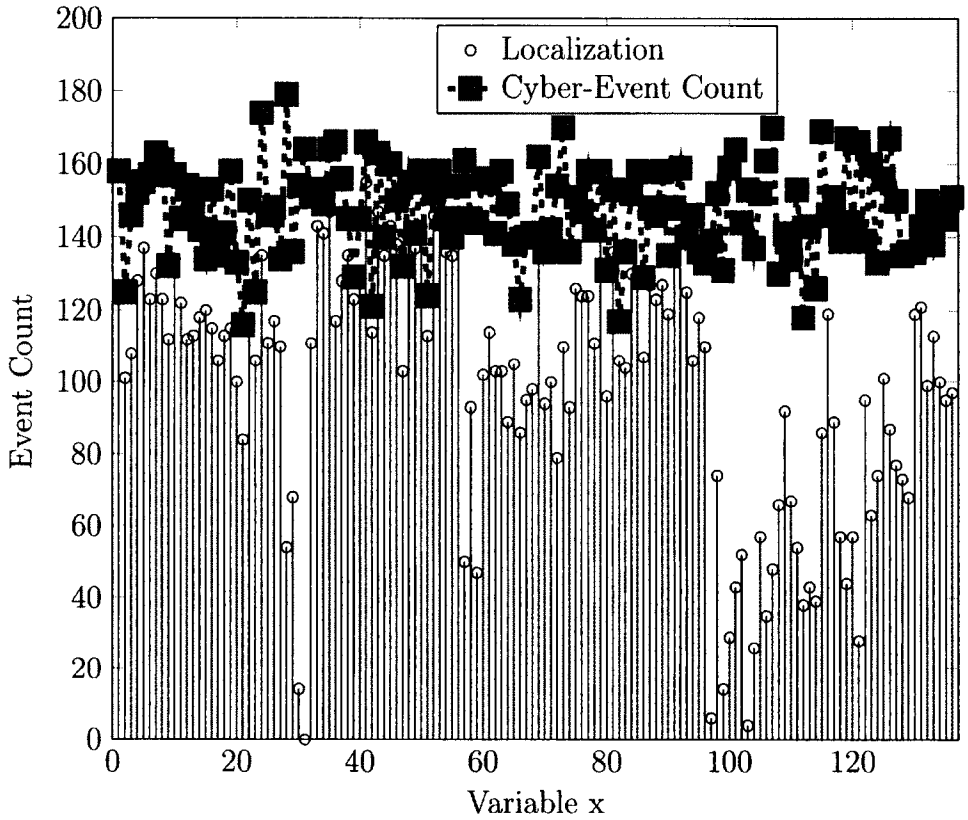

Figure E.14: IEEE 14-Bus With Line Flows SII Localization Results

Table E.14: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x1-x68

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	158	123	77.8	x_{35}	162	136	83.9
x_2	125	101	80.8	x_{36}	136	94	69.1
x_3	146	108	73.9	x_{37}	142	100	70.4
x_4	152	128	84.2	x_{38}	154	79	51.2
x_5	155	137	88.3	x_{39}	170	110	64.7
x_6	157	123	78.3	x_{40}	136	93	68.3
x_7	163	130	79.7	x_{41}	151	126	83.4
x_8	161	123	76.3	x_{42}	147	124	84.3
x_9	132	112	84.8	x_{43}	158	124	78.4
x_{10}	157	134	85.3	x_{44}	142	111	78.1
x_{11}	145	122	84.1	x_{45}	158	141	89.2
x_{12}	154	112	72.7	x_{46}	131	96	73.2
x_{13}	148	113	76.3	x_{47}	153	136	88.8
x_{14}	142	118	83.0	x_{48}	117	106	90.5
x_{15}	134	120	89.5	x_{49}	136	104	76.4
x_{16}	153	115	75.1	x_{50}	152	130	85.5
x_{17}	135	106	78.5	x_{51}	158	128	81.0
x_{18}	141	113	80.1	x_{52}	129	107	82.9
x_{19}	158	115	72.7	x_{53}	148	127	85.8
x_{20}	133	100	75.1	x_{54}	146	123	84.2
x_{21}	116	84	72.4	x_{55}	158	127	80.3
x_{22}	150	117	78	x_{56}	135	119	88.1
x_{23}	125	106	84.8	x_{57}	148	135	91.2
x_{24}	174	135	77.5	x_{58}	159	142	89.3
x_{25}	146	111	76.0	x_{59}	140	125	89.2
x_{26}	148	117	79.0	x_{60}	146	106	72.6
x_{27}	134	110	82.0	x_{61}	136	118	86.7
x_{28}	179	54	30.1	x_{62}	133	110	82.7
x_{29}	136	68	50	x_{63}	139	6	4.31
x_{30}	154	14	9.09	x_{64}	152	74	48.6
x_{31}	164	0	0	x_{65}	131	14	10.6
x_{32}	151	111	73.5	x_{66}	159	29	18.2
x_{33}	153	143	93.4	x_{67}	164	43	26.2
x_{34}	149	141	94.6	x_{68}	144	52	36.1

Table E.15: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x69-x136

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_{69}	164	147	89.6	x_{103}	153	4	2.61
x_{70}	166	117	70.4	x_{104}	137	26	18.9
x_{71}	156	128	82.0	x_{105}	152	57	37.5
x_{72}	145	135	93.1	x_{106}	161	35	21.7
x_{73}	129	123	95.3	x_{107}	170	48	28.2
x_{74}	145	130	89.6	x_{108}	130	66	50.7
x_{75}	166	155	93.3	x_{109}	141	92	65.2
x_{76}	121	114	94.2	x_{110}	134	67	50
x_{77}	163	147	90.1	x_{111}	153	54	35.2
x_{78}	140	135	96.4	x_{112}	118	38	32.2
x_{79}	160	143	89.3	x_{113}	143	43	30.0
x_{80}	150	138	92	x_{114}	126	39	30.9
x_{81}	132	103	78.0	x_{115}	169	86	50.8
x_{82}	155	143	92.2	x_{116}	146	119	81.5
x_{83}	141	137	97.1	x_{117}	151	89	58.9
x_{84}	158	143	90.5	x_{118}	139	57	41.0
x_{85}	124	113	91.1	x_{119}	167	44	26.3
x_{86}	152	146	96.0	x_{120}	144	57	39.5
x_{87}	158	155	98.1	x_{121}	166	28	16.8
x_{88}	145	136	93.7	x_{122}	139	95	68.3
x_{89}	140	135	96.4	x_{123}	160	63	39.3
x_{90}	154	147	95.4	x_{124}	133	74	55.6
x_{91}	161	50	31.0	x_{125}	156	101	64.7
x_{92}	145	93	64.1	x_{126}	167	87	52.0
x_{93}	144	47	32.6	x_{127}	150	77	51.3
x_{94}	156	102	65.3	x_{128}	135	73	54.0
x_{95}	155	114	73.5	x_{129}	136	68	50
x_{96}	141	103	73.0	x_{130}	136	119	87.5
x_{97}	158	103	65.1	x_{131}	143	121	84.6
x_{98}	149	89	59.7	x_{132}	150	99	66
x_{99}	138	105	76.0	x_{133}	138	113	81.8
x_{100}	123	86	69.9	x_{134}	148	100	67.5
x_{101}	140	95	67.8	x_{135}	145	95	65.5
x_{102}	141	98	69.5	x_{136}	151	97	64.2

Multivariate Type I Attack (MI)

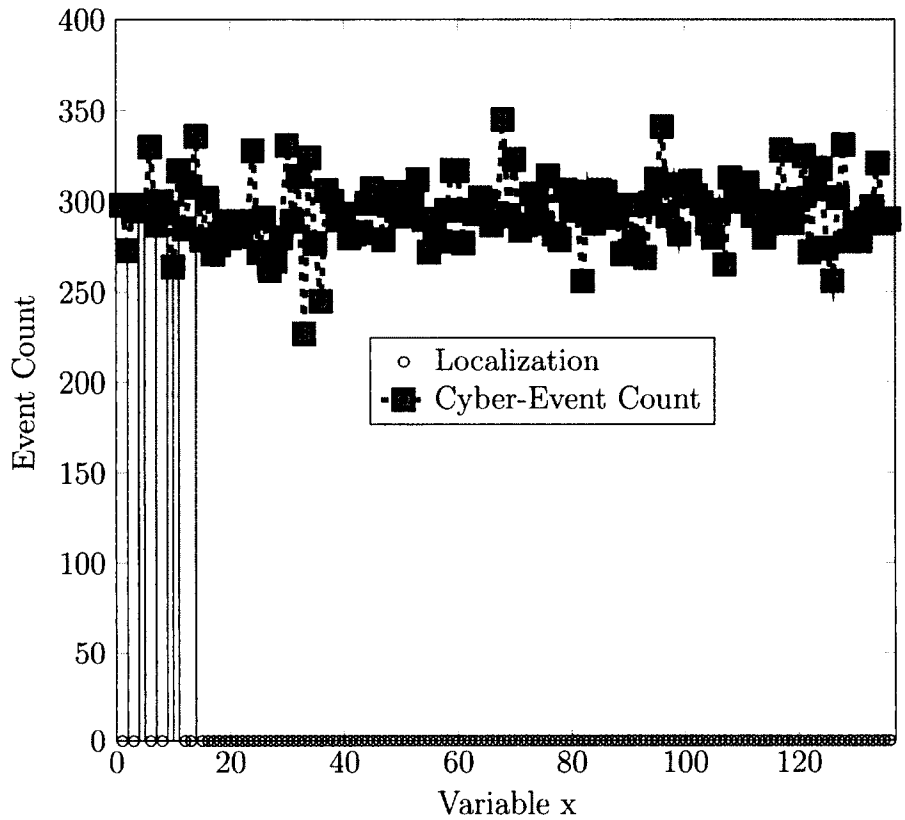

Figure E.15: IEEE 14-Bus With Line Flows MI Localization Results

Table E.16: IEEE 14-Bus With Line Flows MI Localization Results

Event Variable	Number of Events	Localized	% Identified
x_2	273	273	100
x_4	298	298	100
x_5	296	296	100
x_7	287	287	100
x_9	294	294	100
x_{10}	264	264	100
x_{11}	317	316	99.7
x_{14}	336	333	99.1

Multivariate Type II Attack (MII)

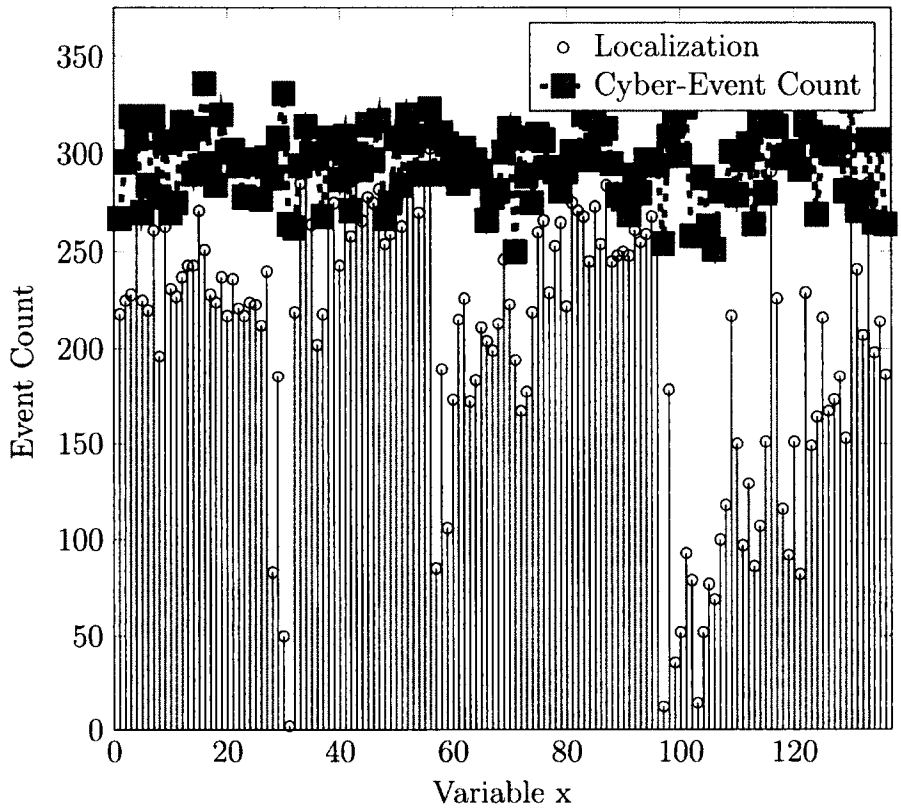

Figure E.16: IEEE 14-Bus With Line Flows MII Localization Results

Table E.17: IEEE 14-Bus Without Line Flows MII Localization Results for State Variables x1-x68

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_1	267	218	81.6	x_{35}	301	246	81.7
x_2	296	225	76.0	x_{36}	313	223	71.2
x_3	319	228	71.4	x_{37}	250	194	77.6
x_4	308	271	87.9	x_{38}	308	167	54.2
x_5	270	225	83.3	x_{39}	289	177	61.2
x_6	284	220	77.4	x_{40}	275	219	79.6
x_7	319	261	81.8	x_{41}	310	260	83.8
x_8	278	196	70.5	x_{42}	307	266	86.6
x_9	306	263	85.9	x_{43}	293	229	78.1
x_{10}	270	231	85.5	x_{44}	291	253	86.9
x_{11}	275	227	82.5	x_{45}	281	265	94.3
x_{12}	316	237	75	x_{46}	291	222	76.2
x_{13}	308	243	78.8	x_{47}	301	275	91.3
x_{14}	290	243	83.7	x_{48}	300	271	90.3
x_{15}	313	271	86.5	x_{49}	320	268	83.7
x_{16}	336	251	74.7	x_{50}	297	245	82.4
x_{17}	295	228	77.2	x_{51}	318	273	85.8
x_{18}	284	224	78.8	x_{52}	310	254	81.9
x_{19}	320	237	74.0	x_{53}	313	284	90.7
x_{20}	301	217	72.0	x_{54}	295	245	83.0
x_{21}	302	236	78.1	x_{55}	279	248	88.8
x_{22}	294	221	75.1	x_{56}	277	250	90.2
x_{23}	278	217	78.0	x_{57}	269	248	92.1
x_{24}	297	224	75.4	x_{58}	289	261	90.3
x_{25}	295	223	75.5	x_{59}	280	255	91.0
x_{26}	277	212	76.5	x_{60}	297	259	87.2
x_{27}	298	240	80.5	x_{61}	297	268	90.2
x_{28}	288	83	28.8	x_{62}	294	257	87.4
x_{29}	308	185	60.0	x_{63}	254	12	4.72
x_{30}	331	50	15.1	x_{64}	309	178	57.6
x_{31}	264	2	0.75	x_{65}	316	36	11.3
x_{32}	262	219	83.5	x_{66}	299	52	17.3
x_{33}	294	285	96.9	x_{67}	324	93	28.7
x_{34}	314	296	94.2	x_{68}	258	79	30.6

Table E.18: IEEE 14-Bus Without Line Flows SII Localization Results for State Variables x69-x136

x_i	Number of Events	Number Localized	% Identified	x_i	Number of Events	Number Localized	% Identified
x_{69}	300	264	88	x_{103}	258	14	5.42
x_{70}	298	202	67.7	x_{104}	288	52	18.0
x_{71}	268	218	81.3	x_{105}	263	77	29.2
x_{72}	308	295	95.7	x_{106}	251	69	27.4
x_{73}	303	275	90.7	x_{107}	281	100	35.5
x_{74}	287	243	84.6	x_{108}	281	118	41.9
x_{75}	309	285	92.2	x_{109}	301	217	72.0
x_{76}	271	258	95.2	x_{110}	279	150	53.7
x_{77}	300	288	96	x_{111}	297	97	32.6
x_{78}	292	266	91.0	x_{112}	305	129	42.2
x_{79}	315	278	88.2	x_{113}	264	86	32.5
x_{80}	297	275	92.5	x_{114}	315	107	33.9
x_{81}	317	282	88.9	x_{115}	280	151	53.9
x_{82}	267	254	95.1	x_{116}	319	291	91.2
x_{83}	275	259	94.1	x_{117}	314	226	71.9
x_{84}	308	286	92.8	x_{118}	298	116	38.9
x_{85}	284	263	92.6	x_{119}	299	92	30.7
x_{86}	320	292	91.2	x_{120}	301	151	50.1
x_{87}	306	287	93.7	x_{121}	292	82	28.0
x_{88}	290	270	93.1	x_{122}	315	229	72.6
x_{89}	309	289	93.5	x_{123}	311	149	47.9
x_{90}	323	303	93.8	x_{124}	269	164	60.9
x_{91}	290	85	29.3	x_{125}	304	216	71.0
x_{92}	311	189	60.7	x_{126}	308	167	54.2
x_{93}	305	106	34.7	x_{127}	300	173	57.6
x_{94}	294	173	58.8	x_{128}	306	185	60.4
x_{95}	285	215	75.4	x_{129}	281	153	54.4
x_{96}	303	226	74.5	x_{130}	327	304	92.9
x_{97}	289	172	59.5	x_{131}	271	241	88.9
x_{98}	297	183	61.6	x_{132}	280	207	73.9
x_{99}	291	211	72.5	x_{133}	307	285	92.8
x_{100}	266	204	76.6	x_{134}	265	198	74.7
x_{101}	278	199	71.5	x_{135}	307	214	69.7
x_{102}	281	213	75.8	x_{136}	264	186	70.4

BIBLIOGRAPHY

[1] J. Glover, *Power System Analysis and Design*, 5th ed. Stamford, CT: Cengage Learning, 2012.

[2] W. Stevenson, *Elements of Power System Analysis*, 4th ed. New York, NY: McGraw-Hill, 1982.

[3] T. Macaulay, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.* Boca Raton, FL: CRC Press, 2012.

[4] B. Miller and D. Rowe, "A survey of SCADA and critical infrastructure incidents," in *Proc. of ACM Conference on Research in Information Technology*, 2012, pp. 51–56.

[5] Z. Lukszo, *Securing Electricity Supply in the Cyber Age: Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure.* Dordrecht, NY: Springer, 2010.

[6] L. Grigsby, *Power System Stability and Control.* Boca Raton, FL: CRC Press, 2007.

[7] T. Gönen, *Electric Power Distribution System Engineering.* Boca Raton, FL: CRC Press, 2008.

[8] U.S. Department of Homeland Security, "Cyber security procurement language for control systems," Washington DC, September 2009.

[9] National Science and Technology Council, "A policy framework for the 21st century grid: Enabling our secure energy future," Washington DC, June 2011.

[10] P. Myrda, "Panel discussion: Great lakes symposium on smart grid and the new energy economy," Chicago, Illinois, September 2013.

[11] U.S. Department of Homeland Security, "Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies," Washington DC, October 2009.

[12] ICS-CERT, U.S. Department of Homeland Security, "Project shine," *ICS-CERT Monitor*, vol. October-December, 2012.

[13] "Security response: Targeted attacks against the energy sector," White Paper, Symantec, January 2014.

[14] ICS-CERT, U.S. Department of Homeland Security, "Incident response activity," *ICS-CERT Monitor*, vol. January-April, 2014.

[15] "Annual security report," White Paper, Cisco, January 2014, www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf [June 20 2014].

[16] ICS-CERT, U.S. Department of Homeland Security, "Incident response activity," *ICS-CERT Monitor*, vol. October-December, 2014.

[17] U.S. Senate, Committee on Homeland Security & Government Affairs, "Threats to the homeland," Hearing, 14 November 2013, Washington DC.

[18] "Common cyber security vulnerabilities observed in control system assessments," White Paper, Idaho National Laboratory, November 2008.

[19] *Energy Independence and Security Act of 2007.* [Washington, D.C. :U.S. G.P.O.: Supt. of Docs., U.S. G.P.O., distributor], 2007.

[20] *The American Recovery and Reinvestment Act of 2009*, ser. Report 111th Congress, 1st session, House of Representatives: 111-4. [Washington, D.C. : U.S. G.P.O.], 2009.

[21] U.S. Department of Energy, "The american recovery and reinvestment act of 2009 smart grid investment grant program progress report," July 2012.

[22] U.S. Department of Energy, "Smartgrid integrated project reporting information system," 2014, www.sipris.energy.gov [June 29, 2014].

[23] U.S. Department of Energy, "Advanced metering infrastructure and customer systems smart meters deployed," Report, 2014.

[24] D. Geelen, G. van Kempen, F. van Hoogstraten, and A. Liotta, "A wireless mesh communication protocol for smart-metering," in *Proc. ICNC*, January 2012, pp. 343 –349.

[25] B. Lichtensteiger, B. Bjelajac, C. Mu andller, and C. Wietfeld, "Rf mesh systems for smart metering: System architecture and performance," in *Proc. SmartGridComm*, October 2010, pp. 379 –384.

[26] S. Brinkhaus and D. Carluccio, "Smart hacking for privacy," in *Proc. 28th Chaos Comm. Congr.*, 2011.

[27] J. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, pp. 23–40, Feburary 2011.

[28] L. Grigsby, *Power Systems.* Boca Raton, FL: CRC Press, 2007.

[29] F. Schweppe and J. Wildes, "Power system static-state estimation, part i: Exact model," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–125, 1970.

[30] Y. Gu, T. Liu, D. Wang, X. Guan, and Z. Xu, "Bad data detection method for smart grids based on distributed state estimation," in *Proc. ICC*, 2013, pp. 4483–4487.

[31] A. Kumar, *Knowledge Discovery Practices and Emerging Applications of Data Mining Trends and New Domains.* Hershey, PA: Information Science Reference, 2011.

[32] S. Dua, *Data Mining and Machine Learning in Cybersecurity.* Boca Raton: CRC Press, 2011.

[33] T. M. Nguyen, *Complex Data Warehousing and Knowledge Discovery for Advanced Retrieval Development : Innovative Methods and Applications.*, ser. Premier Reference Source. Hershey, PA: Information Science Reference, 2010.

[34] N. Rountree and Y. S. Koh, *Rare Association Rule Mining and Knowledge Discovery: Technologies for Infrequent and Critical Event Detection.* Hershey, PA: Information Science Reference, 2010.

[35] R. Sarker, *Heuristics and Optimization for Knowledge Discovery.* Hershey, PA: Idea Group Pub, 2002.

[36] W. Hsu, *Temporal and Spatio-temporal Data Mining.* Hershey, PA: IGI Pub, 2008.

[37] K. Cios, W. Pedrycz, R. Swiniarski, and L. Kurgan, *Data Mining: a Knowledge Discovery Approach.* New York London: Springer, 2010.

[38] N. Hatziargyriou, S. Papathanassiou, and M. Papadopoulos, "Decision trees for fast security assessment of autonomous power systems with a large penetration from renewables," *IEEE Transactions on Energy Conversion*, vol. 10, no. 2, pp. 315–325, 1995.

[39] H. Mori, "State-of-the-art overview on data mining in power systems," in *Proc. PSCE*, 2006, pp. 33–34.

[40] L. Wehenkel, *Automatic Learning Techniques in Power Systems.* Boston, MA: Kluwer Academic, 1998.

[41] J. Momoh and M. El-Hawary, *Electric Systems, Dynamics, and Stability with Artificial Intelligence Applications.* New York, NY: M. Dekker, 2000.

[42] H. Wang and K. C. Sevcik, "Histograms based on the minimum description length principle," *The Internal Journal on Very Large Data Bases*, vol. 17, no. 3, pp. 419–442, May 2008.

[43] K. Lo, P. Zeng, E. Marchand, and A. Pinkerton, "New bad-data detection and identification technique based on rotation of measurement order for sequential state estimation [for power systems]," *IEEE Proceedings of Generation, Transmission and Distribution*, vol. 139, no. 5, pp. 387–401, 1992.

[44] X. Nian-de, W. Shi-ying, and Y. Er-keng, "A new approach for detection and identification of multiple bad data in power system state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. 101, no. 2, pp. 454–462, 1982.

[45] L. Liu, M. Esmalifalak, and Z. Han, "Detection of false data injection in power grid exploiting low rank and sparsity," in *Proc. ICC*, 2013, pp. 4461–4465.

[46] N. H. Abbasy and W. El-Hassawy, "Power system state estimation: Ann application to bad data detection and identification," in *Proc. AFRICON*, vol. 2, 1996, pp. 611–615.

[47] H. Shyh-Jier and L. Jeu-Min, "Artificial neural network enhanced by gap statistic algorithm applied for bad data detection of a power system," in *Proc. T&D-AP*, vol. 2, 2002, pp. 764–768.

[48] S. P. Teeuwsen and I. Erlich, "Neural network based multi-dimensional feature forecasting for bad data detection and feature restoration in power systems," in *Proc. PES-GM*, 2006, p. 6.

[49] Y. Yu, "A survey of anomaly intrusion detection techniques," *ACM Journal of Computing Sciences in Colleges*, vol. 28, no. 1, pp. 9–17, October 2012.

[50] D. Denatious and A. John, "Survey on data mining techniques to enhance intrusion detection," in *Proc. ICCCI*, 2012, pp. 1–5.

[51] M. Shyu, T. Quirino, Z. Xie, S.-C. Chen, and L. Chang, "Network intrusion detection through adaptive sub-eigenspace modeling in multiagent systems," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 2, no. 3, September 2007.

[52] S. J. Stolfo, W. Lee, P. K. Chan, W. Fan, and E. Eskin, "Data mining-based intrusion detectors: An overview of the columbia ids project," *ACM Special Interest Group on Management of Data*, vol. 30, no. 4, pp. 5–14, December 2001.

[53] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Journal of Computer Surveys*, vol. 41, no. 3, pp. 15:1–15:58, July 2009.

[54] M. Coutinho, G. Lambert-Torres, L. da Silva, J. da Silva, J. Neto, and H. Lazarek, "Improving a methodology to extract rules to identify attacks in power system critical infrastructure: New results," in *Proc. T&D*, 2008, pp. 1–6.

[55] B. D. Pitt and D. Kitschen, "Application of data mining techniques to load profiling," in *Proc. PICA*, 1999, pp. 131–136.

[56] T. Van Cutsem, L. Wehenkel, M. Pavella, B. Heilbronn, and M. Goubin, "Decision tree approaches to voltage security assessment," *IEEE Proceedings of Generation, Transmission and Distribution*, vol. 140, no. 3, pp. 189–198, 1993.

[57] N. Hatziargyriou, G. Contaxis, and N. C. Sideris, "A decision tree method for on-line steady state security assessment," *IEEE Transactions on Power Systems*, vol. 9, no. 2, pp. 1052–1061, 1994.

[58] C.-C. Yang and Y.-Y. Hsu, "Estimation of line flows and bus voltages using decision trees," *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1569–1574, 1994.

[59] N. Wallace and T. Atkison, "Observing industrial control system attacks launched via metasploit framework," in *Proc. ACMSE*, 2013, p. 22.

[60] H. Hashimoto and T. Hayakawa, "Distributed cyber attack detection for power network systems," in *Proc. CDC-ECC*, December 2011, pp. 5820–5824.

[61] F. Dorfler, F. Pasqualetti, and F. Bullo, "Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach," in *Proc. Ann. Allerton Conf*, September 2011, pp. 1486–1491.

[62] A. Tajer, S. Kar, H. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. SmartGridComm*, October 2011, pp. 202–207.

[63] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Proc. PES-GM*, July 2011, pp. 1–8.

[64] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, March 2014.

[65] M. Coutinho, G. Lambert-Torres, L. da Silva, H. G. Martins, H. Lazarek, and J. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," in *Proc. DEST*, June 2009, pp. 733–738.

[66] M. Coutinho, G. Lambert-Torres, L. da Silva, H. G. Martins, and H. Lazarek, "Improving detection attacks in electric power system critical infrastructure using rough classification algorithm," in *Proc. ICoFCS*, November 2007, pp. 18–23.

[67] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[68] J. Kogan, C. K. Nicholas, and M. Teboulle, *Grouping Multidimensional Data: Recent Advances in Clustering.* Springer, 2006.

[69] C. Huberty, *Applied Discriminant Analysis.* New York, NY: Wiley, 1994.

[70] S. Deladreue, F. Brouaye, P. Bastard, and L. Peligry, "Application of anova methodology to the uncertainties management in power system planning in an open market environment," in *Proc. Porto Power Tech*, vol. 1, 2001, p. 4.

[71] Y. Zhang, J. Zhang, J. Ma, and Z. Wang, "Fault detection based on discriminant analysis theory in electric power system," in *Proc. SUPERGEN*, 2009, pp. 1–5.

[72] Y. Zhang, Z. Wang, and J. Zhang, "Bayesian fault detection based on wams/pmu measurement system," in *PES-GM*, 2012, pp. 1–6.

[73] G. Garcia, J. Bernussou, and M. Berbiche, "Pattern recognition applied to transient stability analysis of power systems with modeling including voltage and speed regulation," *IEEE Proceedings of Electric Power Applications*, vol. 139, no. 4, pp. 321–335, 1992.

[74] S. Kollias, *International Conference Artificial Neural Networks.* Berlin New York: Springer, September 2006.

[75] B. Everitt, *The Cambridge Dictionary of Statistics.* Cambridge New York: Cambridge University Press, 2010.

[76] W. Härdle and L. Simar, *Applied Multivariate Statistical Analysis.* Heidelberg New York: Springer, 2012.

[77] F. Grubbs, "Procedures for detecting outlying observations in samples," *Technometrics*, vol. 11(1), pp. 1–21, 1969.

[78] W. Stefansky, "Rejecting outliers in factorial designs," *Technometrics*, vol. 14, pp. 469–479, 1972.

[79] G. Yuma and K. Kusakana, "Damping of oscillations of the ieee 14 bus power system by svc with statcom," in *Proc. EEEIC*, May 2012, pp. 502–507.

[80] M. Moghbel, H. Mokui, M. Masoum, and M. Mohseni, "Reactive power control of dfig wind power system connected to ieee 14 bus distribution network," in *Proc. AUPEC*, September 2012, pp. 1–7.

[81] D. Fitiwi and K. S. R. Rao, "Assessment of ann-based auto-reclosing scheme developed on single machine-infinite bus model with ieee 14-bus system model data," in *Proc. TENCON*, Januarary 2009.

[82] N. Hashim, N. Hamzah, M. Latip, and A. A. Sallehhudin, "Transient stability analysis of the ieee 14-bus test system using dynamic computation for power systems (dcps)," in *Proc. ISMS*, Feburary 2012, pp. 481–486.

[83] N. Mithulananthan, C. A. Canizares, and J. Reeve, "Indices to detect hopf bifurcation in power systems," in *Proc. NAPS*, 2000, pp. 15–18.

[84] T. Overbye, "A power flow measure for unsolvable cases," *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1359–1365, August 1994.

[85] A. Feinstein, *Multivariable Analysis: an Introduction.* New Haven, Conn: Yale University Press, 1996.

[86] MATLAB, *version 7.14.0.739 (R2012a).* Natick, Massachusetts: The MathWorks Inc., 2012.

[87] J. Brockman, *The Next Fifty Years: Science in the First Half of the Twenty-First Century.* New York: Vintage Books, 2002.

[88] F. de Leon and A. Sernlyen, "Iterative solvers in the newton power flow problem: preconditions, inexact solutions and partial jacobian updates," *IEEE Proceedings of Generation, Transmission and Distribution*, vol. 149, no. 4, pp. 479–484, July 2002.

[89] H. Brown, G. Carter, H. Happ, and C. Person, "Power flow solution by impedance matrix iterative method," *IEEE Transactions on Power Apparatus and Systems*, vol. 82, no. 65, pp. 1–10, April 1963.

[90] A. Semlyen, "Fundamental concepts of a krylov subspace power flow methodology," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1528–1537, August 1996.

[91] K. Talib, I. Musirin, M. Kalil, and M. Idris, "Power flow solvability identification and calculation algorithm using evolutionary programming technique," in *Proc. SCOReD*, December 2007, pp. 1–5.

[92] L. Hu, J. Zhao, J. Hongjie, X. Guo, and Q. Zeng, "Computing the boundary of simple power system feasible region based on the optimization method," in *Proc. ISGT*, May 2012, pp. 1–6.

[93] G. Sun, L. Zhang, and H. Sun, "Face recognition based on symmetrical weighted pca," in *Proc. CSSS*, June 2011, pp. 2249–2252.

[94] K. Guo, X. Xu, F. Qiu, and J. Chen, "A novel incremental weighted pca algorithm for visual tracking," in *Proc. ICIP*, September 2013, pp. 3914–3918.

[95] R. Van de Plas, B. De Moor, and E. Waelkens, "Imaging mass spectrometry based exploration of biochemical tissue composition using peak intensity weighted pca," in *Proc. LiSSA*, November 2007, pp. 209–212.

[96] J. Sotelo, E. Trejos, D. Ordonez, D. Cuesta-Frau, and G. Dominguez, "Weighted-pca for unsupervised classification of cardiac arrhythmias," in *Proc. EMBC*, August 2010, pp. 1906–1909.

VITA

Nathan Wallace was born in Alexandria, Louisiana to Patrick and Patricia Wallace of Lecompte, Louisiana. He graduated from Alexandria Senior High in 2007 where he focused on leadership through the Marine Corps Junior Reserve Officer Training Corps program. Afterwards, he joined Louisiana Tech University completing his undergrad in May 2011 with a Bachelor of Science in Electrical Engineering and a Bachelor of Science in Physics. It was upon completion of these programs when he become a Licensed Engineering Intern (EIT) in the state of Louisiana. In May 2013 he received a Master of Science in Electrical Engineering.

He has spent his graduate tenure working as a graduate research assistant for the Digital Forensics and Control System Security Lab at Louisiana Tech University. In this capacity he has mentored numerous high school and undergraduate students in the areas of digital forensics and cybersecurity. Lastly he has been inducted into the Eta Kappa Nu and Sigma Pi Sigma honor societies and holds active memberships in the Institute of Electrical and Electronic Engineers (IEEE), and the Association of Computing Machinery (ACM).