

**Improved Monitoring and Security Assessment of Power
Systems using Machine Learning Techniques and Phasor
Measurements along-with their Optimal Placement**

Ph.D. Thesis

by

T.VENKATESH



**DISCIPLINE OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE**

April 2018

**Improved Monitoring and Security Assessment of Power
Systems using Machine Learning Techniques and Phasor
Measurements along-with their Optimal Placement**

A THESIS

*Submitted in partial fulfillment of the
requirements for the award of the degree
of*

DOCTOR OF PHILOSOPHY

by

T.VENKATESH



**DISCIPLINE OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE**

APRIL 2018



INDIAN INSTITUTE OF TECHNOLOGY INDORE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **Improved Monitoring and Security Assessment of Power Systems using Machine Learning Techniques and Phasor Measurements along-with their Optimal Placement** in the partial fulfillment of the requirements for the award of the degree of **DOCTOR OF PHILOSOPHY** and submitted in the **DISCIPLINE OF ELECTRICAL ENGINEERING, Indian Institute of Technology Indore**, is an authentic record of my own work carried out during the time period from January 2013 to March 2018 under the supervision of Dr. Trapti Jain, Associate Professor, Indian Institute of Technology Indore, India.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other institute.

Signature of the student with date
(T.VENKATESH)

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Signature of Thesis Supervisor with date
(Dr. TRAPTI JAIN)

T.Venkatesh has successfully given his Ph.D. Oral Examination held on -----.

Signature of Chairperson (OEB)
Date:

Signature of External Examiner
Date:

Signature of Thesis Supervisor
Date:

Signature of PSPC Member #1
Date:

Signature of PSPC Member #2
Date:

Date:

Signature of Convener, DPGC
Date:

Signature of Head of Discipline
Date:

ACKNOWLEDGEMENTS

I take this opportunity to acknowledge my heartfelt gratitude to many people who have directly or indirectly helped me throughout my Ph.D. candidature.

I would like to thank my supervisor, Dr. Trapti Jain, for the patient guidance, encouragement and professional advice she has provided throughout my time as her student. I have been extremely lucky to have a supervisor who cared so much about my work, and who responded to my silly questions and queries so promptly and patiently. She was and remains my best role model for a scientist, mentor and teacher. Her broad knowledge, technical writing skills, encouragement for exploration of new techniques and logical thinking have been helpful to progress in the right direction. More importantly, her qualities of being committed, confident, credible, responsible, supportive, and her forgiving nature created a relaxed learning environment. In particular, I appreciate and value her invaluable guidance, critical reviews, coordination, intellectual exchanges and the support given throughout the study period. I am very fortunate to have worked with her and always admire her dedication to research. Finally, I would be ever grateful for her untiring efforts and strong commitment, which are instrumental in completing this PhD thesis within one month after my PhD open seminar.

I would like to thank my research progress committee members Dr. Amod C. Umarikar and Dr. Abhishek Srivastava for their insightful comments, support throughout the course of my research. I have been constantly encouraged by Dr. I.A. Palani by his valuable advice and suggestions whenever required. I also thank Dr. Shanmugam Dinakaran for his tremendous advice and suggestions in my personal life.

I will be ever grateful to Dr. Satya S. Bulusu (Chairman - PhD Oral Examination Board) for his immense help and support in the final stage of my PhD career. I am also very grateful to Dr. M. Anbarasu and Dr. Srivatsan Vasudevan for their unconditional psychological support, and encouragement throughout my research. Also, for listening to all my problems and frustrations very patiently, and advising me to become an ethical person both professionally and personally. Also, I am thankful to Ms. Monika Gupta for her valuable advice and useful insights, which will be helpful to me throughout my life.

I express my gratitude to Prof. R. Gnanasss, Professor, Pondicherry Engineering College who inspired and motivated me to carry out research, and cultivating a challenging nature in me ever since my graduation. I'm greatly indebted to Dr. E. Marriappane, Professor, Dr. Pauls Engineering College for his unconditional support and for generously extending his support and guidance at all times during this journey. I would like to extend my gratitude to Dr. Sanjeevi Padmanabhan (Aalborg University, Denmark) for his constant encouragement throughout my career.

I also express my thanks to Mr. Parthiban, Technical staff, IIT Indore, who has been more than a brother and helped at all possible means during initial days of my PhD career. The support staff in EE office (Ms. Shagufta Rahim, Mr. Raghavendra Hanswal, Mr. Ram Kumar and Mr. Ravindra Choughan), library (Mr. Satish Bisen), academic office (Mr. Tapesh

Parihar), HOSE office (Ms. Ujjvala), T&P office (Ms. Mamata) and the security guards have made me feel homely in the department. Every morning I receive a smiling greeting from them and any of my requests are treated specially. I owe all of them my deep gratitude.

During this hard career, many friends have supported my family financially and medically. I would like to give special mention to my best buddy Mohammed Mubarak, his wife and their lovable son for their uncountable financial help and support at all times when my family was in need. I would like to thank my friends Dr. R. Parthasarathy (MD, JIPMER), Dr. Ananth (IIIT Kanchipuram) and Dr. Venkat Phanendra Babu (NIT Warangal) who helped me to pay my entire PhD tuition fees for all these years. I will be ever indebted to these people for their support in paying my monthly expenses and medical bills of my parents since past 5 years. I pay my sincere thanks to Arun and Mathi for taking care of my parents during my absence. I thank my legal advisor Mr. Tharani Rajkumar (Puducherry Law Association) for his tremendous help and playing a vital role during this difficult journey. I will be failing as a human if I don't mention Anjali and Shalu for their unconditional love on my parents. I thank my friends Dr. Prakash (IIT Indore) Dr. Akash (ASU, USA) and wish to cherish all the moments with him throughout my life. I would like to pay my sincere thanks to Sofana (VIT Chennai) for her constant encouragement and help in my personal life. I would like to thank few of my institute colleagues Dr. Rohit, Dr. Devendra, Dr. Rajeev, Dr. Sunil Pathak and Dr. Amitesh for their kind support during my career at IIT Indore.

Finally my parents, who educated me, for always believing in my capabilities and waiting for me patiently to complete this wonderful and tough journey. Then my gratitude to my lovable sister, for her loving care and always being there for me during good and bad times. And, I thank the management of VIT University Dr. G. Viswanathan (Chancellor), Dr. Shankar Viswanathan (Vice President) and Ms. Kadambari Viswanathan (Assistant Vice President) for their tremendous and unconditional support given to me. I also thank Dr. Gunasekaran (Vice Chancellor, VIT Bhopal), Dr. Francis Xavier, Dr. Sriram, Dr. Shishir and my fellow colleagues Dr. Sugavaneshwar, Dr. Divya Haridas and Dr. Soundarajan, Dr. Deepika Masand for their beloved care and affection on me. Without them, I would not be in the position, where I am today.

VENKATESH.T

*This thesis is dedicated to my Friends
who made this PhD dream a reality*

ABSTRACT

Phasor Measurement Units (PMUs) are able to provide fast and accurate synchronized measurements than the conventional Supervisory Control And Data Acquisition (SCADA) systems. These synchronized measurements have been recently employed for various power system applications due to their ability of providing updated system information at a particular time. Thus, the synchrophasor technology can play a vital role in enhancing the overall system monitoring, protection and control of power systems. This thesis aims to utilize these synchronized measurements to build some intelligent classifiers for the fast and accurate prediction of power system security. The first part of this thesis is concerned about the optimal placement of PMUs in order to achieve complete observability of the system during normal operation as well as during contingencies. The placement methodology proposed in this thesis is based on a new intelligent search technique, which works in two stages. Stage I uses Best First Search (BFS) algorithm to determine the sub-optimal placement locations of PMUs and stage II uses pruning to remove the redundant PMU locations from the results obtained in stage I. Thus, the proposed method offers complete topological observability with a placement set containing minimum number of PMUs. Further, the proposed method is able to incorporate the presence of single and multiple flow measurements in the system.

Cascaded failures, which often result in islanding, are considered as a severe disturbance and therefore, maintaining system observability during such disturbances is of utmost importance. Considering this perspective, the BFS based two stage method has been further extended to find the optimal locations of PMUs for keeping the system observable during cascaded failures. A topology based algorithm has also been proposed to identify whether a particular cascaded event leads to islanding condition or non-islanding condition. In addition to observability, measurement redundancy is also incorporated in the placement scheme to enhance the state estimation process.

The synchronized measurements are then utilized for developing an improved monitoring and assessment scheme for power system security using intelligent classifiers. To achieve this, a new framework for Static Security Assessment (SSA) and Transient Security Assessment (TSA) has been presented. The proposed framework for SSA consists of four classifiers, where classifier I is used to predict the static security status of the system as secure or insecure for a particular loading condition and classifier II determines the type of violations (either line overload/bus voltage violation or both) that causes insecurity in the power system. Classifier III is used to predict the security status of that particular loading condition with respect to all probable N-1 contingencies. Similarly, classifier IV predicts the type of violations causing insecurity in those insecure patterns identified by classifier III. The inputs

to these classifiers are the synchronized measurements viz. bus voltage phasors, branch real and reactive power flows measured by PMUs. Some of the intelligent classifiers which have been utilized for this assessment include Wavelet Support Vector Machine (WSVM), Case Based Reasoning (CBR) and AdaBoost algorithm. These classifiers are found to have better generalization capability than the traditional classifiers used for security assessment. Simulation results obtained using WSVM, CBR and AdaBoost classifiers are compared with the results obtained using existing techniques.

For TSA, the measured rotor angles of the generators are used as inputs to the proposed classifier models. This TSA framework consists of three classifier models in which classifier I determines the transient security status and classifier II is used to determine the generator coherency. Classifier III is a hybrid classifier, which determines the individual generator synchronism state for a given operating condition. This hybrid classifier consists of an array of parallel classifiers, where one classifier is assigned to each generating unit of the power system. Finally, the proposed approach is implemented and tested on standard benchmark systems such as IEEE 14-bus, IEEE 30-bus and on a practical Indian 246-bus networks. Simulation results reveal that the proposed method can enhance the overall monitoring and assessment of power system with the use of synchronized measurements and with classifiers having high generalization capability.

Publications from the Thesis

Journal Papers:

1. Venkatesh.T, Jain.T. “Synchronized Measurements Based Transient Security Assessment of Power Systems using AdaBoost Classifiers.” *IET Generation, Transmission & Distribution (Provisionally Accepted)*, Mar. 2019 (IF: 2.618).
2. Venkatesh T, Jain T. “AdaBoost Classifiers for Phasor Measurements based Security Assessment of Power Systems.” *IET Generation, Transmission & Distribution*, 12(8): 1747–1755, Jan. 2018 (IF: 2.618).
3. Venkatesh T, Jain T. “Synchronized Measurements based Power System Static Security Assessment and Classification Using Case Based Reasoning Classifiers.” *Computers & Electrical Engineering*, 68: 513–525, Jan. 2018 (IF: 1.747).
4. Venkatesh T, Jain T. “Placement of Synchronized Measurements for Power System Observability during Cascaded Outages using Intelligent-search Technique.” *International Journal of Emerging Electric Power Systems*, 18(6):(Press), Dec. 2017 (IF: 0.86).
5. Venkatesh T, Jain T. “Intelligent-search technique based strategic placement of synchronized measurements for power system observability.” *Expert System with Applications*, 42(10): 4768–4777, Jun. 2015 (IF: 3.928).

Conference Papers:

1. Venkatesh T, Jain T. “Wide Area Static Security Assessment of Power Systems using Wavelet Support Vector Machine.” *In Proc (Offline): IEEE PES General Meeting*, Chicago, USA, Jul. 16–20, 2017.
2. Venkatesh T, Jain T. “Optimal PMU placement using best first search algorithm with pruning.” *In Proc: Eigtheenth National Power Systems Conference*, IIT Guwahati, India, Dec. 18–29, 2014.

Contents

ABSTRACT	i
LIST OF PUBLICATIONS	iii
LIST OF FIGURES	ix
LIST OF TABLES	ix
LIST OF ABBREVIATIONS	xii
1 Introduction	1
1.1 Background	1
1.2 Power System Security Analysis	3
1.2.1 Operating States of a Power System	3
1.2.2 Major Components of Security Assessment	5
1.3 Phasor Measurement Units	6
1.4 Applications of Machine Learning Techniques for Power System Security Assessment	8
1.4.1 Decision Trees	8
1.4.2 Artificial Neural Networks	9
1.4.3 Support Vector Machines	9
1.5 State-of-the-Art	10
1.5.1 Optimal Placement of PMUs	10
1.5.2 Phasor Measurements based SA Methods	14
1.5.3 Applications of Machine Learning Concepts for SA	15
1.6 Motivation and Objectives	16
1.7 Thesis Outline	18
2 Optimal Placement of PMUs using Intelligent search Method	21
2.1 Introduction	21
2.2 Observability Rules	22
2.3 Proposed Approach	23
2.3.1 Modelling of Zero Injection Buses (ZIBs)	28
2.3.2 Optimal PMU placement during single branch outage	30
2.3.3 Optimal PMU placement during single PMU outage	30
2.3.4 PMU Placement in the presence of Conventional Flow Measure- ments (CFM)	32
2.4 Case Studies	33
2.4.1 Optimal PMU placement during system intact condition	35

2.4.2	Optimal PMU placement during contingency conditions	35
2.4.3	Optimal PMU placement during the presence of CFM	38
2.5	Conclusions	39
3	Optimal Placement of PMUs Considering Cascaded Failures	40
3.1	Introduction	40
3.2	Proposed Approach	42
3.2.1	Simulation of Cascaded Failures	42
3.2.2	Proposed Redundant Observability method	44
3.3	Case Studies	46
3.3.1	OPP during Cascaded Failures	46
3.3.2	OPP during Cascaded Failures with Contingencies	49
3.3.3	OPP considering Measurement Redundancy	53
3.4	Conclusions	55
4	Review of Various Machine Learning Techniques	56
4.1	Introduction	56
4.1.1	Literature Review	57
4.2	Wavelet Support Vector Machine (WSVM)	59
4.2.1	Support Vector Machine (SVM)	59
4.2.2	Wavelet Analysis	60
4.2.3	Wavelet SVM	61
4.3	Case Based Reasoning (CBR)	62
4.3.1	Case Base Representation	63
4.3.2	Retrieval	63
4.3.3	Revise using Heuristics and Adaptation	64
4.3.4	Updation of Weight Vector	65
4.4	AdaBoost Classifier with SVM as weak Classifier	69
4.4.1	Weak Classifier	69
4.4.2	AdaBoosting Algorithm	70
4.5	Conclusions	72
5	Static Security Assessment using Different Machine Learning Techniques	73
5.1	Introduction	73
5.2	Proposed Static Security Index	74
5.3	Proposed Framework of SSA	75
5.3.1	Design of Monitoring and Security Assessment System	76
5.3.2	Input Data Generation	77
5.3.3	Dimensionality Reduction of Phasor Measurements	77
5.3.4	Synthetic Minority Oversampling Technique (SMOTE)	79
5.4	Case Studies & Discussions	80
5.4.1	Details of Input Data	80
5.4.2	Comparison of WSVM, AdaBoost & CBR Algorithm	84
5.4.3	Computational Requirement for Online Implementation	86
5.4.4	Results of SMOTE for Class Imbalance Problem	87
5.4.5	Analysis of the Proposed SSA Results with Existing Methods	88
5.5	Conclusions	92

6	Transient Security Assessment using Machine Learning Techniques	93
6.1	Introduction	93
6.2	Data Generation & Rotor Trajectory Index	95
6.3	Proposed Synchronism Status Index	96
6.4	Proposed Framework of TSA	96
6.5	Case Studies	99
6.6	Conclusions	107
7	Conclusions	108
7.1	Discussion and Conclusions of the Work	108
7.2	Major Contributions of the Work	111
7.3	Future Scope	111
	REFERENCES	112

List of Figures

1.1	Various Operating States of a Power System [1]	4
1.2	Functional Block Diagram of a Phasor Measurement Unit	7
2.1	Proposed Method for PMU Placement	24
2.2	Flowchart of Stage I of Optimal PMU Placement	26
2.3	Optimal PMU Placement for a Four Bus System (a) With No ZIBs, and (b) Considering Bus 3 as a ZIB	28
2.4	Logical Representation of Modelling of ZIBs	30
2.5	Flowchart of Optimal PMU Placement during Single PMU Outage	31
2.6	With Single (a) and Multiple CFMs (b) Connected to a Bus ' k '	32
3.1	Flowchart for Island Identification	43
3.2	Flowchart of the Proposed Redundant Observability Method	45
3.3	Splitting of IEEE 14-bus System	48
3.4	Splitting of IEEE 30-bus System	48
4.1	Schematic Diagram of CBR system	62
4.2	Architecture of AdaBoost Algorithm	70
5.1	Detailed Framework of Static Security Assessment	76
5.2	Illustration of SMOTE Sample Generation	80
6.1	Proposed Framework of Transient Security Assessment	97
6.2	Proposed Structure of Hybrid Classifier for Synchronism Status Detection . .	98

List of Tables

2.1	Details of the Three Test Systems	34
2.2	Optimal Number of PMUs during System Intact Condition	34
2.3	Optimal PMU Locations for the System Intact Case with No PMUs at ZIBs	35
2.4	Optimal PMU Placement during Single Branch Outage	36
2.5	Optimal PMU Placement during Single PMU Outage	37
2.6	Comparative Study of the Proposed Method with the Existing Methods	37
2.7	Branches with Flow Measurements	38
2.8	Optimal PMU Placement during the Presence of CFM	38
3.1	Post-contingency Leading to Cascaded Outages with Non-Islanding Operation	47
3.2	Post-contingency Leading to Cascaded Outages with Islanding Operation	47
3.3	Optimal Locations of PMUs during Cascaded Failures	50
3.4	Optimal Locations of PMUs during Cascaded Failures with Single Line Outage	50
3.5	Optimal Locations of PMUs during Cascaded Failures with Single PMU Outage	52
3.6	Optimal PMU Placement during Multiple Operating Scenarios	52
3.7	Redundant Observability based Optimal PMU Placement Solution during Normal Operation	53
3.8	Comparison of the Proposed Observability and Redundant Observability Methods during Cascaded Islanding Operation	54
3.9	Proposed Observability and Redundant Observability Methods based Total Observability during Normal Operation	54
3.10	Proposed Observability and Redundant Observability Methods based Total Observability during Cascaded Islanding Operation	55
3.11	Proposed Observability and Redundant Observability Methods based Total Observability during Cascaded Non-Islanding Operation	55
5.1	Details of the Three Test Systems	81
5.2	All 42 Variables and their 'F' Indices of IEEE 14 Bus System	82
5.3	Details of Data Generation for Classifiers I and III	83
5.4	Details of Training and Testing Data for Classifiers I and II	83
5.5	Details of Training and Testing Data for Classifiers III and IV	83
5.6	Details of Testing Patterns for Classifiers I, II, III and IV	84
5.7	Results of Classifiers I, II, III and IV using WSVM Classifier	85
5.8	Results of Classifiers I, II, III and IV using AdaBoost Algorithm	85
5.9	Results of Classifiers I, II, III and IV using CBR algorithm	85
5.10	Computation Time (in seconds) of the Proposed CBR Classifiers	86
5.11	Computation Time (in seconds) of the Proposed CBR Classifiers for Indian 246-bus System Before and After Parallel Computation	87

LIST OF TABLES

5.12	Computation Time (in seconds) of Different Classifiers for Indian 246-bus System	87
5.13	Results of Classifier IV (VV Prediction) for IEEE 30 Bus System before and after SMOTE	88
5.14	Performance Analysis of Various Classifiers for IEEE 14-bus and 30-bus systems	90
5.15	Performance Analysis of SSA Results Obtained using Various Classifiers for Indian 246-bus System	90
6.1	Coherent Group Classification	98
6.2	Details about Various Parameters in the Test Systems	99
6.3	Details about time domain simulation for Test Systems	100
6.4	Security Assessment (Classifier I) of the Testing Patterns using the Proposed Approach	100
6.5	Coherent Generator Group Prediction (Classifier II) for IEEE 14-bus System .	102
6.6	Coherent Generator Group Prediction (Classifier II) for IEEE 30-bus System .	102
6.7	Coherent Generator Group Prediction (Classifier II) for Indian 246-bus System	103
6.8	Synchronism Status Prediction (Classifier III) for IEEE 14-bus System	104
6.9	Synchronism Status Prediction (Classifier III) for IEEE 30-bus System	104
6.10	Synchronism Status Prediction (Classifier III) for Indian 246-bus System (of 14 Random Generators)	105
6.11	TSA of Indian 246-bus System at Different Loading Levels using the Traditional Method	106
6.12	TSA of Indian 246-bus System at Different Loading Levels using the Proposed Approach	106

List of Abbreviations

ANN Artificial Neural Network.

BFS Best First Search.

CBR Case Based Reasoning.

CFM Conventional Flow Measurement.

COI Center Of Inertia.

DT Decision Tree.

FCT Fault Clearing Time.

kNN k-Nearest Neighbour.

LOV Line Overload Violation.

NRLF Newton Raphson Load Flow.

OPP Optimal PMU Placement.

PMU Phasor Measurement Unit.

RTI Rotor Trajectory Index.

SA Security Assessment.

SCADA Supervisory Control And Data Acquisition.

SI Security Index.

SMOTE Synthetic Minority Oversampling Technique.

SSA Static Security Assessment.

SSI Synchronism Status Index.

SVM Support Vector Machine.

TO Total Observability.

TRO Total Redundant Observability.

TSA Transient Security Assessment.

VV Voltage Violation.

WSVM Wavelet Support Vector Machine.

ZIB Zero Injection Bus.

Chapter 1

Introduction

1.1 Background

Modern power systems have become more complex due to the presence of diversified generation sources, loads and energy storage systems. The security assessment of power systems has always been a major concern but their changing operational paradigm makes it more challenging now. The penetration of renewable energy generations and flexible loads tend to change the operating conditions more rapidly in comparison to the traditional power systems. In addition, the continuous increase in load demand have forced the power system operators to operate the systems under greater stress, as the transmission lines often carry electric power near to their limits. In such situations, the loss of critical generating station or transmission line may pose a serious threat to the security of the power system. The conventional method of security assessment involves solving full AC load flow equations for each contingency scenario. This is highly time consuming and not suitable for real time applications. In order to avert catastrophic events, the control actions need to be initiated quickly necessitating fast security assessment.

The major aim of power system operation is to provide an uninterrupted electric supply to consumers under all conditions. This can be achieved by maintaining proper amount of spinning reserve and through proper utilization of the remaining units to manage the deficit. A power system is said to be secure if it is able to withstand severe contingencies due to the tripping of one or more system components. There may be several reasons viz. hurricanes and other natural calamities, etc., for the system components to fail. During the occurrence of such unplanned events, the remaining transmission lines can take the additional loading

and may continue to operate within limits for a shorter duration. However, when no immediate action is taken to reduce the loading, then it may be followed by a series of events which causes the tripping of some of the overloaded elements. If these cascaded events continue, this may result in splitting of the power system, which may ultimately lead to system black-out. Therefore, power systems are always operated in such a manner that their components should be able to withstand the overloading caused by a single event so as to mainly avert the cascaded failures.

Numerous wide-area blackouts triggered by cascaded failures have been witnessed in the past decades. The biggest blackout happened recently in India on the 30th and 31st of July in 2012. This huge blackout is caused due to the uncontrolled splitting of the interconnected regional grids into respective islands by the cascaded tripping of the weak interconnections. This resulted in the collapse of Northern grid with a load loss of 36 GW and eventually leading to the collapse of Northern, Eastern and North-Eastern regional grids with a total load loss of 48 GW [2]. This cascaded collapse is caused by the tripping of a 400 kV transmission line due to the false alarming of its distance relay. Similarly, the 2003 North-east blackout of the United States of America and in Ontario, Canada has a large impact economically. This is effected by the wrong calculations that led to the tripping of 345 kV transmission line. With much of the Midwest, Northeast and Ontario separated into electrical islands, severe power swings among them and its inability to reduce the power imbalance caused blackouts in each of those islands [3]. Finally, it is concluded that one of the principal causes of these blackout was the lack of proper monitoring and situational awareness of the power systems. Therefore, it is of utmost importance for the grid operator to have sufficient real-time monitoring tools to evaluate the reliable and secure operation of power systems.

System monitoring plays an important role in security analysis and control of power systems. Since the introduction of Supervisory Control And Data Acquisition (SCADA), these measurements have been predominately utilized by the operators for power system monitoring and control, however, they typically take 2-10 seconds for providing such measurements across the entire power system. Considering the dynamic nature of the power system and the slow data sampling rate of the SCADA, the security assessment studies conducted using these measurements may become unrealistic in real time. The advent of phasor measurements in early 1980s have created a new pathway in the electricity industry. These devices provide real time information about the system states from different locations of the power system at a

very high sampling time (25-60 samples per second) than the conventional SCADA systems. In fact, the phasor measurement technology [4–6] is considered to be the enabling technology for the development of real-time wide-area monitoring and control applications [7, 8]. Recent literature have presented various methods that use synchronized phasor measurements to carry out on-line security assessment studies. These studies reveal that the application of phasor measurements can significantly improve the possibilities for real time monitoring of power systems even during small disturbances. This improved monitoring can provide advanced and more precise information, which helps the operator to initiate emergency control actions in order to ensure reliable operation of power systems.

1.2 Power System Security Analysis

Security assessment of power system is mainly classified as Static Security Assessment (SSA) and Transient Security Assessment (TSA). Static security analysis is used to evaluate the ability of the power system to withstand credible contingencies without violating the normal operating limits of bus voltage and transmission line flows. Transient security analysis involves studying the system behaviour, especially the rotor angle of the system generators, after a large disturbance.

1.2.1 Operating States of a Power System

The operation of SCADA based Energy Management Systems (EMS) is based on the operating states of the power system. The most important states in which the power system usually operates can be classified into the following three states as shown in Figure 1.1 [1].

Normal

The power system is said to be operating in normal or secure state if its electrical constraints (voltage at the buses) and thermal constraints (current flow in the transmission lines) are within acceptable limits for a particular operating condition. A robust power system must continue to operate in a secure state even during contingencies. The system operator should foresee such credible contingencies and take appropriate control actions (as economical as possible) to maintain the integrity and security of the power system.

Abnormal

The power system enters this state when some of its component's constraints are being operated beyond their acceptable limits. The major challenge in this stage is to relieve the system

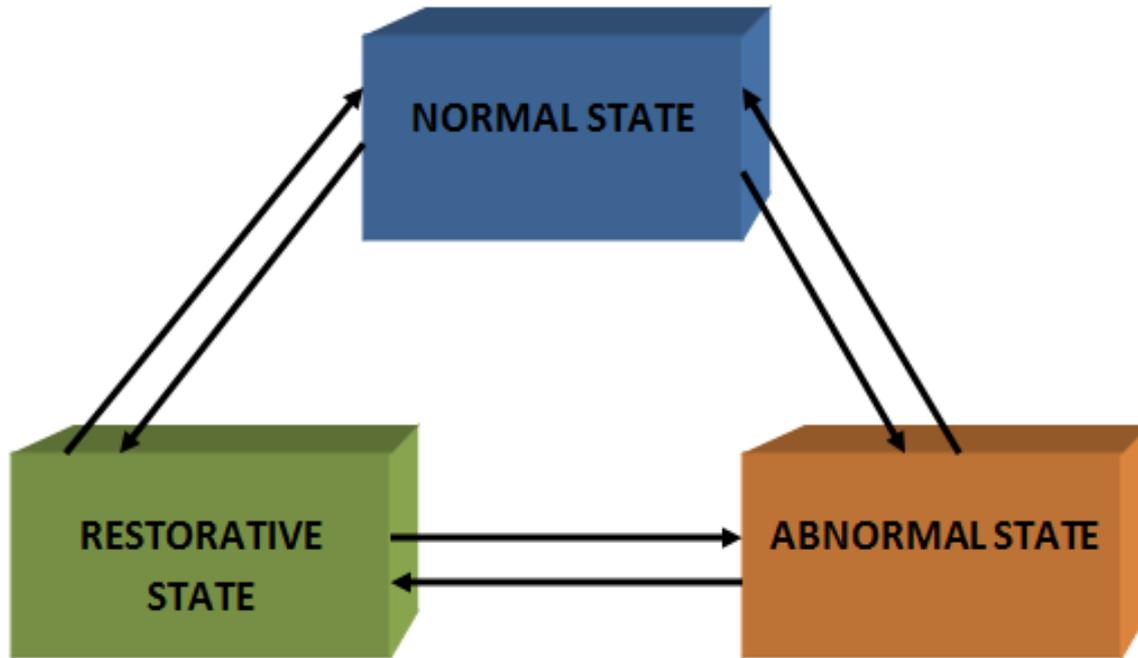


Figure 1.1: Various Operating States of a Power System [1]

stress and to maintain the proper load generation balance. Hence, there is a need of emergency control mechanism as the economic considerations are secondary at this stage. Based on the operating scenario of the power system, this abnormal state can be further classified into the following states as mentioned below,

1. *Alert* - In the event of any slight disturbance, system components may exhibit some violations in their operating limits. However, the system may return to normal operating state if the disturbance is of very short duration.
2. *Emergency* - As the power system reaches this state, immediate control actions such as load shedding are initiated to prevent the system from collapsing.
3. *Extreme* - The power system is said to be in extreme state, when all the emergency control actions fail to prevent the system from near collapsing. At this stage, the system splits into different groups and eventually leads to blackout stage due to the load generation imbalance. Hence, the operator initiates intentional islanding of the system to protect the integrity and stability of each island.

Restorative

This is a transitional state in which one or more operating constraints are met using emergency control actions. However, the load generation balance may have to be restored and the system may enter alert or normal state depending upon the control actions.

1.2.2 Major Components of Security Assessment

An operator in an EMS performs three major functions to assess the security of the system [9]. They are listed as follows.

1. System monitoring
2. Contingency analysis
3. Preventive and corrective actions.

System monitoring – A SCADA system is used to collect data from the various power system elements viz. bus bars and sensors which are located at remote terminal units and transmit these data to a central site for both monitoring and controlling purposes. Thus, based on the information received from the SCADA systems, the operation personnel can have a foresight on the system parameters.

Contingency analysis – A contingency in a power system is caused due to the failure of a system component (such as the loss of a generating unit, transformer or a critical transmission line) or due to the sudden change of system operating conditions (such as an increase or decrease in loading). The main aspect of the contingency analysis is to identify the critical contingency events affecting the system security. It is also used to evaluate the security of the power system and identify the occurrence of any violations due to each contingency and rank them based on their severity. Basically, the contingency analysis is performed in three stages viz.,

1. Contingency Definition
2. Contingency Selection
3. Contingency Evaluation

The main function in **contingency definition** is to conduct a detailed study to select the list of all possible contingencies whose probability of occurrence is high.

During **contingency selection** stage, only the most credible contingencies is identified from the large list of available contingencies obtained in the previous stage. The authors in [9, 10] have emphasized various screening methods to select contingencies from a presumed list of contingency set. The authors in [11–13] have studied the effect of multiple

component contingencies caused by substation and protection failures. In addition to N-1 contingencies, the other contingencies such as N-1-1, N-2, etc., also have a huge potential to initiate cascaded outages, which may eventually lead to overall system blackout. However, it is impractical to analyze all such probable contingencies in a simulation environment owing to huge computational complexity and limited resources. Hence, some approximation techniques based on load flow methods or artificial intelligent methods have been used to rank all the probable contingencies on the basis of severity.

In the **contingency evaluation** process, load flow is performed to check for any violations for each contingency available in the probable contingency list. Finally, only those contingencies, which causes violations on the system operating limits are listed as the credible ones.

Preventive and corrective actions – Based on the experience and the list of contingencies made available, the operator initiates immediate corrective control actions to prevent the system from collapsing in case of occurrence of similar contingencies.

1.3 Phasor Measurement Units

Phasor Measurement Units (PMUs) have revolutionized the field of power systems because of its ability to provide synchronized measurements across the system. It is a measurement device which is capable of measuring the synchronized values of voltage and current phasors in the power system. The calculation of phasors using Discrete Fourier Transform (DFT) usually requires an accuracy of greater than 1 milliseconds. The Global Positioning Satellite (GPS) can provide timing signals even more accurate in the order of 1 microseconds at any locations around the world. The synchronization among the PMUs installed in the system is obtained by the same time sampling of voltage and current phasors using a common reference from the GPS signal [14]. The accurate calculation of phasor values by the PMUs have made them one of the most important measuring device in the electric grids. A detailed analysis on the synchronization accuracy required for various phasor applications have been reported in [14]. Due to these advantages, PMUs have been recently used for many applications in power system such as multi-area state estimation, voltage stability prediction, frequency monitoring, system oscillation monitoring, power system restoration and security assessment [15]. Figure 1.2 illustrates a functional block diagram of a PMU, which consists of the following three main components [15].

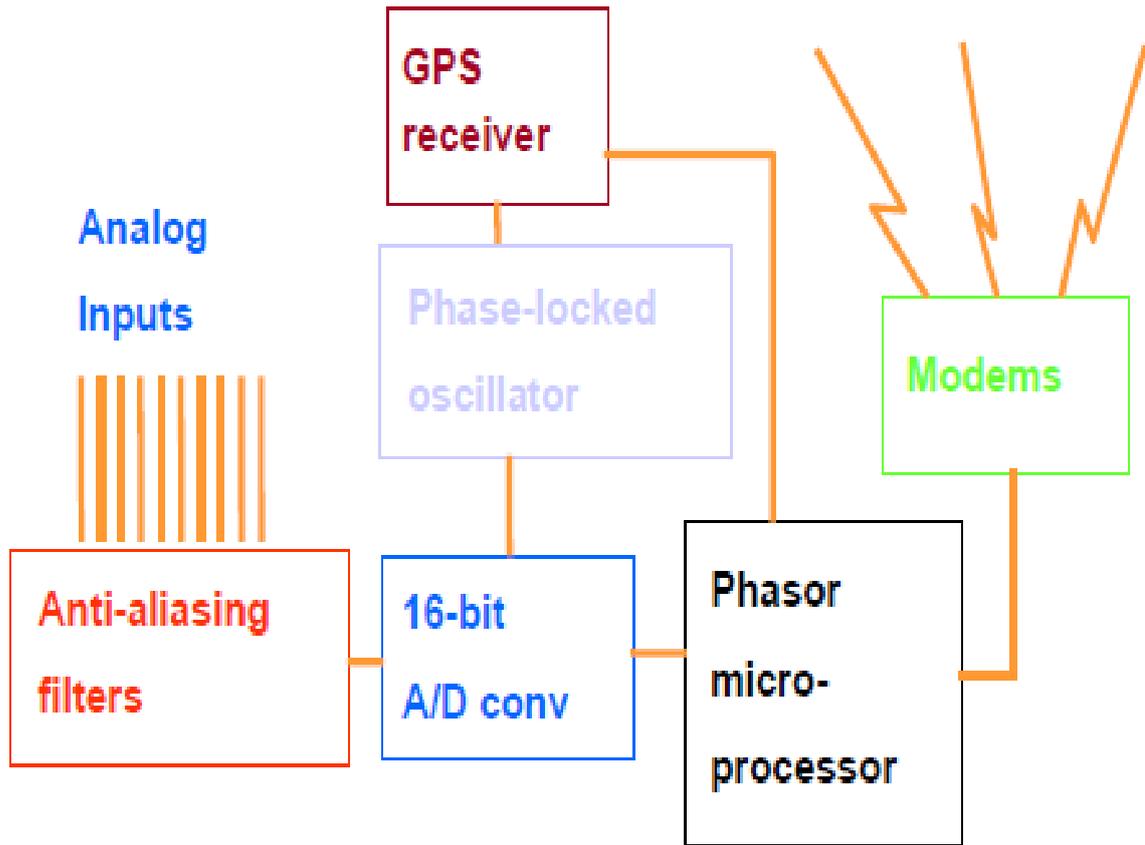


Figure 1.2: Functional Block Diagram of a Phasor Measurement Unit

1. Anti-aliasing Filter
2. Phase locked oscillator
3. Phasor microprocessor

The *anti-aliasing filter* removes the waveform with frequencies above Nyquist rate from the input waveform. The *phase locked oscillator* is used to convert the GPS 1 pulse per second into high speed timing pulses which is used for waveform sampling. Then, the *phasor microprocessor* calculates the phasors using DFT techniques. This calculated phasor is then time stamped and transmitted to the Phasor Data Concentrator (PDC) using high speed optic fibre communication links to match the fast streaming phasor measurements. Therefore, it is understood that any deployment of PMUs would require additional installation of communication infrastructure. A PMU installed at a bus can directly measure the voltage phasor of that bus and the current phasors of all the branches connected to that bus. Thus, the placement of PMUs at each bus would directly measure all the voltage phasors eliminating the need of state estimator. Furthermore, the dynamic performance of the power system can be analysed due to its high sampling rate.

1.4 Applications of Machine Learning Techniques for Power System Security Assessment

Machine learning techniques have been predominately employed for security assessment, since they can provide better performance in terms of accuracy and computation than the traditional methods of Security Assessment (SA). The important steps involved in this concept is the creation of a data base and a suitable classifier design. The data base consists of a large number of operating conditions, each of which is characterized by a vector of pre-disturbance steady state variables. These operating conditions should be able to represent all possible situations of the power system to have a better knowledge base. The entire knowledge base is the basis for training of the machine learning methods. Finally, the classifier after successful learning, can effectively predict the post-disturbance status of the system security. This section focuses the application of some of the important machine learning techniques used for security assessment of power systems.

1.4.1 Decision Trees

Decision Tree (DT) is a supervised learning algorithm which predicts the target value by learning simple decision rules. DT was first introduced in the year 1980 [16] and was later adopted for many applications in power systems [17–20]. This method is used to split the input data into numerous branches and model a tree-like graph of decisions and their possible outcomes. There are various types of decision trees viz. classification trees and regression trees. The DT is a classification tree if the target is a discrete class, while it is regression tree if the target is a continuous value [21]. During classification tree, the splitting rules are selected to ensure the cases in each of the divided subset are as pure as possible, whereas, in regression tree, the splitting rules are selected in such a way that the overall absolute deviation or square error is minimized. The basic requirement for the training of DTs is the database consisting of a number of cases. Each case in the database represents a vector of input attributes and a target, which is the security status of a power system at a specific operating condition. DTs have been widely employed in various applications because of their ability to extract or to identify the missing information from the input data [22]. Hence, these techniques have been widely regarded as a replacement for traditional statistical methods. Due to these advantages, DTs have been considered as a better technique for classification problems and

hence received significant attention in various power system applications including security assessment.

1.4.2 Artificial Neural Networks

Artificial Neural Networks (ANNs) work in a manner similar to the functioning of the biological nervous systems such as the brain that processes entire information in the human body. It consists of a large number of highly interconnected processing elements called neurons which are used to solve a specific task. It is used for fast pattern recognition and classification problems, through a learning process. The most commonly used neural network for security assessment is the multi-layered perceptron with back propagation algorithm, since it has been effective in solving many practical problems [23]. The ANN architecture consists of three layers viz. input layer, hidden layer and an output layer. The input layer consists of neurons needed for the desired input information. The number of hidden layers and the number of neurons in each layer is chosen based on the complexity of the classification problem. The number of neurons in the output layer depends upon the number of classes in a classification problem and upon the number of desired outputs in a regression problem. The training of the neural network requires a set of network inputs and the target outputs. During learning, the weights between the hidden nodes and the output nodes are iteratively adjusted to minimize the rate of error value calculated at the output nodes. This increases the training time of ANN methods and requires a large amount of training data [24].

1.4.3 Support Vector Machines

Support Vector Machine (SVM) is a supervised machine learning algorithm which analyze data for learning decision boundaries in pattern recognition problems. A decision boundary is the one that separates the set of objects belonging to different class groups. It performs classification by first mapping the input data to multi dimensional feature space by some non-linear mapping. Then an optimal hyperplane is constructed which separates the mapped input data into two classes with maximum margin. The concept of kernel mapping makes the SVM algorithm to perform nonlinear classifications even with complex boundaries. There are many kernel mapping functions viz., linear, polynomial, quadratic, multi-layer perceptron and radial basis function. However, the radial basis function (gaussian) kernel has been widely used as the mapping function due to its capability of handling nonlinear relation existing between input data and the class labels.

1.5 State-of-the-Art

Applications of PMUs in power system are expected to improve their monitoring significantly. As mentioned in section 1.3, the deployment of PMU at every bus eliminates the need of state estimator as it makes the entire power system observable. However, the high installation cost of PMUs prohibits their deployment at every bus and this motivates their strategic placement across the power grid. Once, the PMUs are placed optimally in the network, then the synchronized measurements received from them can be utilized in various power system applications such as security assessment, voltage stability, dynamic state estimation, etc. Further, the role of machine learning techniques in power system monitoring is also important. Thus, this section is divided into three sub-sections: Optimal Placement of PMUs, Phasor Measurement based SA Methods, Applications of Machine Learning Concepts for SA. Section 1.5.1 presents a detailed literature study on the various methods used for solving the PMU placement problem. Section 1.5.2 discusses about the popular security indices that have been developed using phasor measurements for directly computing the system security. Section 1.5.3 gives the information regarding the application of various machine learning techniques used for power system security assessment.

1.5.1 Optimal Placement of PMUs

Since the invent of PMUs in mid 1980s, many techniques have been developed for their optimal placement in the network. In 1993, the authors in [25] have first proposed the use of graph theoretic based approaches such as Depth First Search (DFS) and Spanning Tree (ST) to solve the Optimal PMU Placement (OPP) problem. In this algorithm, the complete system observability has been achieved since the PMUs are placed at the nodes in the order of highest connectivity. However, this method results in unwanted redundancy due to the positioning of more number of PMUs. Hence, the mathematical formulation based Integer Programming (IP) methods have been widely employed for determining the optimal locations of PMUs. An Integer Linear Programming (ILP) based multi-criteria decision making approach has been proposed in [26] to identify the suitable locations of PMUs in the power system network. The authors in [27] have presented a non-linear programming based approach for the optimal placement of PMUs, while an ILP based PMU placement formulation has been proposed in [28]. An optimal multistage PMU placement model alongwith measurement redundancy has been proposed in [29]. A new formulation based on IP method has been proposed in [30]

to identify all the possible PMU placement solutions. Then the sequential algorithm is used to identify the placement set which is having the least state estimation error covariance. However, this method is time consuming for larger power system networks. It is understood that a PMU with the limited channel capacity can observe only limited number of nodes among all the adjacent nodes. This perspective has been first considered by the authors in [31]. A new and efficient formulation based on ILP has been proposed in [32] to solve the PMU placement problem considering channel limits along-with additional single line and PMU outages. This method considers that the PMUs with unlimited channel capacities have been used to measure sufficient number of voltage phasors and currents. The same authors in [33] have proposed an another formulation to solve the optimal PMU placement problem such that the PMUs with varying number of channels can be considered. Although these methods provide optimal solution, their final solution is obtained based upon the initial guess chosen. Moreover, in case of larger power networks, these mathematical based methods can take longer simulation time due to increase in the number of variables and constraints.

To overcome this drawback, evolutionary algorithms have been utilized in the recent years to determine the optimal PMU locations. These methods can provide a near global optimal solution and are found to be effective in handling multi-objective problems. The authors in [34] have proposed the use of a Genetic Algorithm (GA) based approach for solving optimal PMU placement problem, while a Non Dominated Sorting Genetic Algorithm (NSGA) based multi-objective PMU placement algorithm has been presented in [35] to identify the optimal locations of PMUs. The number of input parameters required for GA based methods and their selection needs thorough investigation. Improper selection of these input settings may lead to the poor convergence and may result in longer simulation time. The authors in [36, 37] have used Simulated Annealing (SA) to determine the optimal PMU locations, which is also a computationally extensive method. In [38, 39], Tabu Search method has been used to find the optimal locations of PMUs. This method determines the placement locations using an augmented incidence matrix and the computation of this matrix for larger systems is very complex and time consuming. The authors in [40] have utilized the Binary Particle Swarm Optimization (BPSO) to optimally place the PMUs to ensure complete system observability, whereas, the authors have achieved a multi objective placement solution in [41] by minimizing the number of PMUs and maximizing the measurement redundancy using BPSO. In order to improve the overall convergence rate and its speed, an Improved Particle

Swarm Optimization (IPSO) method has been proposed in [42] for the optimal placement of PMUs. This work also considers the numerical observability, while placing the PMUs. A modified Artificial Bee Colony (ABC) based multi-objective PMU placement algorithm has been proposed in [43] to enhance the performance of system observability and voltage stability. In [44], the authors have used Fruit Fly Optimization (FFO) for the PMU placement problem. Due to the capability of solving complex optimization problems, these methods have been widely employed for solving the OPP problem. However, the major drawback of these evolutionary algorithms is the higher simulation time for larger power system networks.

The literature study reveals that the PMU placement methodologies for maintaining system observability predominately considers only the topological observability of the system. In comparison, numerical observability based PMU placement methods have also been studied in [45–47]. A power system is said to be numerically observable if the rank of the measurement Jacobian matrix is full. However, numerical observability of the system may not be feasible under system contingencies due to the change in system topology. The authors in [48] considers this perspective and investigated the numerical observability of the system, while considering contingency events. The authors in [47] has highlighted the needs of complementing the topological observability based PMU placement techniques with the numerical observability analysis. For this purpose, a two-stage PMU placement technique has been proposed for ensuring the topological observability along-with numerical observability analysis of the given power system. The stage-1 uses an ILP based approach to place the PMUs for maintaining complete observability of the power systems topologically. In stage-2, the numerical observability analysis has been carried out by determining the measurement Jacobian matrix H , which consists of voltage and current measurements obtained from the PMUs. The authors in [49] have considered the new concept of PMU placement technique, which they defined it as observability reliability. It considers the failures of PMUs and transmission branches while placing the PMUs for observability.

The use of phasor information has been successful in identifying and removing the bad data from the system measurements during the state estimation process. A new formulation based on Weighted Least Square (WLS) state estimation has been proposed in [50] to combine the conventional measurements with the phasor measurements. This method is also used to determine the optimal number of PMUs in order to have an enhanced state estimation. A similar WLS based method for state estimation has been proposed in [51], which

includes both traditional as well as the phasor information obtained from PMUs. The proposed work is also used to predict the bad data in the conventional and phasor measurements. The power system parameters changes continuously due to the dynamic nature of loads connected to it. This necessitates the need of dynamic state estimator to identify the system states in real-time. In [52], the authors have optimally placed the PMUs to track the generator rotor angles and speeds in order to assist the dynamic state estimation process. Similar work has been reported in [53], where the dynamic state estimation process has been carried out using the phasor measurements. The authors in [54] have presented a bi-objective PMU placement solution that identifies the potential placement locations to have a better dynamic state estimation process as well as to ensure the numerical observability of the power system.

Recent research have suggested a placement method that considered the minimization of both the PMU locations and the Phasor Data Concentrators (PDCs) [55, 56]. Most of the studies reported in the literature reveal that the PMU placement methods usually aims at maintaining complete observability of the system with a minimum placement set of PMUs. In contrast, there have been few instances where the PMU placement methods based on the degree of observability have also been considered. The authors in [57] have used a probabilistic PMU placement method to minimize the unobservability, while an empirical observability gramian method has been proposed in [58] to quantify the degree of observability.

Practically, it may not be economically viable for the system operators to depend solely on the PMUs to ensure complete system observability due to its high installation cost and sophisticated communication infrastructures [59]. Traditionally, the Remote Terminal Units (RTUs), which use the network time protocol for time synchronization provide the real and reactive power flows of the transmission lines to the SCADA systems. Considering the voltage phasor at one end of a branch is known by a PMU, then, the voltage phasor at the other end of a branch can be computed using the Kirchoff's laws as its real and reactive power flows have already been measured by the corresponding remote terminal units [48]. Therefore, the consideration of flow measurements leveraged together with PMU placement effectively reduces the total number of PMUs required for maintaining complete system observability, thereby reducing the total installation cost. The authors in [60] have proposed a mixed integer linear programming based placement of PMUs and conventional flow measurements to make the system completely observable during N-2 contingencies. Further, this placement strategy has also been extended into multi-stage placement method to present an

effective solution for handling limited financial budgets. The authors in [61] have considered the presence of conventional flow measurements while optimally placing the PMUs. This method also focuses on the consideration of single as well as multiple flow measurements connected to a bus. Although this approach enables a smooth transition from the current SCADA-based system monitoring to the future PMU-dominated WAMS, there has been issues while integrating flow measurements with the phasor measurements in real-time due to the difference in their sampling time. This issue involved in the combination of both the phasor measurements and SCADA measurements has been well investigated in [62].

1.5.2 Phasor Measurements based SA Methods

Several approaches of phasor measurements based security assessment of power systems have been reported in the recent years. A review of some examples is detailed in the rest of this section. An ensemble learning technique has been used in [63] to calculate the severity indices using the phasor information obtained from the PMU data. These indices, which usually represent the stability of the system, can be helpful in identifying the weak buses of the given power system. Therefore, these indices can act as better indicator in predicting extreme events affecting the system security. The authors in [64] have proposed a framework for real-time monitoring of voltage security of power systems using synchronized measurements. The QV sensitivities are calculated at each sub-station using the PMU measurements. These indices from the local centers are then collected at the main control center to compute the voltage security index. An online voltage security monitoring scheme using synchronized measurements has been proposed in [65]. Initially, the decision trees are trained using the pre-contingency system parameters obtained using PMUs. Following a new contingency, the decision trees are periodically updated using the fault information and the current magnitudes obtained from the phasor measurements. These measurements are then compared with the threshold values of the decision trees to access the voltage security in real time. The authors in [66] have proposed a phasor measurement based contingency assessment scheme for voltage dip and voltage instability problem. A practical and efficient method to calculate online dynamic stability index using phasor measurements is proposed in [67]. In [68], PMU data has been used to compute Singular Value Decomposition (SVD) for assessment of voltage stability. An algorithm based on QV sensitivity indices has been proposed in [69] for voltage security monitoring, wherein the QV sensitivities are computed from the phasor

measurements. The authors in [70] have presented a novel algorithm for the online computation of voltage collapse sensitivity indices. These indices are computed using the information obtained from PMUs, which are considered to be placed at each bus. Similarly, another algorithm based on phasor measurements has been proposed in [71] for voltage stability monitoring. The algorithm presented here computes the stability index during normal operation as well as during contingency cases, which allows the dynamic monitoring of voltage stability of the given power system. Another important aspect analyzed in this work includes voltage stability monitoring during small disturbances viz. gradual increase in loading conditions and voltage stability monitoring during large disturbances such as branch loss or short circuit faults. A new voltage stability index obtained using the real time measurements from PMUs installed at the two ends of the branches is presented in [72]. These measurements include terminal end voltages and the power flows of the branches, provided that the PMUs are placed at the terminals of the transmission lines. A similar work reported in [73] calculates the stability index based on the voltage and current phasor measurements, which are obtained using the PMUs installed at high voltage level buses. Finally, this index is used to identify the high voltage buses that are vulnerable in case of occurrence of contingencies. In [74], the authors propose a novel method for voltage security assessment of a wind power plant using PMU measurements. These measurements are initially used to compute the Thevenin matrix, using which the fault location and its impact on each bus can be calculated.

1.5.3 Applications of Machine Learning Concepts for SA

The advent of the pattern recognition approaches in early 1970s have been considered as a prominent tool for security assessment. Since then, many techniques such as DTs [75–81], ANNs [82–93], SVM [94, 95], Self-Organizing Maps (SOM) [96, 97], etc., have been used for security assessment. These methods overcome the drawbacks of the traditional methods, thereby making the security assessment computationally more efficient and reliable. The authors in [75–81] have applied DTs to evaluate power system security assessment. DTs can accurately interpret the relationship existing between events, however, they may result in poor classification in case of occurrence of other contingencies. In the recent years, several approaches using ANN have been used for security assessment. Moreover, the improved generalization capability of these methods make them feasible for security assessment of modern power systems [82]. The importance of these methods to power system security assessment

has been elaborated in detail in [98–101]. The authors in [83] have proposed a security module using Multi-Layered Feed Forward Neural Network (MLFFNN) and Radial Basis Neural Network (RBNN) for predicting the security status by computing the performance indices and to rank the contingencies based on severity. The authors in [88–90] have proposed the use of cascade feed forward neural networks for the fast and efficient screening and ranking of line flow contingencies. Similar works have been reported in [91, 92] using counter propagation network for real power contingency ranking. In [93], the authors have investigated the voltage contingency ranking using parallel self-organizing hierarchical neural network. However, it is important to have an efficient contingency screening module, which is capable of ranking the severity based on both line flow and voltage violations. Considering this perspective, the authors in [84, 86] have proposed an online security module incorporated with MLFFNN and RBNN for power system security assessment. These ANN based security assessment methods are extremely faster in computing the security status of the power system than the conventional techniques. However, it requires the weights between the hidden and the output nodes to be updated several times based on the rate of error value calculated at the output nodes. This increases the computational complexity of training the neural networks for larger power systems [94]. As the power system security evaluation is a complex non-linear separability problem, the authors in [94, 95] have applied SVM for power system security assessment. However, its performance mainly depends on the proper selection of kernel parameters and the choice of margin parameter (C), which is a more challenging task when the underlying distribution of the data is not known.

1.6 Motivation and Objectives

There have been various approaches proposed to solve the optimal PMU placement problem. The methods which have been predominately used are graph theory based methods, mathematical approaches and evolutionary algorithms. Although graph theory based methods such as DFS and ST algorithms were the first used to solve this PMU placement problem, these methods ensure observability with more number of PMUs. These additional PMUs increase the redundancy at some of the system buses which is not required. IP based mathematical approaches involve minimization of cost of PMUs subject to certain constraints for maintaining complete observability of the system. Although these mathematical methods have been computationally faster and simpler, their final optimal solution is mainly depen-

dent on the initial guess chosen. Since the optimal PMU placement problem is NP-hard and does not have a unique solution, evolutionary algorithms have been employed to solve this problem [102]. Some of these methods which have been widely used are FFO, GA, NSGA, BPSO and IPSO based techniques. These methods provide near optimal solutions but their simulation time increases with the increase in system size. Though many methods have been reported in the literature for solving the optimal PMU placement problem, these methods are found to be either computationally inefficient or they do not provide optimal solution. Moreover, they have focussed only on finding the optimal PMU locations considering operation of power system as a single and integrated network. Hence, the solution obtained by these methods do not provide complete observability during the islanding disturbances, where the power system may break into several islands in an uncontrollable manner. Therefore, it is important to have a placement solution which guarantees sufficient number of PMUs in each island to ensure their observability.

The classical approach to security analysis in power system involves the computation of security indices through load flow solutions for the assessment of its post-contingency situations. Some of the widely used indices for the assessment of security are sensitivity matrix, security indicators, distribution factors, etc. The literature studies highlight that these analytical approaches cannot be effectively used for online assessment of power system security because of their computation complexity and the time associated with it. The wide deployment of PMUs and their applications in the SCADA centres have brought the complex decision making process in a much simpler and faster way. The increase in the number of market participants, penetration of renewable power generation and smart loads increases the complexity in decision making [103, 104]. Several attempts have been made to improve the performance of the security assessment methods by using machine learning techniques, thereby making it feasible for online implementation. The most effective algorithms used to security assessment are ANN, SVM and DTs. Although these techniques have been successfully applied over the years for security assessment of power systems, their performance is mainly dependent on the proper selection of training patterns, representing all operating conditions of the power system. Hence, these methods often have a low prediction accuracy and a high misclassification rate. Therefore, it is concluded that there is a need of more accurate and faster security assessment technique, which is vital for real-time monitoring and control of the emerging power systems to avert any catastrophic events.

In view of the advantages of the phasor measurements based security assessment and considering the limitations of existing machine learning techniques used for security assessment, the main objectives of this thesis are discussed below.

1. To develop a new intelligent search technique based OPP scheme for maintaining complete observability during system intact as well as during cascaded failures. It is also aimed at incorporating measurement redundancy for enhancing the state estimation process using phasor measurements.
2. To develop a suitable framework consisting of classifier models that can effectively predict system static security as well as the violations (bus voltage deviation and line flow overloads) that causes insecurity of power systems.
3. To develop a suitable framework for predicting transient security status of power system, synchronism status of the generating units, and identification of coherent group of generators.
4. To explore different machine learning techniques with higher generalization ability to improve power system monitoring.

1.7 Thesis Outline

The work carried out in this thesis has been organized in seven chapters. The current chapter provides basic definitions and concepts related to security assessment of power systems. This chapter also highlights the importance of phasor measurements based security assessment and presents the relevant state-of-the-art survey on various PMU placement methods. Finally, it sets the motivation behind the research work carried out in this thesis.

Chapter 2 presents a two stage method for solving the PMU placement problem, where stage I utilizes the best first search algorithm to identify the locations of PMUs and the redundant locations are identified and removed using pruning in stage II. Also, the proposed approach of PMU placement for system intact and contingency cases are compared with the results of other existing placement methods to elucidate its performance improvement. The proposed approach is made flexible by incorporating the presence of conventional flow measurements in the system. Another important outcome of this work is its capability to handle both single and multiple flow measurements connected to a bus, while optimally placing the PMUs.

Chapter 3 emphasises the need to analyze other power system contingencies such as cascaded failures and the importance of having a robust measurement system so that the system remains completely observable even during such catastrophic events. The OPP scheme proposed in Chapter 2 is extended to determine the optimal locations of PMUs for maintaining complete system observability during both cascaded islanding and non-islanding situations. In order to identify whether a particular cascaded failure leads to islanding condition, an algorithm based on system topology information has also been developed. To have an accurate and reliable state estimation, measurement redundancy is also incorporated along-with system observability in this chapter. Additional contingencies such as single line loss and single PMU loss have also been considered to take place after the cascaded events.

Chapter 4 illustrates the applications of various machine learning techniques used for security assessment of power systems. Some of the new machine learning techniques used in this work for security assessment include - Wavelet Support Vector Machine, Case Based Reasoning and AdaBoost Algorithm. The description of these techniques has been presented in this chapter in detail.

Chapter 5 proposes a new framework for Static Security Assessment (SSA) of power systems using the synchronized measurements obtained from PMUs, which are optimally placed in the given power system for complete observability. The proposed framework is capable of predicting the type of violations which may be either line overload/voltage violation or both in the insecure operating conditions in addition to security status. Further, a new security index consisting of line overload and bus voltage violation has also been proposed to classify the training patterns into secure or insecure class. The effectiveness of the proposed approach has been demonstrated on IEEE 14-bus, IEEE 30-bus and Indian 246-bus systems. Finally, test results of the proposed approach has been compared with the traditional methods of SA, which predominately use SVM, ANN or kNN classifiers as decision models. Their analyses reveal that the proposed machine learning techniques perform better than the traditional classifiers in terms of classification accuracy.

Chapter 6 presents an implementation of the proposed classification framework for the Transient Security Assessment (TSA) of power systems using the synchronized measurements. These synchronously sampled values of the generator rotor angles which are collected by the PMUs at regular intervals, following a disturbance, are used to construct a new synchronism stability index. The proposed framework can predict transient security status of

the power system and the synchronism status of the generating units as well as the coherent group of generators. From Chapter 5, it is observed that both Wavelet SVM and AdaBoost classifiers have similar prediction results and exhibit better generalization capability than the existing classifiers including case based reasoning. Therefore, it is beneficial to use either of these two classifiers for the proposed framework of transient security monitoring. In this chapter, the proposed approach has been implemented using AdaBoost algorithm for all test systems such as IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus systems.

Chapter 7 concludes the important findings of the work presented in the thesis and ideas from which research directives can be drawn for the future work.

Chapter 2

Optimal Placement of PMUs using Intelligent search Method

2.1 Introduction

The installation of PMU at a bus can measure the voltage phasor of that bus and the current phasors of some or all the branches connected to it, depending on the number of channels available in each PMU device. Thus, the deployment of PMUs at each bus would make the entire power system observable, thereby eliminating the need of state estimation. However, due to the high cost associated with the PMU device and its communication facilities, it is neither economical nor feasible to install PMUs at all the system buses. Therefore, it is imperative to determine the optimal placement of PMUs.

In the past two decades, various approaches have been proposed to solve the optimal PMU placement problem. Some of the techniques widely used are graph theory based approaches, mathematical and evolutionary programming techniques. Graph theory based approaches such as Depth First Search (DFS) and Spanning Tree (ST) were the first used to solve this PMU placement problem [25]. The DFS method is based on placing the PMUs in the order of the largest connectivity hence, it ensures complete observability but with more number of PMU locations. These additional PMUs causes the observable islands to overlap each other resulting in unwanted redundancy at a few system buses. The Integer Programming (IP) based methods [28] [29] [33] [61] [32] have also been used to solve the PMU placement problem with multiple constraints such as line loss, PMU loss, channel limits and flow measurements. Although these methods are found to be effective in finding the opti-

mal solution in a lesser simulation time, their final solution is mainly dependent upon the initial guess chosen. The evolutionary algorithms, which can provide a near global optimal solution, are effective in handling multi-objective problems. Hence, these methods have been predominately utilized in the recent years to solve the PMU placement problem. Some of these techniques, which have been widely employed include - Non-dominated Sorting Genetic Algorithm (NSGA) [35], Simulated Annealing (SA) [36], Tabu Search (TS) [38], Binary Particle Swarm Optimization (BPSO) [41], Fruit Fly Optimization (FFO) [44]. The major drawback of these evolutionary algorithms is the higher simulation time for larger power system network.

These studies reported that most of the methods employed for solving the PMU placement problem are either computationally intensive especially for large scale practical power systems or do not guarantee global optimal solution. Thus, there is a need to develop a suitable PMU placement method which can provide global optimal solution in a lesser simulation time.

In this chapter, a new intelligent search based method has been proposed to determine the optimal locations of PMUs while achieving complete system observability. The proposed method works in two stages. In stage I, the possible locations of PMUs are determined using a Best First Search (BFS) method, which is an intelligent search method. It has an ability to identify the most promising nodes and change its search path from the current node to the most promising node [105]. Out of the possible locations determined by BFS, redundant PMUs are identified and removed by applying pruning in stage II. A simple topological transformation method has also been proposed to model the zero injection buses. Further, the proposed method also considers the presence of single and multiple conventional flow measurements connected to a bus while determining the optimal locations of PMUs. The proposed method has been tested on IEEE 14-bus, IEEE 30-bus and a practical 246-bus Indian system under system intact case as well as during contingencies.

2.2 Observability Rules

In a power system, a bus is said to be observable if its node voltage can be directly measured or calculated by using the known node voltage and branch currents at other buses. If all buses in the system are made observable, then the power system can be defined as the system with full observability. The placement of a PMU on a bus in a power system can provide (1)

voltage phasor at that bus, and (2) current phasors of all branches connected to that bus. With the known voltage phasor at one bus (bus 'i') and the branch current phasor (I_{ij}), the voltage phasor at the adjacent bus (bus 'j') can be directly computed using the Ohm's law.

$$V_j = V_i - Z_{ij}I_{ij} \quad (2.1)$$

where Z_{ij} is the impedance of the line $i - j$. Similarly, the voltage of any other bus connected to bus 'i' can be computed. Thus, a PMU placed at a bus can observe that bus as well as all buses adjacent to it [25], [106]. This implies that the power system can be made completely observable with the number of PMUs significantly lesser than the number of system buses. It is further noted that the placement of PMU at the radial bus is usually avoided as the PMU placement at this bus can observe only that bus and its adjacent bus. In such situations, the buses incident to the radial buses are selected as predefined locations and assigning PMUs to these buses help the algorithm to converge soon. However, if the bus incident to the radial bus is a Zero Injection Bus (ZIB), then PMU placement at the ZIB is not considered as the voltage and current phasors at the radial bus can be obtained by applying Kirchoff's law at the ZIB. In case, if two or more radial buses are connected to the same ZIB, then a PMU must be placed there.

2.3 Proposed Approach

The PMU placement solution is said to be an optimal one, when the power system nodes are made observable with a placement set containing minimum number of PMUs. Most of the graph theoretic methods such as DFS, ensures this by placing PMUs at the nodes having largest connectivity but results in redundant PMUs, which is not desirable [25]. Being a blind search procedure, the DFS algorithm searches every node in the system which leads to non-optimal path to reach the goal state. This behavioural characteristic of the DFS algorithm is replaced by an intelligent-search technique called Best First Search (BFS) method. While moving towards the goal state, this method utilizes information about each node by computing an evaluation function at each of them. It helps the BFS algorithm to search and explore only the most promising nodes, thereby making the search process, more simpler and faster one [107]. The most promising nodes are identified as those having least/highest score of an evaluation function. While searching towards the least optimal cost path, the BFS algorithm has the capability to change its search path from the current search path to the most

promising path [105]. This characteristic makes the BFS method superior over other graph theoretical methods for optimal PMU placement problem.

In this chapter, the optimal locations of PMUs have been determined in two stages as shown in Figure 2.1. Stage I employs the BFS approach to find the sub-optimal nodes for PMU placement and stage II employs pruning to remove the redundant PMUs.

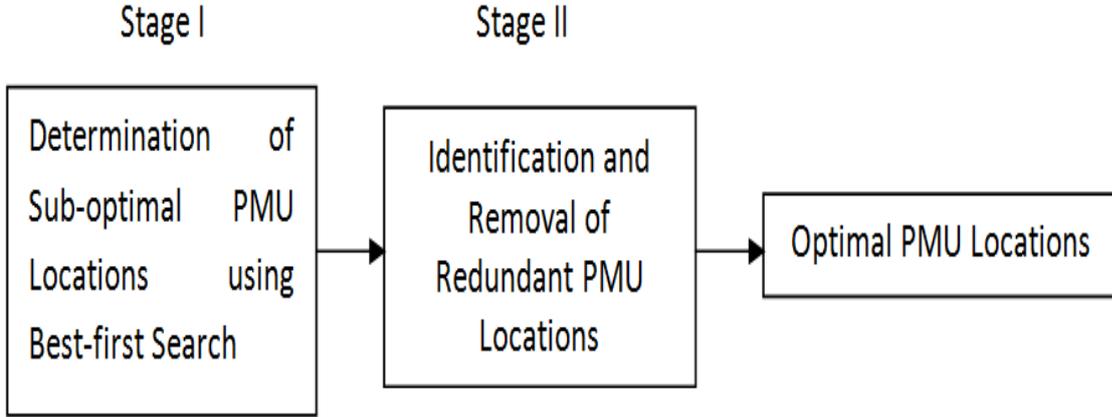


Figure 2.1: Proposed Method for PMU Placement

The brief description of these stages is given below.

Stage I: In this stage, BFS method has been utilized to determine the sub-optimal locations of PMUs while maintaining system observability. In order to identify the most promising nodes, the evaluation function (f_i) at a node ' i ' is formulated as the ratio of coverage value (Y_i) of a node to the cost of PMU placement (X) and can be written as,

$$f_i = Y_i/X \quad (2.2)$$

The coverage value (Y_i) of a node is defined as,

$$Y_i^b = \sum_{j=1}^{nb} C_{ij} * \lambda, \quad \forall i \in nb \quad (2.3)$$

and,

$$C_{ij} = \begin{cases} 1, & \text{if node 'i' and 'j' are connected} \\ 1, & \text{if } i = j \\ 0, & \text{if node 'i' and 'j' are not connected} \end{cases}$$

Here, C_{ij} is the binary connectivity matrix and coefficient (λ) is a biasing factor that makes the BFS algorithm to search towards the unobserved node. Initially, this bias value is taken as one and for successive searches, it is incremented by the largest coverage value obtained at the previous search. The cost of PMU installation (X) is defined as a product

of the number of nodes/buses (nb) in the system and the PMU count (p). This count is assumed to be one for the initial search and is incremented by the number of PMU installations obtained till the previous level of search. As the power system nodes are explored on the basis of their evaluation function described in (2.2), the nodes with the highest value of the evaluation function are given priority in PMU placement. Once a PMU is placed on a node, the evaluation function at that node is nullified so as to avoid it from further consideration. After the PMU placement, the given power system network is checked for observability by computing its corresponding observability vector, OV^b .

The elements of an observability vector, OV^b at the b^{th} iteration can be obtained using,

$$OV_i^b = \begin{cases} 2, & \text{if node } i \text{ is observed by a PMU at node } k \\ 1, & \text{if a PMU is placed at node } i \text{ (or } i=k) \\ 0, & \text{if node } i \text{ is unobserved by a PMU at node } k \end{cases}, \quad \forall i \in nb \quad (2.4)$$

Finally, the total observability vector at the b^{th} iteration, TO^b is computed by adding the observability vector at the b^{th} iteration, OV^b with the total observability vector, TO^m obtained at the m^{th} iteration as follows,

$$TO_i^b = TO_i^m + OV_i^b, \quad \forall i \in nb \quad (2.5)$$

$$\text{where, } m = \begin{cases} b-1, & \text{if } f_l^b \gg f_r^{b-1} \\ 1, & \text{otherwise} \end{cases}$$

It is assumed that the elements of TO^m are zero for initial search. If there are any unobserved nodes in the system, the BFS algorithm identifies the unobserved node ' l ' having the largest coverage value. Then, the evaluation function at this node ' l ' is updated by reconstructing the binary Connectivity Matrix (CM). This evaluation function is compared with the evaluation function retained at the previous search and the node with the highest value of the evaluation function is chosen as the next PMU location. This process is continued till all the nodes in the system are observed. The flowchart to determine the sub-optimal PMU locations using BFS method is shown in Figure 2.2

Stage II: The sub-optimal locations of PMUs obtained in stage I are used as input to this stage. The redundant PMU locations are identified and eliminated by applying a pruning technique which is enumerated below.

The system observability is checked by removing a PMU from the placement set. If the

2.3. PROPOSED APPROACH

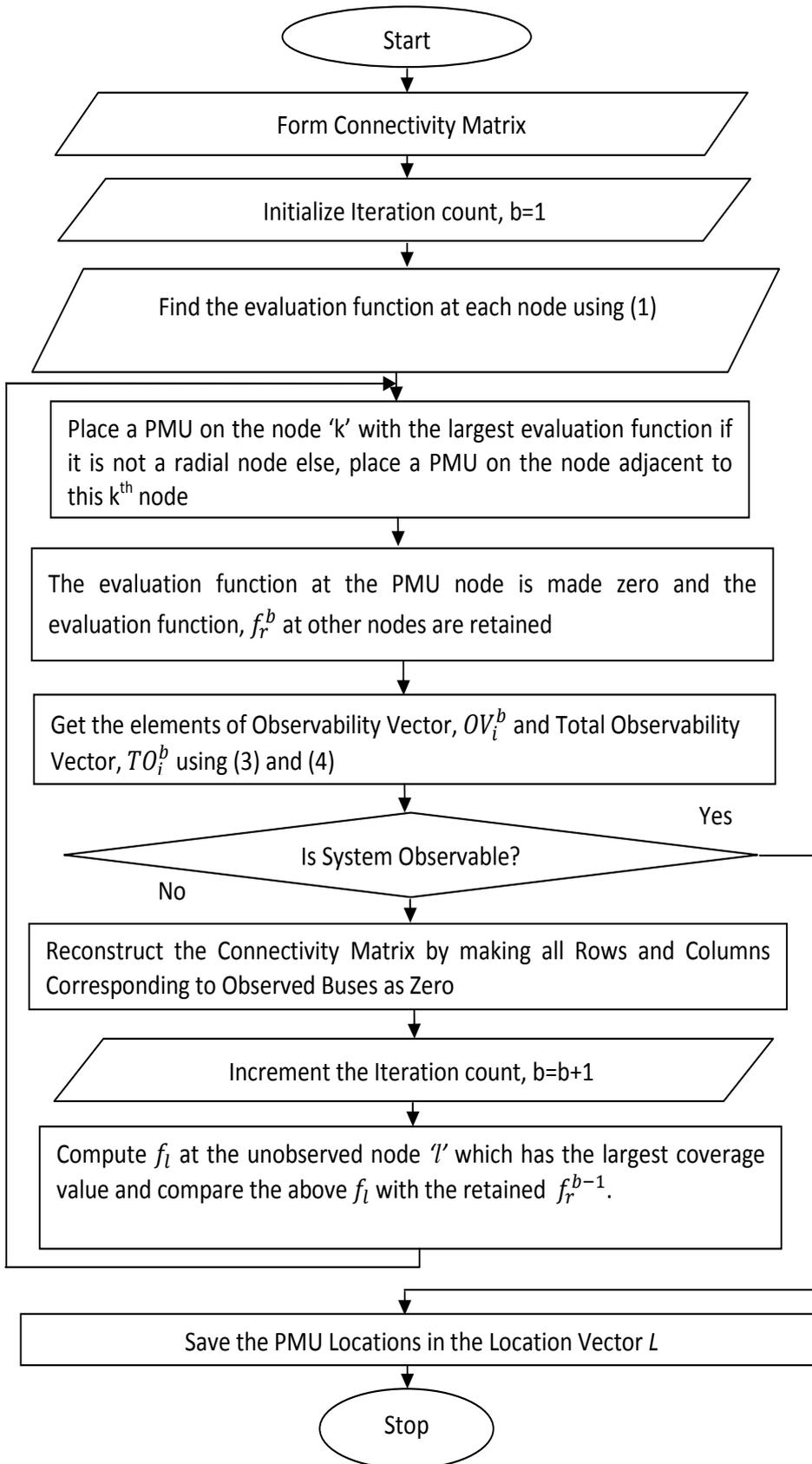


Figure 2.2: Flowchart of Stage I of Optimal PMU Placement

system is not completely observable, then that PMU is preserved as it is crucial for observability else, that PMU is considered as redundant and it is removed. This is repeated for each PMU location obtained in stage I. Finally, it is ensured that only PMUs at the crucial nodes are retained. Thus, the complete system observability is achieved by removing the redundant PMUs, which makes the proposed method more effective than the existing methods. Henceforth, the placement set obtained after stage II is the optimal set required to make the system completely observable with the minimum number of PMUs. The stepwise procedure for the identification and removal of redundant PMU locations in the placement set obtained from stage I is described below.

1. The number of PMUs (N) and locations obtained from BFS algorithm are stored in a location vector L .
2. Set the iteration count for pruning, $bp = 1$.
3. Remove one PMU at a time from the location vector L such that the number of elements in the modified location vector L' is reduced to $(N - 1)$.
4. For each iteration, compute the product element P^{bp} using,

$$P^{bp} = \prod_{j=1}^{nb} R_j$$

where,

$$R_j = \sum_{p \in L'} C_{pj}, \quad \forall j \in nb$$

5. Check whether the product value for all the elements in the location vector L is obtained (or $bp = N$), if yes go to the next step else, increment the iteration count, $bp = bp + 1$ and repeat from step 1.
6. The nodes with the non zero element in the product vector P_N are stamped as additional PMU locations. Here, P_N consists of product element P^{bp} obtained after removal of each PMU (ie., $P_N = P^1, P^2, \dots, P^N$). Thus, the complete system observability is ensured with a minimum placement set by removing redundant PMUs from these locations.
7. Save the optimal PMU locations.

2.3.1 Modelling of Zero Injection Buses (ZIBs)

Zero Injection Buses (ZIBs) are considered as pseudo buses as there is no generation or load connected to them. Hence, the sum of the current phasors on all the incident branches to the ZIB is zero [108]. In order to further reduce the number of PMUs needed to make the system observable, the proposed placement scheme can be modified to incorporate the Zero Injection (ZI) effect. To understand this issue, consider a four bus example shown in Figure 2.3.

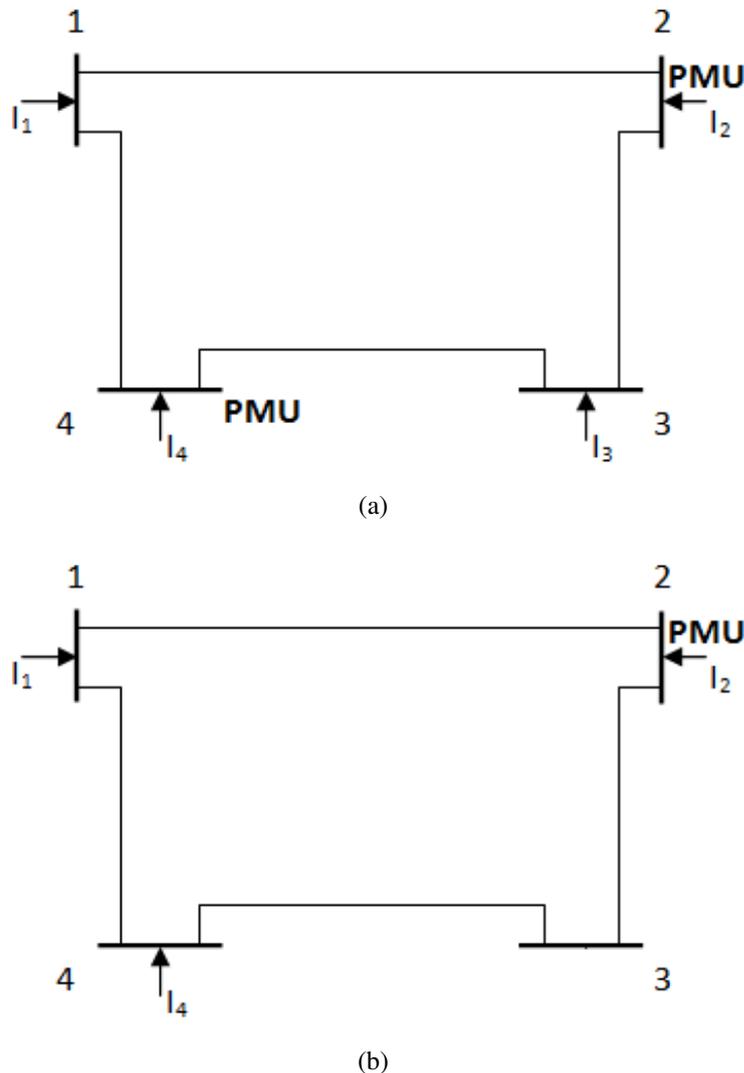


Figure 2.3: Optimal PMU Placement for a Four Bus System (a) With No ZIBs, and (b) Considering Bus 3 as a ZIB

Figure 2.3 (a) considers that there is no ZIB is present in the four bus system while bus 3 is considered as a ZIB in Figure 2.3 (b). For the system in Figure 2.3 (a), it can be easily seen that a minimum of two PMUs are required to make the system completely observable.

If a PMU is placed on bus 2, another PMU at any of the buses viz. 1, 3 or at bus 4 is required to observe bus 4. In contrast, consider a system in Figure 2.3 (b). With a PMU at bus 2, current in branch 3-4 also becomes known as the bus 3 is a ZIB, i.e., $I_{23} = I_{34}$. Since the line parameters are known, the voltage at bus 4 can be calculated using,

$$V_4 = V_3 - I_{23}Z_{34} \quad (2.6)$$

Therefore, a separate PMU is not required to observe bus 4 for the system shown in Figure 2.3 (b). Henceforth, it is seen that inclusion of ZI effect can be helpful in reducing the total number of PMUs required for complete system observability. Considering this perspective, the following rules have been considered in the PMU placement scheme.

1. *If all the branch current phasors incident to a ZIB are known except one, then the unknown branch current phasor can be obtained by applying Kirchoff's current law at the ZIB.*
2. *Similarly, when the voltage phasors at all the buses incident to the ZIB are known, then the voltage phasor at the ZIB can be obtained using Kirchoff's voltage law at the ZIB.*

To model the zero injection effect in the proposed placement method, a simple topological transformation method has been developed in this chapter.

Considering ZIBs as virtual buses, the binary connectivity matrix of the power system is transformed using,

$$C_{mn}^{(z)} = C_{mn} + T_{mn} \quad (2.7)$$

Consider a three bus system, where buses 'm' and 'n' are incident to a ZIB 'k' as shown in Figure 2.4. The elements of the transformation matrix are determined using the following conditions.

Condition 1: If buses 'm' and 'n' are not radial or ZIBs, then these buses can be connected to one another making $T_{mn} = 1$ and $T_{nm} = 1$, as shown in zone I.

Condition 2: If either bus 'm' or bus 'n' is a radial or ZIB, then the binary connectivity parameter between these buses is modified using, $T_{mn} = 1$ and $T_{nm} = 0$ as shown in zone II.

Condition 3: When both the buses 'm' and 'n' are radial and ZIBs as shown in zone III then, the connectivity parameter between these buses cannot be modified, ie., $T_{mn} = 0$ and $T_{nm} = 0$.

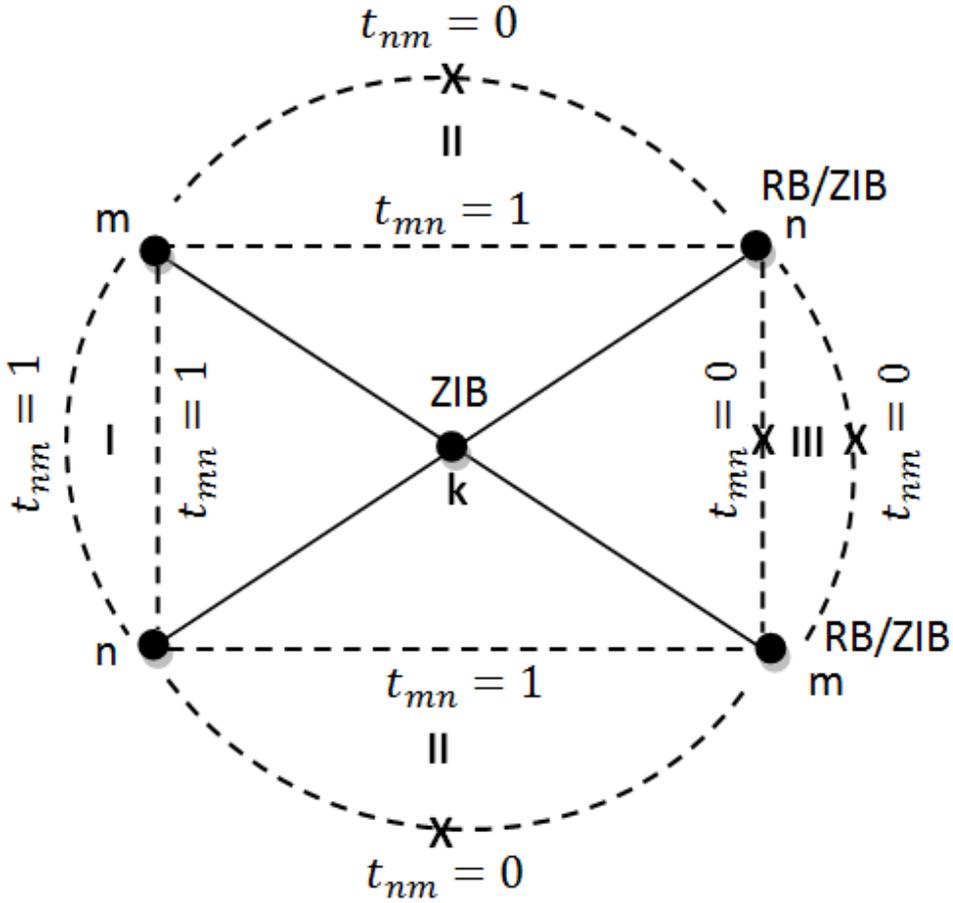


Figure 2.4: Logical Representation of Modelling of ZIBs

2.3.2 Optimal PMU placement during single branch outage

The loss of line between buses ‘*i*’ and ‘*j*’ makes the elements of CM: $C_{ij} = 0$ and $C_{ji} = 0$. As the number of branch outages increase, the optimal number of PMUs required to make the system completely observable also increases. However, the outage of the line connecting radial buses is not considered because any outage on the radial link islands the radial bus from the rest of the system. This makes the entire power system unobservable without restoring those lines [109].

2.3.3 Optimal PMU placement during single PMU outage

The optimal placement set obtained during the system intact conditions do not guarantee complete observability in the event of any measurement loss due to PMU failure. The complete observability during single PMU outage is determined after stage II of the proposed method. This is achieved by modifying the observability condition such that each bus is ob-

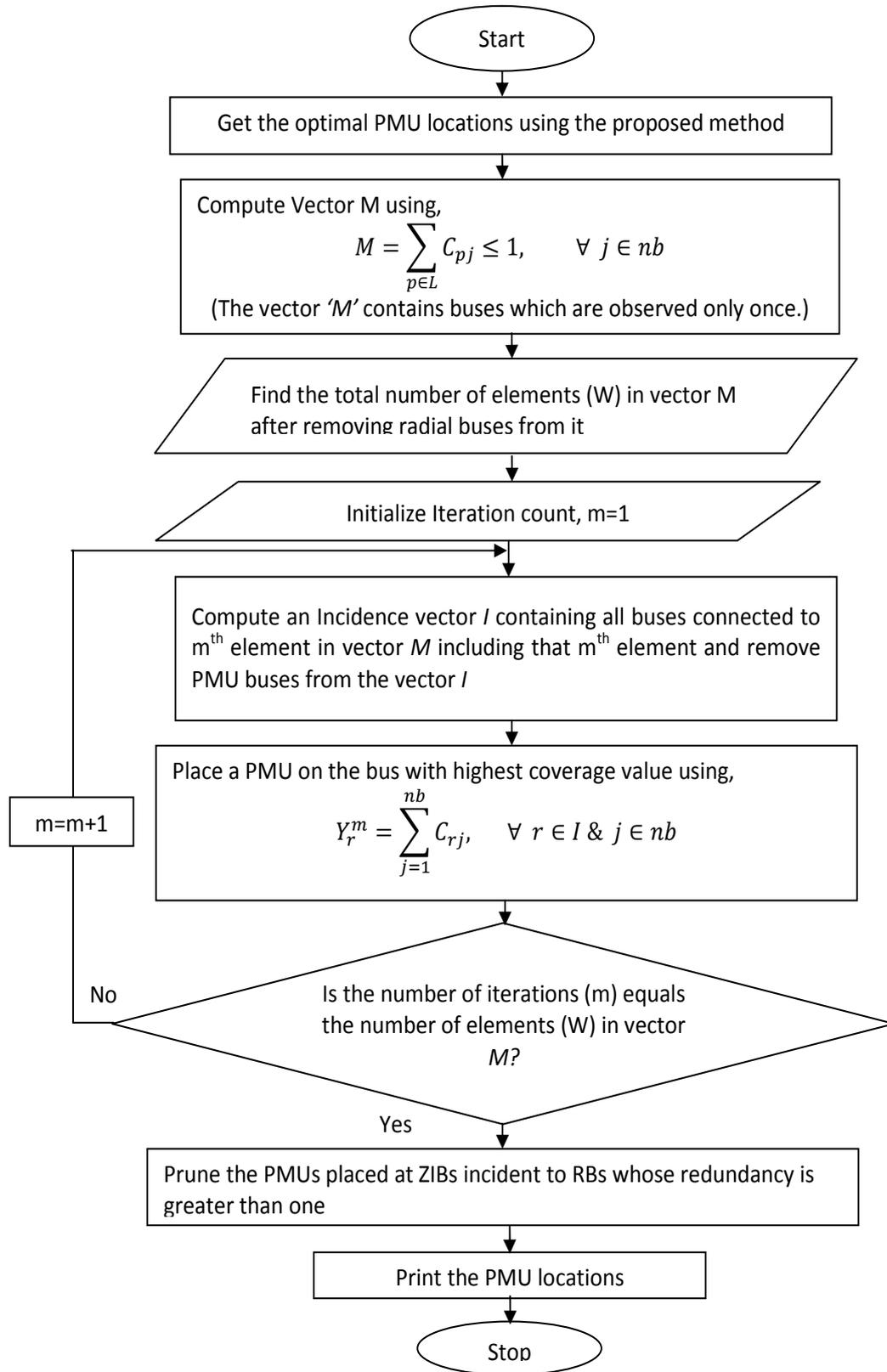


Figure 2.5: Flowchart of Optimal PMU Placement during Single PMU Outage

served atleast once by two different PMUs. In other words, the observability of each bus is set to two. However, the radial buses which are already observed by the zero injection effect are excluded from this condition. This is to ensure that no PMUs are placed at the ZIBs incident to the radial buses. The flowchart for obtaining PMU placement during single PMU outage using the proposed method is shown in Figure 2.5.

2.3.4 PMU Placement in the presence of Conventional Flow Measurements (CFM)

Most of the methods have considered only single flow measurement connected to a bus whereas, the proposed approach is designed in such a way that it can handle both single as well as multiple flow measurements connected to a bus. Consider the three buses in which a flow meter is placed on a line k - j as shown in Figure 2.6 (a). The complex power injected into bus ‘ k ’ of the power system is determined using,

$$V_k I_{kj}^* = P_{kj} + jQ_{kj} \quad (2.8)$$

The line flows (P_{kj}, Q_{kj}) on the line k - j can be measured directly using a flow meter installed at line k - j . As the voltage phasor (V_k) at bus ‘ k ’ is obtained indirectly by a PMU at bus ‘ i ’, the line current (I_{kj}) can be determined using (2.8). With the known line current (I_{kj}) and voltage phasor (V_k) at one end of the line, the voltage phasor (V_j) at the other end can be easily obtained using the observability rules discussed in section 2.2. Thus, the presence of flow meter on the line k - j makes the bus ‘ j ’ observable by a PMU installed at far-end neighbor bus ‘ i ’.

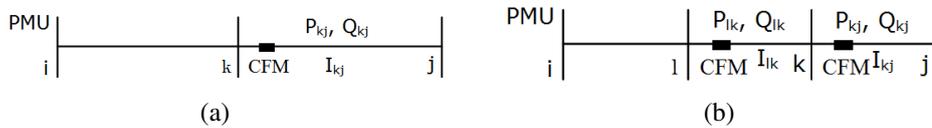


Figure 2.6: With Single (a) and Multiple CFMs (b) Connected to a Bus ‘ k ’

Similar approach has been implemented when multiple flow measurements are connected to a bus ‘ k ’ as shown in Figure 2.6 (b). Here, the complex power injected into bus ‘ l ’ is determined using,

$$V_l I_{lk}^* = P_{lk} + jQ_{lk} \quad (2.9)$$

Since the line flows (P_{lk}, Q_{lk}) are known and the voltage phasor (V_l) at bus ‘ l ’ is measured

by a PMU at bus 'i', the line current (I_{lk}) can be determined using (2.9). Therefore, the voltage phasor (V_k) at bus 'k' is obtained using the rules mentioned in section 2.2. Similarly, the line current (I_{kj}) can be directly determined using (2.8) as the line flows (P_{kj}, Q_{kj}) and the voltage phasor (V_k) at bus 'k' are known. Hence, the voltage phasor (V_j) at the bus 'j' can be obtained using the observability rules discussed in section 2.2. Thus, the presence of multiple flow meters on a bus 'k' makes the buses 'k' and 'j' observable if a PMU is installed at bus 'i'.

To incorporate these flow measurements into the PMU placement, the topology of the entire network is reconfigured using,

$$C_{ij}^{(f)} = C_{ij} + F_{ij} \quad (2.10)$$

and,

$$F_{ij} = \begin{cases} 1, & \text{if } CFM_{kj} = 1 \text{ and buses 'k' and 'i' are incident} \\ 1, & \text{if } CFM_{lk} = 1 \text{ and } CFM_{kj} = 1 \\ 0, & \text{if } CFM_{kj} = 0 \end{cases}$$

In addition to these flow measurements, excluding ZIBs from the PMU placement set reduces the requisite PMU quantity to a minimum PMU numbers necessary for obtaining complete system observability.

2.4 Case Studies

The two stage method described in section 2.3 is used as the placement algorithm to derive the minimum number of PMUs required for system observability under system intact as well as during contingency conditions such as single line loss and single PMU loss. The simulation results obtained on IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus networks using the proposed two stage method are presented in this section. These results are also compared with the existing methods to validate the effectiveness of the proposed approach. The information about the system characteristics, single line diagram and generation as well as load data of the above test systems are given in Appendix B, C and D respectively. The optimal PMU placement has been obtained under system intact condition considering two cases viz. (i) Including ZIBs for PMU placement, (ii) Excluding ZIBs for PMU placement. Further, the presence of flow measurements has also been considered for obtaining PMU placement in order to validate the proposed method in the existing power system.

Table 2.1: Details of the Three Test Systems

Test Systems	Radial Buses		Zero Injection Buses	
	Numbers	Locations	Numbers	Locations
IEEE 14-bus	1	8	1	7
IEEE 30-bus	3	11, 13, 26	6	6, 9, 22, 25, 27, 28
Indian 246-bus	31	2, 4, 5, 12, 30, 31, 38, 41, 47, 51, 52, 53, 58, 76, 77, 112, 120, 123, 124, 135, 149, 153, 156, 159, 172, 178, 189, 208, 224, 242, 246	58	54, 56, 59, 61, 62, 63, 69, 70, 71, 72, 73, 74, 75, 80, 81, 86, 102, 103, 104, 107, 122, 126, 129, 131, 147, 154, 155, 167, 175, 179, 180, 183, 209, 210, 211, 212, 213, 214, 215, 216, 217, 221, 222, 226, 229, 230, 231, 232, 233, 234, 236, 237, 238, 239, 240, 241, 243, 244

Table 2.2: Optimal Number of PMUs during System Intact Condition

Test Systems	Including ZIBs		Excluding ZIBs	
	Stage I(BFS)	Stage II(Pruning)	Stage I(BFS)	Stage II(Pruning)
IEEE 14-bus	4	4	3	3
IEEE 30-bus	10	10	8	7
Indian 246-bus	83	77	65	57

2.4.1 Optimal PMU placement during system intact condition

The details about the number and locations of radial buses and zero injection buses for the three test systems are given in Table 2.1. The number of PMUs obtained at the end of stage I and stage II under system intact case is shown in Table 2.2 for all the test systems with inclusion as well as exclusion of ZIBs from the placement set. It can be seen that there is no or little difference in the number of PMUs obtained at the end of the two stages for IEEE 14-bus and IEEE 30-bus systems. This is due to the smaller size of the test systems. However, in the practical 246-bus Indian system, 83 buses are selected for the placement of PMUs (including ZIBs) at the end of stage I and these are further reduced to 77 buses at the end of stage II. Similar observations are made while excluding ZIBs from the PMU placement set. The optimal number of PMUs required for an Indian 246-bus system is 77 with the inclusion of ZIBs in the placement set and 57 when ZIBs are excluded from the placement set under system intact case. Table 2.3 shows the optimal locations of PMU for the test systems under system intact condition with no PMUs at ZIBs.

Table 2.3: Optimal PMU Locations for the System Intact Case with No PMUs at ZIBs

Test Systems	PMU Locations
IEEE 14-bus	2, 6, 9
IEEE 30-bus	2, 4, 10, 12, 18, 24, 29
Indian 246-bus	3, 6, 11, 15, 21, 24, 29, 33, 34, 35, 36, 40, 44, 48, 54, 55, 63, 65, 82, 83, 88, 89, 91, 96, 97, 106, 109, 113, 116, 118, 121, 125, 132, 134, 140, 141, 142, 157, 158, 160, 165, 166, 168, 181, 185, 187, 190, 191, 194, 199, 201, 203, 205, 218, 219, 235, 245

2.4.2 Optimal PMU placement during contingency conditions

Any contingencies incurred due to the loss of line or PMU would require higher number of PMU installations to maintain system observability under these conditions. This is because the loss of line between any two nodes changes the entire topology of the system. As discussed earlier in section 2.3.2, the outage at the radial line has not been considered while performing this analysis. The optimal number and locations of PMU obtained during single line outage for all the test systems are shown in Table 2.4.

It can be seen that the number of PMUs required to maintain system observability increases in this case as compared with those obtained under system intact case. A failure of

Table 2.4: Optimal PMU Placement during Single Branch Outage

Test Systems	Outaged Line	No of PMUs	PMU Locations
IEEE 14-bus	1-2	5	3, 5, 9, 11, 12
IEEE 30-bus	27-28	7	2, 4, 10, 12, 18, 24, 29
Indian 246-bus	121-122	58	3, 6, 11, 15, 21, 24, 29, 33, 34, 35, 36, 40, 44, 48, 54, 55, 63, 65, 82, 83, 88, 89, 91, 96, 97, 106, 109, 113, 116, 118, 121, 122, 125, 132, 134, 140, 141, 142, 157, 158, 160, 165, 166, 168, 181, 185, 187, 190, 191, 194, 199, 201, 203, 205, 218, 219, 235, 245

a single PMU device or multiple devices affects the System Observability (SO) adversely as it leaves some of the buses unobservable. However, the proposed method ensures complete observability even in the loss of single PMU device. The results of the proposed method for all the test systems considering single PMU failure are shown in Table 2.5.

It can be observed that the loss of single PMU has more adverse effects on the system observability in comparison with the results obtained during single line outage. The results of the proposed method for system intact and contingency cases are compared with the results of the existing methods as shown in Table 2.6. These results indicate that the proposed method requires same number of PMUs as determined by existing methods for IEEE 14-bus system during system intact and during contingencies. The results obtained for IEEE 30-bus and Indian 246-bus systems clearly show that the proposed method offers complete system observability with a lesser number of PMUs than the existing PMU placement methods during all operating conditions.

Table 2.5: Optimal PMU Placement during Single PMU Outage

Test Systems	No of PMUs	PMU Locations
IEEE 14-bus	7	2, 4, 5, 6, 9, 10, 13
IEEE 30-bus	13	1, 2, 4, 7, 10, 12, 15, 16, 18, 19, 24, 27, 29
Indian 246-bus	117	1, 3, 6, 7, 9, 10, 11, 13, 14, 15, 20, 21, 23, 24, 27, 29, 32, 33, 34, 35, 36, 39, 40, 42, 44, 45, 46, 48, 49, 54, 55, 56, 61, 62, 63, 64, 65, 67, 68, 70, 74, 82, 83, 84, 85, 88, 89, 90, 91, 92, 96, 97, 100, 101, 105, 106, 109, 111, 113, 116, 118, 119, 121, 125, 130, 132, 133, 134, 136, 138, 139, 140, 141, 142, 143, 145, 146, 150, 157, 158, 160, 161, 162, 163, 165, 166, 168, 169, 170, 173, 181, 182, 185, 186, 187, 190, 191, 193, 194, 195, 197, 199, 201, 202, 203, 204, 205, 207, 218, 219, 221, 223, 234, 235, 238, 239, 245

Table 2.6: Comparative Study of the Proposed Method with the Existing Methods

Analytical Data	IEEE 14-bus			IEEE 30-bus			Indian 246-bus		
	Case I	Case II	Case III	Case I	Case II	Case III	Case I	Case II	Case III
Binary Search [110]	3	7	NA	7	10	NA	NA	NA	NA
Integer Programming [111]	3	NA	7	7	NA	17	NA	NA	NA
Binary ILP [112]	3	7	7	7	13	14	NA	NA	NA
ILP Method [28, 113]	3	7	7	7	13	15	70	71	NA
Proposed BFS Method	3	5	7	7	7	13	57	58	117

Case I - Optimal PMU placement results during system intact case,
Case II - Optimal PMU placement results during single line outage,
Case III - Optimal PMU placement results during single PMU outage.

2.4.3 Optimal PMU placement during the presence of CFM

When flow measuring devices are installed at some of the transmission lines, the given power system network can be made completely observable with a limited number of PMUs. This is because some buses can be directly observed through the measurements obtained from the flow meters. The transmission lines having flow measurement device are shown in Table 2.7. In this case, the number of PMUs required to make the system completely observ-

Table 2.7: Branches with Flow Measurements

Test Systems	Numbers	Location of flow measurements
IEEE 14-bus	3	1-5, 6-11, 9-10
IEEE 30-bus	7	1-2, 2-4, 2-5, 5-7, 6-10, 9-11, 27-30
Indian 246-bus	77	43-44, 50-55, 51-54, 52-54, 54-55, 25-57, 2-187, 59-32, 59-216, 3-71, 4-62, 62-71, 63-70, 7-79, 64-67, 65-100, 66-67, 67-91, 70-72, 72-73, 74-86, 74-246, 75-76, 75-91, 11-86, 82-83, 82-92, 87-100, 13-90, 90-96, 90-97, 16-125, 116-128, 129-232, 132-149, 133-182, 140-143, 140-144, 142-145, 146-148, 147-150, 181-230, 156-158, 163-167, 168-171, 169-170, 173-174, 24-191, 24-192, 24-1, 184-197, 187-189, 195-196, 198-1, 1-199, 1-226, 201-231, 27-203, 211-217, 32-33, 32-218, 223-39, 231-39, 234-237, 40-41, 235-236, 61-53, 6-5, 10-8, 72-84, 240-139, 23-22, 209-185, 210-187, 211-190, 215-27, 235-38

Table 2.8: Optimal PMU Placement during the Presence of CFM

Test Systems	PMUs	PMU Locations	% Decrease in PMUs
IEEE 14-bus	2	4, 13	33.33
IEEE 30-bus	5	2, 12, 15, 20, 30	28.57
Indian 246-bus	33	15, 21, 29, 32, 34, 35, 36, 40, 48, 55, 60, 65, 82, 89, 101, 106, 109, 113, 121, 125, 133, 141, 144, 157, 160, 165, 168, 174, 186, 194, 205, 219, 245	44.07

able decreases as compared with the results obtained during system intact conditions. The results of the proposed method for the three test systems considering flow measurements are shown in Table 2.8, alongwith the amount of reduction in the number of PMUs due to flow measurements. These results have been obtained under system intact case.

2.5 Conclusions

This chapter proposes a new method based on intelligent search technique for the optimal placement of PMUs to make the power system topologically observable. The proposed method determines the optimal locations of PMUs in two stages. Stage I determines the sub-optimal locations of PMUs using best first search, which is an intelligent search algorithm with an ability to change its search path from the current node to the most promising node. From the results of stage I, the redundant PMU locations are identified and eliminated in stage II using pruning. Another important aspect is that the proposed method is extended to incorporate the presence of conventional flow measurements in the system. The proposed placement method is also found to be effective in handling both single as well as multiple flow measurements connected to a bus. The method was successfully applied on the test systems under normal operation as well as during contingencies. Simulation results demonstrate that the proposed method is more effective than the existing methods, especially for larger systems. Further, the proposed method is computationally efficient as the simulation time is less than 2 seconds for all the systems.

Chapter 3

Optimal Placement of PMUs Considering Cascaded Failures

3.1 Introduction

Security of power systems is challenged by the cascaded outages, which may lead to uncontrolled splitting of electric grids called islanding [114]. This uncontrolled splitting of power system network with a reasonable power imbalance is the significant reason for wide-area system blackouts. During such islanding conditions, a portion of the system containing both load and generation may isolate and operate independently even though it is disconnected from the rest of the system [115]. This can be even more dangerous leading to electric shock to maintenance personnel, flickers due to voltage and frequency instability which results in equipment damage. Thus, the unintentional formation of electric islands causes enormous loss to both consumers and utilities. Therefore, an islanding condition must be identified and disconnected immediately in order to save the system from collapsing.

Power system islanding can be classified into controlled islanding and uncontrolled islanding [116]. Controlled islanding is a condition in which the power network is separated into several planned islands in order to prevent catastrophic collapse of the whole system [117]- [118]. Thus, the propagation of the local weaknesses to the rest of the system is eliminated with this known splitting [119]. To date, various methods of controlled islanding have been proposed in [114], [117], [119–123]. The controlled islanding acts as a protection scheme whereas the uncontrolled islanding is a serious disturbance to system integrity and security. As a consequence of the uncontrolled splitting, the island and the

main grid lose their observability to each other. The events that lead to this type of splitting are mainly due to tripping of multiple lines caused by branch limit violations, breaker malfunctions and natural disasters like hurricanes, storms, etc. During such situations, the real time synchronized measurements from all those islanded parts can be utilized to take proper control actions for protecting the stability and integrity of each island. This necessitates observability of individual islands. Hence, there is a need of an appropriate placement scheme of synchronized measurements, which allows effective monitoring of the individual islands in order to mitigate the risk of blackouts.

Most of the existing OPP methods have focussed only on finding the optimal PMU locations considering operation of power system as a single and integrated network. Further, they have been extended to consider contingencies such as line loss and PMU loss. Recognizing the severity of islanding disturbances, an integer linear programming method based OPP scheme has been proposed in [124] considering controlled islanding of power systems. In addition to system islanding, measurement redundancy and single contingencies such as line loss and PMU loss has also been studied alongwith OPP in this work. During this controlled islanding scenario, the entire power system is splitted into several planned islands, following a disturbance, to protect the system from collapsing. However, if control actions fail, the system may break-up into several uncontrolled islands. In such a case, the stable operation of islands become the top priority. This can be achieved by maintaining complete observability of each island using synchronized measurements, which can further be utilized to restore normal operation. This chapter considers this aspect of power system operation while determining the locations of PMUs.

The two stage PMU placement method proposed in Chapter 2 is utilized in this chapter to determine the optimal locations of PMUs for maintaining complete observability of power systems during cascaded outages. Cascaded failures with islanding and non-islanding conditions have been considered. To detect whether a cascaded failure has led to islanding/non-islanding condition, a topology based algorithm has been developed. In addition to power system observability, measurement redundancy is also incorporated to improve state estimation. Additional contingency of single line loss and single PMU loss have also been considered to take place after cascading events. The proposed method has been tested on IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus systems.

3.2 Proposed Approach

3.2.1 Simulation of Cascaded Failures

The propagation of cascaded failures through the bulk transmission network has been studied by analyzing each line outage in detail. Each single line contingency is simulated and the new power flows are calculated using Newton Raphson load flow. The lines violating the flow limits are identified and ranked on the basis of their amount of overloading. If the lines connected to a bus are used to their capacities, then an increase in loading will result in their outages. In such a case, the least loaded line is considered to have sufficient capacity remaining to take additional load without tripping, thus avoiding the isolation of a single bus. While carrying out the above analysis, it was observed that not all the cascaded failures led to islanding conditions. Therefore, in this chapter, two cases have been considered for analyzing cascaded failures (1) cascaded non-islanding condition, and (2) cascaded islanding condition. In order to identify whether a particular cascaded failure leads to islanding condition, an algorithm based on system topology information has been developed. A depth observability vector has been formed, whose elements are obtained using

$$D_j = \sum_{p \in M} C_{pj}, \quad \forall j \in nb \quad (3.1)$$

where, M is a vector consisting of nodes incident to any randomly selected node i , including i^{th} node, C_{pj} is the pj^{th} element of connectivity matrix and nb is the total number of system buses.

A depth observability vector contains information about all the nodes connected to each element in vector ' M '. The element (D_j) of the depth observability vector would be non-zero when bus ' j ' is observed by bus ' i ' ($i \neq j$), where bus ' i ' is a randomly selected bus. The zero value of the element D_j refers that bus ' j ' is not observable by bus ' i '. Thus, after obtaining the observability status of all the buses, the depth observability vector will be a full-1 vector for a healthy system. Failure to achieve full-1 vector demonstrates a physical separation in the system. Using this scheme, both islanding and non-islanding conditions can be easily identified, regardless of the system size. Mathematically, the island detection scheme is expressed using,

$$Islanding = \begin{cases} No, & \text{if } D = \text{Full-1 vector} \\ Yes, & \text{if } D \neq \text{Full-1 vector} \end{cases} \quad (3.2)$$

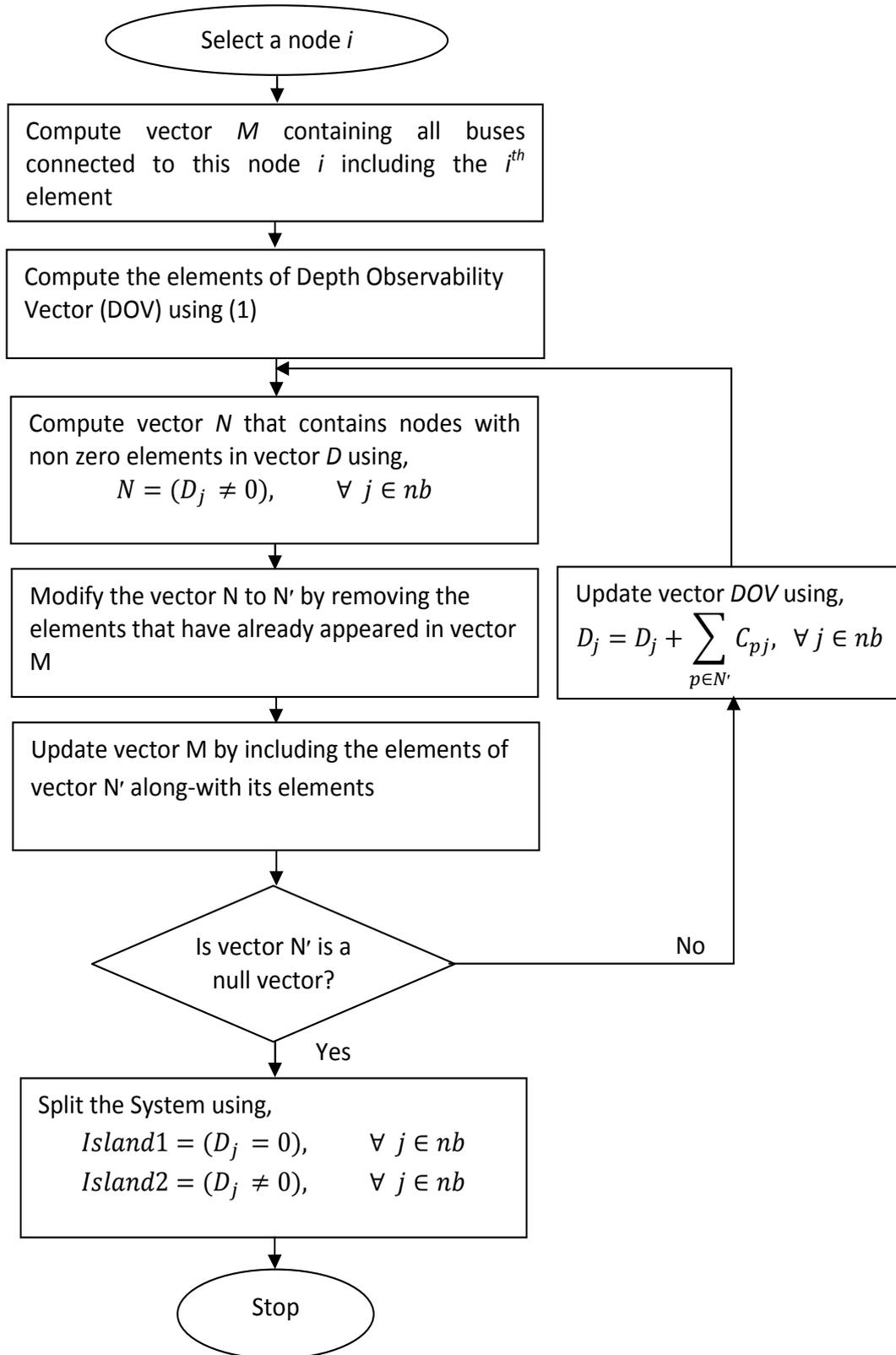


Figure 3.1: Flowchart for Island Identification

The flowchart for detecting islanding and non-islanding conditions using the proposed topology based approach is shown in Figure 3.1. This analysis enables the operator to gain sufficient knowledge on the vulnerable power system elements which may lead to cascaded failures. Considering this perspective, the context of vulnerability assessment for cascaded failures has been analysed in this chapter. Mostly, power system experiences low changes, migrating from one steady state to another. Hence, a steady-state model of the power system has been considered to understand the vulnerability of the cascaded sequence of events.

3.2.2 Proposed Redundant Observability method

Redundant observations are always desirable in order to enhance the reliability of state estimation. A two-stage method proposed in Chapter 2, has been utilized to determine the optimal locations of PMUs such that system is completely observable during cascaded events. In addition to system observability, the above two stage method has been further extended, such that the measurement redundancy is obtained with the same number of PMUs as needed to maintain system observability in chapter 2. To achieve this, PMUs from the locations obtained using the two stage method are sequentially removed and relocated using the following procedure.

1. Remove one PMU from the final placement set and find the number of unobserved nodes.
2. If the number of unobserved node is found to be one, then an incidence vector, I_N is obtained consisting of nodes connected to the unobserved node.
3. Place a PMU at the incident node having the highest connectivity.
4. In case, if the number of unobserved buses are more than one, then that PMU which is removed is considered to be crucial for system observability and hence preserved.
5. This process is repeated for all the PMU locations obtained using the two-stage method.

The proposed method offers multiple PMU placement sets with different levels of redundancy pattern. Among these solution sets, a placement set that offers the highest amount of redundancy at the system buses is chosen as the final optimal solution. The flowchart for obtaining the enhanced observability using the proposed approach is shown in Figure.3.2

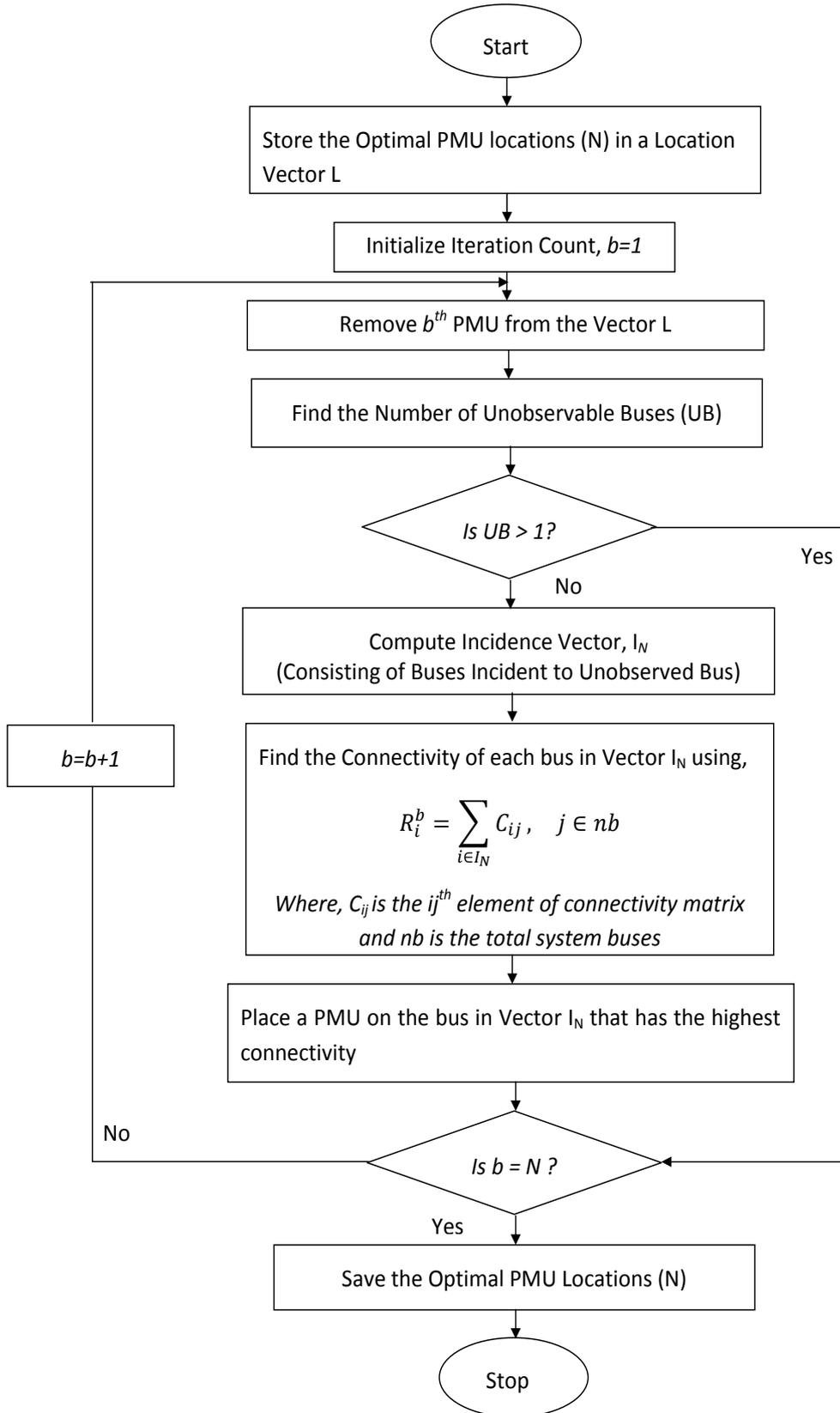


Figure 3.2: Flowchart of the Proposed Redundant Observability Method

3.3 Case Studies

The proposed OPP scheme for complete observability as well as for measurement redundancy has been simulated on IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus networks. These studies have been conducted considering two operating scenarios viz. (1) cascaded outages with non-islanding operation, and (2) cascaded outages with islanding operation. Furthermore, single line and single PMU outage contingencies have also been considered to take place after the cascaded events and their effects on the OPP solution is studied. The results of the proposed OPP scheme obtained for the three test systems are discussed below.

3.3.1 OPP during Cascaded Failures

The post contingent situation of the test systems leading to non-islanding and islanding operations are shown in Tables 3.1 and 3.2, respectively. The outage of lines shown in column 2 of Table 3.1 overloaded the lines depicted in the last column and subsequently resulted in the tripping of these lines. However, the system operates as a single and integrated network even after this cascaded failure. The loss of lines given in column 2 of Table 3.2 resulted in overloading of the lines as shown in the last column and thus, these lines are sequentially removed one by one. When all these overloaded lines are tripped, the system is splitted into islands. The potential islanded regions for IEEE 14-bus and IEEE 30-bus systems are shown in Figure 3.3 and Figure 3.4 respectively. The system partitioning is labeled by the cut-off location and the overloaded lines are represented using the dotted lines. In IEEE 14-bus system, each island contains 7 buses whereas, two islands are formed in IEEE 30-bus system with 24 buses and 6 buses respectively. Similarly, the splitting of Indian 246-bus system is obtained with 231 buses in one of the islands and the rest 15 buses in the other island. The details of the buses falling in the respective islands can be found from column 4 of Table 3.2.

Table 3.1: Post-contingency Leading to Cascaded Outages with Non-Islanding Operation

Test Systems	Outaged Line	No of Islands	No of Buses	Lines Tripped due to Overload
IEEE 14-Bus	1-2	1	14 (1-14)	4-5, 3-4, 10-11, 13-14, 12-13
IEEE 30-Bus	15-23	1	30 (1-30)	18-19, 16-17, 10-21
Indian 246-Bus	121-122	1	246 (1-246)	24-1, 24-191, 1-199, 147-150, 183-34, 17-34, 115-118, 201-226

Table 3.2: Post-contingency Leading to Cascaded Outages with Islanding Operation

Test Systems	Outaged Line	No of Islands	No of Buses	Lines Tripped due to Overload
IEEE 14-Bus	2-3	2	7 (1-2, 5-6, 11-13), 7 (3-4, 7-10, 14)	4-5, 2-4, 2-5, 10-11, 13-14, 12-13
IEEE 30-Bus	15-23	2	24 (1-20, 27-30), 6 (21-26)	18-19, 10-21, 16-17, 10-22, 9-10, 25-27, 1-2
Indian 246-Bus	7-105	2	231 (1-15, 17-41, 43-104, 108-112, 115-122, 126-129, 131-241, 246), 15 (16, 42, 105- 107, 113-114, 123- 125, 130, 242-245)	7-105, 66-130, 66-67, 113- 126, 90-97, 113-127, 109-16, 65-110, 65-68, 78-91, 114- 130, 72-73, 113-114, 87-96, 66-98, 113-129, 79-88, 97- 98, 7-67

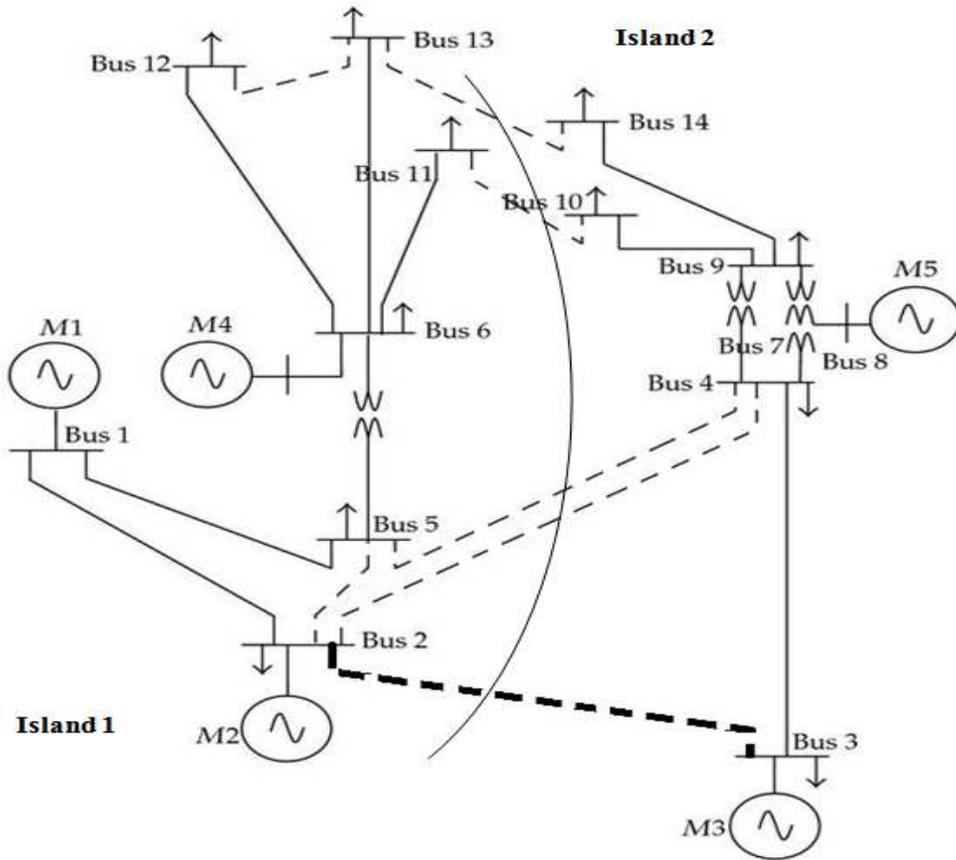


Figure 3.3: Splitting of IEEE 14-bus System

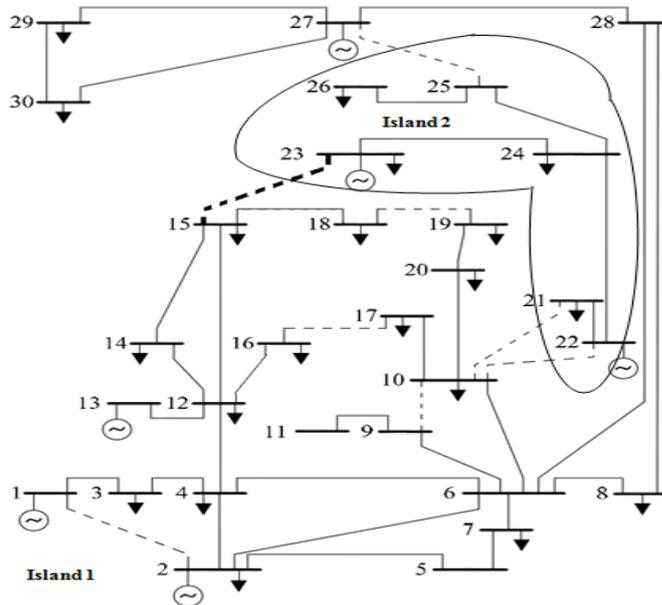


Figure 3.4: Splitting of IEEE 30-bus System

Table 3.3 shows the optimal number and locations of PMUs required to make the test systems observable during cascaded failures leading to non-islanding and islanding operations. It can be observed that the number of PMUs has been considerably increased to 5 and 12

for IEEE 14-bus and 30-bus systems, respectively. However, for Indian 246-bus system, 81 PMUs and 78 PMUs are required for complete observability during cascaded non-islanding and islanding operations, respectively. It is to be noted that these cascaded sequence of events changes, when a different line outage condition is considered. In such a case, the operators should use the knowledge gained from the past experiences to identify the vulnerable portions of the power system. It can be concluded from these results that the number of PMUs required to maintain system observability during cascaded events increases slightly in comparison to that required during system intact case. However, the PMU locations obtained using the proposed approach are able to monitor the system under normal operating conditions as well as during cascaded events. Thus, in case uncontrolled islanding occurs, these synchronized measurements will help to maintain the stable operation of islands and in restoring to normal operation.

3.3.2 OPP during Cascaded Failures with Contingencies

The proposed OPP scheme has also been validated during single line and single PMU outages. The additional loss of line, irrespective of the cascaded outages would make the test systems unobserved with the OPP solution shown in Table 3.4. The outage at the radial link has not been considered because the system cannot be made observable without restoring those lines. The optimal number and locations of PMU obtained during cascaded events with single line contingency are shown in Table 3.4. IEEE 14-bus and IEEE 30-bus systems require 6 PMUs and 12 PMUs, respectively to make them completely observable. The complete observability of Indian 246-bus system can be maintained with 82 PMUs during non islanding operation and 78 PMUs during islanding operation.

Table 3.3: Optimal Locations of PMUs during Cascaded Failures

Test Systems	With No Islanding		With Islanding	
	Number	Locations of PMUs	Number	Locations of PMUs
IEEE 14-bus	5	1-2, 6-7, 9	5	1, 3, 6-7, 9
IEEE 30-bus	12	1, 5-6, 9, 12, 17-19, 21, 24-25, 27	12	1, 5-6, 9, 12, 17-19, 21, 24-25, 27
Indian 246-bus	81	1, 3, 6, 8-9, 15, 19, 23-24, 26, 28-29, 32, 34, 40, 43, 48, 50, 54, 57, 61-68, 70, 74-75, 79-81, 83-85, 87, 90, 92-93, 106, 109, 111, 113, 115, 117-118, 122, 125-126, 132-134, 140-142, 147, 157-158, 160, 163, 165-166, 168, 181, 185, 187, 190-191, 197, 199, 203, 216, 219-220, 225, 228-229, 235, 237, 239, 243, 245	78	1, 3, 6, 10-11, 15, 21, 23, 28-29, 32, 34, 36, 40, 43, 48, 50, 54, 57, 61-63, 65-66, 68, 74-75, 79-80, 83-85, 87, 91-93, 101, 106, 110, 113, 116-117, 121-122, 125-126, 129, 132, 134, 140-142, 147, 157-158, 161, 163, 168, 173, 179, 181-182, 185, 187, 190-192, 199, 201, 203, 216, 219-220, 225, 235, 239, 243, 245

Table 3.4: Optimal Locations of PMUs during Cascaded Failures with Single Line Outage

Test Systems	With No Islanding		With Islanding	
	Number	Locations of PMUs	Number	Locations of PMUs
IEEE 14-bus	6	1-2, 6-7, 10, 14	6	1, 3, 6-7, 10, 14
IEEE 30-bus	12	1, 5-6, 9, 12, 17-19, 21, 24-25, 27	12	1, 5-6, 9, 12, 17-19, 21, 24-25, 27
Indian 246-bus	82	1, 3, 6, 8-9, 15, 19, 23-24, 26, 28-29, 32, 34, 40, 43, 48, 50, 54, 57, 61-63, 67-68, 70, 74-75, 79-81, 83-85, 87, 90, 92-93, 106, 109, 111, 113, 115, 117-118, 122, 125-126, 128, 132-134, 140-142, 147, 157-158, 160, 163, 165-166, 168, 181, 185, 187, 190-191, 197, 199, 203, 216, 219-220, 225, 228-229, 235, 237, 239, 243, 245	78	1, 3, 6, 10-11, 15, 21, 23, 28-29, 32, 34, 36, 40, 43, 48, 50, 54, 57, 61-63, 65-66, 68, 74-75, 79-80, 83-85, 87, 91-93, 101, 106, 110, 113, 116-117, 121-122, 125-126, 129, 132, 134, 140-142, 147, 157-158, 161, 163, 168, 173, 179, 181-182, 185, 187, 190-192, 199, 201, 203, 216, 219-220, 225, 235, 239, 243, 245

Table 3.5 lists the optimal number and locations of PMUs obtained using the proposed method for maintaining complete observability of the test systems during cascaded failures along-with single PMU outage. The failure of a measurement device may leave some portion of the system unobserved. However, a modification in the observability condition that each bus is observed atleast once by two different PMUs, may help in maintaining complete observability during PMU outages also. The radial buses which are already observed by the zero injection effect have been excluded from the above modification. It can be observed that 13 PMUs are needed to make the IEEE 14-bus system completely observable during both cascaded non-islanding and islanding operations. However, 22 PMUs and 23 PMUs are required to keep the IEEE 30-bus system observable during such events. To make Indian 246-bus network observable, 146 PMUs are required for cascaded non-islanding operation, while 140 PMUs are needed during cascaded islanding operation.

The number of PMUs required to monitor the test systems during different scenarios of power system operation alongwith single contingencies viz. line loss and PMU loss are summarised in Table 3.6. It can be seen that the number of PMUs required during single line outage are comparable to that required during the base case, whereas single PMU loss needs more PMUs than the other cases. During single PMU outage, it is found that more than half of the system buses need to be equipped with PMUs to have a reliable measurement system. Hence, it is concluded that the loss of measurement has more adverse effects on the system observability than the single line contingency.

Table 3.5: Optimal Locations of PMUs during Cascaded Failures with Single PMU Outage

Test Systems	With No Islanding		With Islanding	
	Number	Locations of PMUs	Number	Locations of PMUs
IEEE 14-bus	13	1-7, 9-14	13	1-7, 9-14
IEEE 30-bus	22	1-2, 4-6, 9-10, 12, 15-25, 27-29	23	1-6, 9-10, 12, 15-25, 27-29
Indian 246-bus	146	1, 3, 6-11, 15, 19-24, 26-29, 32-35, 39-40, 42-44, 48, 50, 54-57, 59, 61-65, 67-72, 74-75, 79-85, 87-94, 96-97, 101, 105-106, 109, 111-113, 115-118, 121, 125-126, 129-130, 132-134, 136, 138-143, 145-147, 154, 157-158, 160-163, 165-168, 173, 175, 181, 185-187, 190-191, 193-195, 197-199, 201-205, 207, 211, 213-214, 216-217, 219-221, 223, 225, 228-229, 231, 233-235, 237-239, 243, 245	140	1, 3, 6-7, 9-11, 13, 15-16, 20-24, 27-29, 32-36, 39-40, 42-44, 48, 50, 54-57, 59, 61-65, 69, 70-72, 74-75, 80-85, 88-94, 97, 100-101, 105-109, 111, 116-118, 121-122, 125-126, 129, 132-134, 136, 138-143, 145-147, 154, 157-158, 160-163, 165-170, 173, 175, 179, 181-182, 185-187, 190-192, 194-195, 197, 199, 201-205, 207, 211, 213, 216-217, 219-221, 223, 225, 229, 231, 233-235, 239, 243, 245

Table 3.6: Optimal PMU Placement during Multiple Operating Scenarios

Analytical Data	Normal Operating Condition			Cascaded Outages (No Islanding)			Cascaded Outages (Islanding)		
	No Out	Line Out	PMU Out	No Out	Line Out	PMU Out	No Out	Line Out	PMU Out
IEEE 14-bus	4	4	8	5	6	13	5	6	13
IEEE 30-bus	10	10	18	12	12	22	12	12	23
Indian 246-bus	77	77	143	81	82	146	78	78	140

3.3.3 OPP considering Measurement Redundancy

Maximizing the measurement redundancy is advantageous as a major portion of the power system remains observable, even if one of the measurement fails. Hence, maximizing bus measurement redundancy is considered in the PMU placement objective to enhance the system observability and the results are given in Table 3.7 considering normal operation. It can be observed from Table 3.7 that three trials resulted in different OPP solution set for IEEE 30-bus and practical 246-bus Indian systems. For IEEE 30-bus system, the second solution is the optimal solution set as 13 buses are observed more than once, even though its redundant observability value is lesser than the third solution set. In case of 246-bus Indian system, the number of redundant observations of the third solution set is found to be higher than the redundant observations obtained in the other solution sets. Further, the number of buses observed more than once in the third solution set is comparatively higher than the other solution sets. Hence, it is the best solution according to the PMU placement objective.

Table 3.7: Redundant Observability based Optimal PMU Placement Solution during Normal Operation

Test Systems	Solution Set	Number of Buses observed more than Once	Number of Re- dundant Observa- tions
IEEE 14-bus	2, 6, 7, 9	4	5
	1, 5, 6, 9, 10, 12, 15, 18, 25, 27	13	18
IEEE 30-bus	1, 2, 6, 9, 10, 12, 15, 18, 25, 27	13	20
	2, 4, 6, 9, 10, 12, 15, 18, 25, 27	12	22
Indian 246-bus	77 PMUs	103	129
	77 PMUs	107	139
	77 PMUs	108	142

The optimal PMU placement locations obtained by the proposed observability and redundant observability methods during cascaded islanding operation are shown in Table 3.8. There is not much difference between the two methods for IEEE 14-bus system as it is a small system. However, in IEEE 30-bus system, 7 placement locations are commonly selected by both the methods, whereas in practical Indian 246-bus system, 59 buses are commonly identified as the PMU locations. It is confirmed that the proposed observability and redundant observability methods offer different optimal PMU placement locations keeping the total number of PMUs to be same.

3.3. CASE STUDIES

Table 3.8: Comparison of the Proposed Observability and Redundant Observability Methods during Cascaded Islanding Operation

Test Systems	Buses(1)	Buses(2)	Buses(3)
IEEE 14-bus	1, 6-7, 9	3	4
IEEE 30-bus	1, 6, 9, 12, 24-25, 27	5, 17-19, 21	2, 10, 15, 20, 22
Indian 246-bus	6, 10-11, 15, 21, 29, 32, 34, 40, 43, 48, 54, 57, 61-63, 65, 74-75, 80, 83-84, 91, 101, 106, 116-117, 121-122, 125-126, 129, 132, 134, 140-142, 147, 157-158, 163, 168, 173, 179, 181, 185, 187, 190-191, 199, 201, 203, 216, 219-220, 235, 239, 243, 245	1, 3, 23, 28, 36, 50, 66, 68, 79, 85, 87, 92-93, 110, 113, 161, 182, 192, 225	7, 16, 22, 24, 55, 71, 82, 89, 94, 100, 108-109, 118, 139, 160, 194, 202, 221, 234

Buses(1): common between both the methods, Buses(2): only in proposed observability method, Buses(3): only in proposed redundant observability method.

Table 3.9: Proposed Observability and Redundant Observability Methods based Total Observability during Normal Operation

Test Systems	Observability		Redundant Observability	
	PMUs	TO(TRO)	PMUs	TO(TRO)
IEEE 14-bus	4	19(5)	4	19(5)
IEEE 30-bus	10	41(11)	10	50(20)
Indian 246-bus	77	346(100)	77	388(142)

In Table 3.9, Total Observability (TO) times and Total Redundant Observability (TRO) times are shown for all the test systems using the proposed observability and redundant observability methods during normal operation. The proposed redundant observability method is found to enhance the total observability. For Indian 246-bus system, the proposed redundant observability method enhances the total observability as much as 42 (388-346) times with the same number of PMUs as that obtained using the proposed observability method. The results of the OPP obtained using both the proposed observability and redundant observability methods during cascaded islanding and non-islanding operations for the test systems are shown in Tables 3.10 and 3.11, respectively. From these results, it is concluded that the proposed redundant observability method offers increased redundancy than the proposed observability method.

Table 3.10: Proposed Observability and Redundant Observability Methods based Total Observability during Cascaded Islanding Operation

Test Systems	Observability		Redundant Observability	
	PMUs	TO(TRO)	PMUs	TO(TRO)
IEEE 14-bus	5	19(5)	5	21(7)
IEEE 30-bus	12	41(11)	12	48(18)
Indian 246-bus	78	342(96)	78	379(133)

Table 3.11: Proposed Observability and Redundant Observability Methods based Total Observability during Cascaded Non-Islanding Operation

Test Systems	Observability		Redundant Observability	
	PMUs	TO(TRO)	PMUs	TO(TRO)
IEEE 14-bus	5	20(6)	5	22(8)
IEEE 30-bus	12	45(15)	12	55(25)
Indian 246-bus	81	362(116)	81	406(160)

3.4 Conclusions

This chapter proposes a suitable OPP scheme to determine the optimal locations of PMUs for maintaining complete system observability during cascaded failures. Both the islanding and the non-islanding cases were generated for the test cases following the cascaded failures. Then, a topology based approach has also been developed to identify the islanded portions. Additional single line and single PMU contingencies have also been considered after the occurrence of cascaded events. Further, the reliability of power system state estimation is enhanced by incorporating measurement redundancy in the proposed method. These results obtained for all the test systems have been compared with the two stage based observability method proposed in Chapter 2. It clearly indicates that the proposed redundant observability method offers better results than the method proposed in Chapter 2 by providing increased redundancy for the same number of PMUs. Also, the proposed redundancy method provides multiple PMU placement solutions having different levels of redundancy for the same number of PMUs. It is also revealed that the proposed OPP scheme can provide complete observability of the system under different operation scenarios viz. normal operation as well as cascaded islanding and non-islanding conditions.

Chapter 4

Review of Various Machine Learning Techniques

4.1 Introduction

In the recent years, the machine learning techniques have been successfully applied in various power system domains such as voltage sensitivity identification [87–89, 93], contingency ranking [90–92], static security assessment [75–78, 83, 84, 86, 94] and dynamic security evaluation [79–82, 85, 95]. The advent of machine learning techniques can overcome the shortcomings of traditional security assessment methods by computing the system security status in a fast and accurate manner. The most widely used methods for security assessment are Artificial Neural Network (ANN) , Support Vector Machine (SVM) and Decision Tree (DT) classifiers. Although ANN based security assessment methods are significantly faster in predicting the system security status, training of these networks is found to be very difficult and time consuming. This is mainly due to the fact that it requires weights between the hidden and output nodes to be updated several times in order to reduce the rate of error value calculated at the output nodes [94]. In case of SVM based pattern recognition approach, selection of kernel parameters and choice of margin parameter is more difficult and requires thorough investigation. Hence, SVM based security assessment methods often exhibit low performance if the information underlying in the data patterns is not properly known [125]. Although DTs are predominately used in classification problems, the use of statistical tools for tracing the relationship among different events can often lead to poor classification results [125]. Therefore, it is concluded that there is a need for more accurate and

faster security assessment technique, which is the basic requirement for real-time monitoring and control of the emerging power systems to avert any catastrophic events.

This chapter reviews the concepts of some intelligent classifiers viz. Wavelet Support Vector Machine (WSVM), Case Based Reasoning (CBR) and AdaBoost algorithm, which have better generalization capability than the traditional classifiers. These techniques have been successful in various domains and thus exhibit lot of potential for security assessment purpose. The design of these classifiers for the proposed security assessment work has been elaborated in the following sections in detail.

4.1.1 Literature Review

This section gives a detailed review on the use of WSVM, CBR and AdaBoost classifiers for various classification problems. The wavelet techniques have been explicitly used in signal analysis and processing. These techniques employ mathematical functions and have been successfully applied in applications such as transient analysis of signals, image processing and communication systems, etc. This technique has also been considered as a powerful tool for the approximation of arbitrary non-linear functions [126]. In this perspective, a new pattern recognition tool called Wavelet Support Vector Machine (WSVM) has been proposed in [126]. This new WSVM classifier, which combines the wavelets with the SVM classifier, has been recently used in classification and regression problems due to its high prediction capability and better performance than the other machine learning techniques [127]. The authors in [128] have utilized the WSVM for prediction of wind speed and in turn the power generated by the wind, which can be calculated from predicted speed value. A WSVM technique has been used in [129] for the detection and classification of faults in induction motors. In [130], the authors have proposed a novel algorithm using WSVM for the detection and classification of voice activity. These studies reveal that WSVM can provide better prediction for complex classification problems than the traditional SVM kernel classifiers such as linear SVM (l-SVM), quadratic SVM (q-SVM), polynomial SVM (p-SVM), multi-layer perceptron SVM (m-SVM) and radial basis function SVM (r-SVM).

Recent advancements in the field of life sciences has helped the researchers to develop artificial intelligence based tools for medical applications. Case Based Reasoning (CBR) approach solves the new problem by retrieving similar past examples and adapting their solutions. Hence, it has been considered an interesting alternative, and predominately applied

in the field of life sciences [131]. Some of its major applications include prediction and classification [132–136], knowledge inference and evaluation [137, 138], etc. In these applications, CBR systems are built for the classification problems mainly to determine whether a problem is a member of a class or not or which of the several classes it may belong to. The development of machine learning algorithms along with CBR technique has brought new opportunities for regression and classification of training samples. In this context, a hybrid system based on Neural Network and Case Based Reasoning (NN-CBR) has been proposed in [139] for classification problems. The authors in [140] have used CBR technique and Naive Bayes learner for the design and development of intelligent report system for forensic autopsy. Similarly, the authors in [141] have suggested an expert system, which combines the capabilities of both CBR and ANN for the prediction of diode qualification rate in industries. Studies reveal that CBR system has better generalization capability than the traditional classifiers due to the following reasons - (1). It explicitly uses the knowledge gained from previous disturbances for predicting the solution of a new problem. (2). The knowledge base can be continuously updated with the additional data acquired during learning. This increases the online learning capability, which is necessary for many real time applications.

As mentioned in Chapter 1, the machine learning techniques often have a low prediction accuracy and a high misclassification rate if the underlying information in the input data is not known. To overcome this drawback, Freund and Schapire in 1996 had first proposed an AdaBoost algorithm to effectively combine the learning ability of many weak classifiers in order to design a strong classifier. Initially, AdaBoost classifier has been used for two important biometric applications such as face detection [142–144] and facial expression recognition [145, 146]. The authors in [147] have proposed a novel cascaded AdaBoost classifier model for the classification of hyperspectral image data. An another model of cascaded AdaBoost classifiers have been proposed in [148] for the detection of vehicles. In [149], a hierarchical method based on AdaBoost classifiers has been proposed for the classification of surface images of marble slabs. In addition to biometric and pattern recognition applications, AdaBoost algorithm has also been utilized in other important applications such as traffic sign detection [150], short term wind prediction [151], intelligent transportation systems [152, 153], power quality assessment [154] and early warning scheme for transmission line galloping [155]. However, the application of AdaBoost algorithm to security assessment has not been explored so far. Review results indicate that AdaBoost algorithm can be a sig-

nificant tool for classification problems and hence, this classifier is utilized to enhance the monitoring and assessment of power system security.

4.2 Wavelet Support Vector Machine (WSVM)

In this section, WSVM proposed in [126] has been elaborated in detail. The translation invariant kernel or Morlet wavelet, which is used as a new mapping function in this classifier, replaces the traditional kernels used in SVM classifiers. The description about this classifier is given in the following subsections.

4.2.1 Support Vector Machine (SVM)

SVM is a supervised machine learning algorithm, which analyzes data for learning decision boundaries in pattern recognition problems [156]. A decision boundary is the one that separates the set of objects belonging to different class groups. It performs classification by first mapping the input data to multi dimensional feature space by some non-linear mapping. Then an optimal hyperplane is constructed which separates the mapped input data into two classes with maximum margin. The linear estimate function is defined as,

$$y = \omega^T \phi(x) + b, \quad \forall x \in R^N, y \in R \quad (4.1)$$

where, x is the input vector, R^N is the input space, y is the output and $\phi(x)$ is the non linear mapping. In order to construct an optimal hyperplane, SVM algorithm employs an iterative training process which is aimed at minimizing the following objective function as described below,

$$\min(F) = \frac{1}{2} \omega^T \omega + C \sum_{i=1}^N (\xi_i + \xi_i^*) \quad (4.2)$$

subject to constraints:

$$y_i - \omega \phi(x_i) - b \leq \varepsilon + \xi_i;$$

$$\omega \phi(x_i) + b - y_i \leq \varepsilon + \xi_i^*;$$

$$\xi_i, \xi_i^* \geq 0, \forall i = 1, 2, \dots, N$$

where, ω is the weight vector of the hyperplane, C is the penalty factor proportional to the amount of the constraint violation, ε is an insensitive loss function, ξ_i and ξ_i^* are the slack variables which represents parameters for handling non-separable input data, b is a threshold bias value and $\phi(x)$ is a mapping function called kernel function, which transforms the data from the input space to the feature space. The value of C should be chosen in a

manner to avoid overfitting as larger the value of C , more the error is penalized. The problem (4.2) is solved using Lagrange multiplier technique and the solution obtained leads to dual optimization problem as described below,

$$W(\alpha^{(*)}) = -\varepsilon \sum_{i=1}^l (\alpha_i^* + \alpha_i) + \sum_{i=1}^l (\alpha_i^* - \alpha_i) y_i - \frac{1}{2} \sum_{i=1}^l \sum_{j=1}^l (\alpha_i^* - \alpha_i)(\alpha_j^* - \alpha_j) K(x_i, x_j) \quad (4.3)$$

subject to:

$$\sum_{i=1}^l (\alpha_i^* - \alpha_i) = 0; \quad \alpha_i^* \in [0, C]$$

Thus, the resulting estimate function of SVM is linear, which is of the following form,

$$f(x) = \sum_{i=1}^N (\alpha_i^* - \alpha_i) K(x, x_i) + b \quad (4.4)$$

where, α_i and α_i^* are the non-negative Lagrange multipliers, $K(x, x_i)$ is the Support Vector (SV) kernel as it satisfies the Mercer's condition (ie), $K(x, x_i) = K(\langle x, x_i \rangle)$ [157].

This concept of kernel mapping makes the SVM algorithm to perform nonlinear classifications even with complex boundaries. There are many kernel mapping functions like linear, polynomial, quadratic, multi-layer perceptron and radial basis function. However, the radial basis function (gaussian) kernel has been widely used as the mapping function due to its capability of handling nonlinear relation existing between input data and the class labels. The gaussian kernel is defined as,

$$K(x, x') = \exp\left(\frac{-\|x - x'\|^2}{2\sigma^2}\right) \quad (4.5)$$

where, σ is the width of the gaussian kernel, which helps to find the influence area of the support vectors over the data space.

4.2.2 Wavelet Analysis

The basic principle of wavelet analysis is to express or approximate a signal or functions by a family of functions generated by dilations or translations of a mother wavelet function, $h(x)$ [126]. This function is expressed as follows,

$$h_{a,c}(x) = |a|^{-1/2} h\left(\frac{x-c}{a}\right) \quad (4.6)$$

where, a is a dilation factor, c is a translation factor and $h(x)$ is a mother wavelet which satisfies the following condition [158, 159],

$$W_h = \int_0^\infty \frac{|H(\omega)|^2}{|\omega|} d\omega < \infty \quad (4.7)$$

where, $H(\omega)$ is the Fourier transform of $h(x)$. The wavelet transform of a function $f(x)$ can be expressed as,

$$W_{a,c}(f) = \langle f(x), h_{a,c}(x) \rangle \quad (4.8)$$

where, $\langle \cdot, \cdot \rangle$ is the dot product, which also represents the decomposition of a function $f(x)$ on a wavelet basis $h_{a,c}(x)$. Thus, the function $f(x)$ can be reconstructed using the following equation,

$$f(x) = \frac{1}{W_h} \int_{-\infty}^{\infty} \int_0^{\infty} W_{a,c}(f) h_{a,c}(x) da/a^2 dc \quad (4.9)$$

Considering only finite terms for approximation [158], the above equation can be rewritten as,

$$\widehat{f}(x) = \prod_{i=1}^N h(x_i) \quad (4.10)$$

where, $\widehat{f}(x)$ is an approximated form of $f(x)$.

4.2.3 Wavelet SVM

A wavelet function can be represented in the following form [158] as shown below,

$$h(X) = \prod_{i=1}^N h(x_i) \quad (4.11)$$

where, $X = [x_1, \dots, x_N] \in R^N$. The wavelet kernel can be expressed as below,

$$K(x, x') = \prod_{i=1}^N h\left(\frac{x_i - c_i}{a}\right) h\left(\frac{x'_i - c'_i}{a}\right) \quad (4.12)$$

and the translation invariant wavelet kernels are obtained using [126],

$$K(x, x') = \prod_{i=1}^N h\left(\frac{x_i - x'_i}{a}\right) \quad (4.13)$$

A new mother wavelet function is constructed based on the wavelet function proposed in [160]. This is described as shown below,

$$h(x) = \cos(1.75x) \cdot \exp\left(-\frac{x^2}{2}\right) \quad (4.14)$$

Now, substitute (4.14) into (4.13) to obtain the wavelet kernel of this mother wavelet, which is defined below,

$$K(x, x') = \prod_{i=1}^N \left(\cos\left(1.75 \cdot \left(\frac{x_i - x'_i}{a}\right)\right) \exp\left(-\frac{\|x_i - x'_i\|^2}{2a^2}\right) \right) \quad (4.15)$$

which is an admissible SV kernel. The additional proof for this wavelet kernel can be found in [126]. Now substitute the above equation in (4.4) to obtain the WSVMs as,

$$f(x) = \sum_{i=1}^l (\alpha_i - \alpha_i^*) \prod_{j=1}^N h\left(\frac{x^j - x_i^j}{a_i}\right) + b \quad (4.16)$$

where, x_i^j denotes the j^{th} component of the i^{th} training pattern. The SVMs in the above equation are called WSVMs as they use wavelet functions as kernels.

4.3 Case Based Reasoning (CBR)

Case based reasoning is a problem solving artificial intelligence methodology that solves new cases by adapting previous successful solutions to similar problems. There may be many variations in the CBR working scheme depending on the applications and the features used. A scheme on the CBR working cycle proposed in [161] is shown in Figure 4.1. In

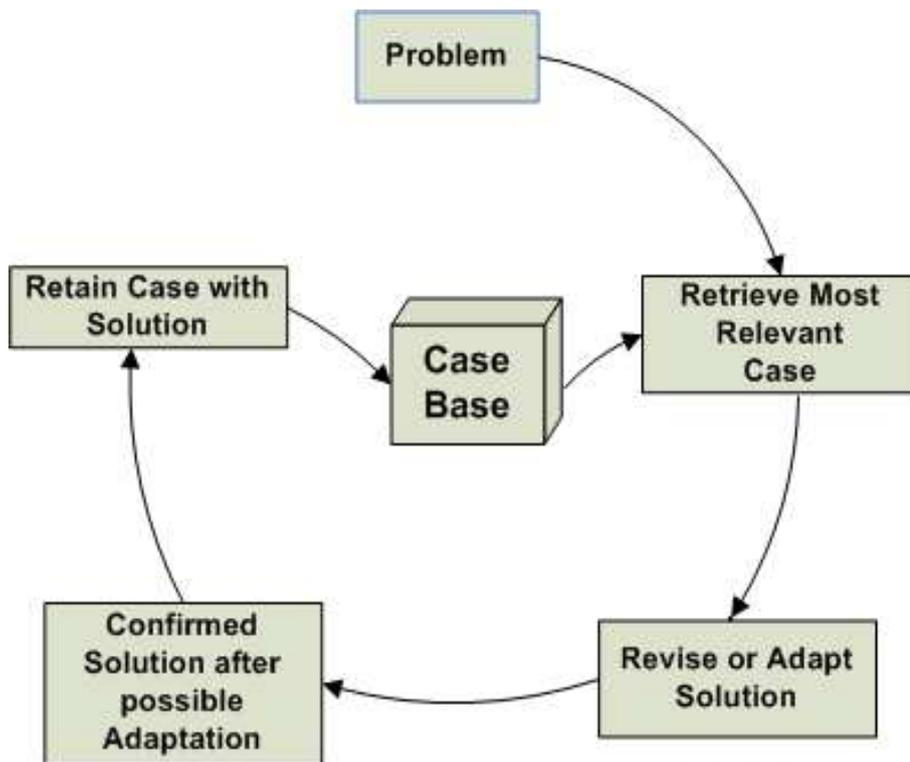


Figure 4.1: Schematic Diagram of CBR system

this CBR scheme, one or more cases are *retrieved* by matching a problem case against the cases from the case base. The solution suggested by the retrieved case is then *reused* or adapted according to the problems' description. If the retrieved case is not a similar match, then the solution will have to be *revised* (adapted) and evaluated for success. Finally, the case after successful evaluation is *retained* and the case base is updated. Existing CBR

systems use null adaptation where the solution of the retrieved case is directly assigned as the solution of the target problem [162]. However, the performance and the application of CBR systems can be improved significantly with the development of different case adaptation techniques [163]. Therefore, in this chapter, a novel case adaptation strategy based on fuzzy clustering thresholding technique is proposed to enhance the learning capability of CBR system for the proposed security assessment. The detailed steps involved in the design of CBR system are given in the following sub-sections.

4.3.1 Case Base Representation

The case base in the CBR system is the memory of all previously stored experiences or problems. The cases could be people, things, situations, diagnoses, designs or plans and objects. In many practical CBR applications, cases are usually represented as two unstructured sets of attributes viz. the problem and the solution feature [164]. However, all existing cases are not needed to be stored. In situations, where two or more cases are similar, then only one case may be stored.

4.3.2 Retrieval

For a given problem description, a retrieval algorithm should retrieve cases that are most similar to the problem currently presented to the CBR system. This retrieval mechanism usually works on the basis of indices and the organisation of the case memory, while searching the most similar cases for the current problem. There are many retrieval algorithms such as induction search, nearest neighbour search, serial search, hierarchical search, parallel search, etc. The most simple method of retrieval mechanism is the one-nearest neighbour search of the case base, which performs similarity matching on all the cases in the case base and returns just one best match [165]. This increases the computation time of the retrieval algorithm, particularly in the case of large case bases. Therefore, cases are usually pre-selected using k-NN search prior to similarity matching. In this work, k-NN search with similarity matching algorithm is used to retrieve the most similar case which can be potentially useful for solving the currently encountered problem. For a given test case, 2 samples from the case memory with the smallest Euclidean distance are identified as nearest neighbours. Euclidean distance ' d ' between the problem case ' q ' and a sample from the nearest neighbours ' p ' is

obtained using,

$$d_{pq} = \sqrt{\sum_{i=1}^n (q_i - p_i)^2} \quad (4.17)$$

where, n is the total number of features.

Among many methods available in the literature, a cosine matching function [166] has been used in this work for the measure of similarity among neighbours. This matching function has been widely used in information retrieval for matching the query with the documents in the database. It is a measure of similarity between two vectors of an inner product space that measures the cosine of the angle between them. Consider two vectors of attributes A and B , the cosine similarity, $\cos(\Theta)$ is obtained using a dot product and magnitude as,

$$\text{Similarity} = \cos(\Theta) = \frac{A \cdot B}{\|A\| \|B\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}} \quad (4.18)$$

where, A_i and B_i are the vector components of selected test case and its nearest neighbour respectively and n is the total number of features in a case. With the resulting similarity ranging from 0 to 1, a case with the highest similarity index among the group of neighbours is selected as the most similar feature for the selected test case. Hence, the class label of the neighbour case with less Euclidean distance and with highest similarity index is chosen as the appropriate class label for the selected test case.

4.3.3 Revise using Heuristics and Adaptation

The solution of the most similar case obtained using retrieval algorithm is assigned as the solution of the test case. However, this solution may not be an appropriate solution, if there are significant differences between the retrieved case and the given test case. In such situations, the solution obtained by the retrieval mechanism needs to be adapted to account for those differences. Adaptation usually finds the differences between the retrieved case and the present test case, and then applies a set of rules to account for those differences before suggesting a solution. In this work, a heuristic function as shown in (4.19) is formulated to find the solution for a given test case.

The function (f_j) for each training pattern is defined as the ratio of weighted sum of its features (Y_j) to the square root of its difference value (X). Mathematically,

$$f_j = \frac{Y_j}{\sqrt{X}}, \quad \forall j \in T \quad (4.19)$$

The value (Y_j) of a training pattern is defined as a product of the sum of all its features and

its corresponding weight (λ). The weight parameter (λ) is updated in each iteration. The difference value (X) is defined as the product of the number of nearest neighbours (k) and the sum of all elements of the difference vector. The difference vector is obtained by taking the difference between the elements of the j^{th} training pattern with the elements of the given test case.

$$Y_j = \lambda_j \sum_{i=1}^n p_{ji} \quad (4.20)$$

$$X = k \sum_{i=1}^n (p_{ji} - q_i) \quad (4.21)$$

where, p_j is the j^{th} training pattern, q is the given test case, n is the total number of features and T is the total input patterns available in the training set.

The pattern with the highest evaluation function is identified and its class label is selected as the predicted class label for the given test case. However, if the predictions obtained using both retrieval and heuristic methods are not similar, the solution obtained may not be an appropriate one and hence needs to be adapted. In such a case, the retrieved case is removed from the training set and the new case is retrieved for the given test case after updating the weights for the training patterns. This procedure is repeated until similar predictions are obtained using retrieval and heuristic methods. In case, if the solution obtained using both the predictions are similar, then the present test case with its class label is retained. This test case with its solution is then updated in the training set and considered for further assessment. This procedure is repeated for all samples available in the test case.

4.3.4 Updation of Weight Vector

The weights (λ) are initialized uniformly for all the input training patterns (T) using,

$$\lambda_j = \frac{1}{N}, \quad \forall j \in T \quad (4.22)$$

where, N is the total number of training patterns.

For successive iterations, weights are updated using fuzzy clustering thresholding method [167]. It is a histogram based thresholding method which has been predominately used in image processing. The histograms are constructed using Gaussian distribution by splitting the training data and its dataweights into different clusters based on their class labels. A threshold is determined corresponding to the minimum probability value between the two distributions. Then, a criterion function is formulated to identify the optimal threshold, which

also yields the class separation between the two distributions. The minimum error criterion proposed in [168] is used in this paper to select an optimal threshold.

The detailed steps involved in the updation of weights using this method is given below:

1. Split the training patterns and their corresponding weights into two clusters based on their class labels.
2. Construct histograms, \mathbf{h}^1 and \mathbf{h}^2 of size $(t \times n)$ for each cluster respectively where, 't' is the total number of threshold steps (here, $t=10$) and 'n' is the total number of features.
3. Form two error matrices, \mathbf{M}^1 and \mathbf{M}^2 using the histogram data such that,

$$\mathbf{M}^1 = \mathbf{h}^1 + \mathbf{h}^2$$

and,

$$\mathbf{M}^2 = \sum_{i=1}^N (\lambda_i) \mathbf{U} - \mathbf{M}^1$$

where, ' \mathbf{U} ' is the unity matrix of size $(t \times n)$ and ' \mathbf{N} ' is the total number of training patterns.

4. Form vectors, \mathbf{V}^1 and \mathbf{V}^2 with minimum error values of matrices \mathbf{M}^1 and \mathbf{M}^2 respectively using,

$$\mathbf{V}^1 = [m_1^1 \ m_2^1 \ m_3^1 \ \dots \ m_n^1]$$

and,

$$\mathbf{V}^2 = [m_1^2 \ m_2^2 \ m_3^2 \ \dots \ m_n^2]$$

where, $m_i^1 = \min(\mathbf{M}^1(1:t, i))$ and $m_i^2 = \min(\mathbf{M}^2(1:t, i))$, $\forall i = 1, 2, 3, \dots, n$. Also, form vectors, \mathbf{T}^1 and \mathbf{T}^2 with threshold values corresponding to these minimum values such that,

$$\mathbf{T}^1 = [k_1^1 \ k_2^1 \ k_3^1 \ \dots \ k_n^1]$$

and,

$$\mathbf{T}^2 = [k_1^2 \ k_2^2 \ k_3^2 \ \dots \ k_n^2]$$

where, k_i^1 and k_i^2 are the row indices corresponding to the minimum value of the i^{th} feature of matrices \mathbf{M}^1 and \mathbf{M}^2 respectively.

5. Form matrices, \mathbf{Z}^1 and \mathbf{Z}^2 whose elements are obtained using,

$$\mathbf{Z}^1 = [\mathbf{E}^1 \ \mathbf{I}^1 \ \mathbf{C}^1 \ \mathbf{F}^1]$$

and

$$\mathbf{Z}^2 = [\mathbf{E}^2 \ \mathbf{I}^2 \ \mathbf{C}^2 \ \mathbf{F}^2]$$

where, vectors $\mathbf{E}^1 = [(\mathbf{V}^1)]^T$; $\mathbf{E}^2 = [(\mathbf{V}^2)]^T$ and vectors $\mathbf{I}^1 = [(\mathbf{T}^1)]^T$; $\mathbf{I}^2 = [(\mathbf{T}^2)]^T$.

And, class label vectors of clusters I and II are $\mathbf{C}^1 = [(\mathbf{CL}^1)]^T$ and $\mathbf{C}^2 = [(\mathbf{CL}^2)]^T$, where, $CL_i^1 = 1$ and $CL_i^2 = 0$, $\forall i = 1, 2, 3, \dots, n..$ Similarly, feature vector of clusters I and II are $\mathbf{F}^1 = [1 \ 2 \ 3 \ \dots \ n]^T$ and $\mathbf{F}^2 = [1 \ 2 \ 3 \ \dots \ n]^T$.

6. Form vectors, \mathbf{N}^1 and \mathbf{N}^2 with minimum error values of matrices \mathbf{Z}^1 and \mathbf{Z}^2 respectively such that,

$$\mathbf{N}^1 = [e^1 \ i^1 \ c^1 \ f^1]$$

and

$$\mathbf{N}^2 = [e^2 \ i^2 \ c^2 \ f^2]$$

where, error values, e^1 and e^2 are determined using, $e^1 = \min(\mathbf{Z}^1(1 : n, 1))$ and $e^2 = \min(\mathbf{Z}^2(1 : n, 1))$.

And,

$$i^1 = \mathbf{I}^1(l); \ c^1 = \mathbf{C}^1(l); \ \text{and} \ f^1 = \mathbf{F}^1(l)$$

and,

$$i^2 = \mathbf{I}^2(p); \ c^2 = \mathbf{C}^2(p); \ \text{and} \ f^2 = \mathbf{F}^2(p)$$

where, 'l' and 'p' are the row indices corresponding to the error values e^1 and e^2 respectively.

7. Concatenate vectors, \mathbf{N}^1 and \mathbf{N}^2 to form a matrix \mathbf{F} such that,

$$\mathbf{F} = \begin{bmatrix} e^1 & i^1 & c^1 & f^1 \\ e^2 & i^2 & c^2 & f^2 \end{bmatrix}$$

8. Form a minimum error vector, \mathbf{E}_m whose elements are obtained using,

$$E_m = [e_m \ i_m \ c_m \ f_m],$$

where, minimum error value, $e_m = \min(\mathbf{F}(1 : 2, 1))$ and 'm' is the row index corresponding to this minimum error value, e_m ; threshold index, $i_m = \mathbf{F}(m, 2)$; label index, $c_m = \mathbf{F}(m, 3)$; and feature index, $f_m = \mathbf{F}(m, 4)$.

9. Form two vectors, \mathbf{R}_{\min} and \mathbf{R}_{\max} by finding the minimum and maximum values of each feature in the training patterns, \mathbf{T}_r viz.,

$$\mathbf{R}_{\min} = [a_1 \ a_2 \ a_3 \ \dots \ a_n]$$

and

$$\mathbf{R}_{\max} = [b_1 \ b_2 \ b_3 \ \dots \ b_n],$$

where, $a_i = \min(\mathbf{T}_r(1 : N, i))$; $b_i = \max(\mathbf{T}_r(1 : N, i))$, $\forall i = 1, 2, 3, \dots, n$ and 'N' is the total number of training patterns.

10. Construct a linearly spaced threshold vector, \mathbf{T}_v using the boundary conditions such that,

$$\mathbf{T}_v = [mind \dots\dots maxd]_{1 \times t},$$

where, $mind = \mathbf{R}_{\min}(f_m)$ and $maxd = \mathbf{R}_{\max}(f_m)$ and the spacing between successive elements are obtained using $(maxd - mind)/(t - 1)$.

11. An optimal threshold value, t_o is identified from the threshold vector, \mathbf{T}_v using, $t_o = \mathbf{T}_v(i_m)$, where, ' i_m ' is the threshold index obtained corresponding to the minimum error value, e_m .

12. Form a vector, \mathbf{S} whose elements are obtained using, $\mathbf{S}_{j \times 1} = [\mathbf{T}_r]_{j \times p}$, $\forall j \in N$ and $p = f_m$.

13. Finally, classify the training patterns based on the following conditions,

$$\text{if } c_m = 1, \text{ then } \mu_j = \begin{cases} 1, & \text{if } \mathbf{S}_{j \times 1} \geq t_o \\ 0, & \text{otherwise} \end{cases}$$

$$\text{if } c_m = 0, \text{ then } \mu_j = \begin{cases} 1, & \text{if } \mathbf{S}_{j \times 1} < t_o \\ 0, & \text{otherwise} \end{cases}$$

where, ' μ_j ' is the predicted class label for the j^{th} training pattern.

Thus, an optimal threshold (t_o) with minimum error (e_m), which divides the training patterns into two classes is calculated.

The classification error (α) is calculated for each iteration using the following equation,

$$\alpha = \frac{1}{2} \log\left(\frac{1 - e_m}{e_m}\right) \quad (4.23)$$

And, the weight of all the training patterns is updated for each iteration using,

$$\lambda_j^{new} = \frac{\lambda_j^{old} \exp(-\alpha C_j \mu_j)}{\sum_j^N (\lambda_j^{old} \exp(-\alpha C_j \mu_j))}, \quad \forall j \in T \quad (4.24)$$

where, C_j and μ_j are the original and predicted class labels of the j^{th} training pattern respectively; λ_j^{old} and λ_j^{new} are the weights of the j^{th} training pattern before and after weight updation respectively. For better understanding of this algorithm, an example is given in Appendix A.

4.4 AdaBoost Classifier with SVM as weak Classifier

The AdaBoost algorithm is used to construct a strong classifier by combining the group of weak classifiers. It has been employed for classification problems as the rate of misclassification can be significantly reduced with the increase in number of weak classifiers [142]. The algorithm considers training patterns as inputs $(\vec{x}_1, y_1), \dots, (\vec{x}_m, y_m)$, where each \vec{x}_i is an input pattern vector with d selected features and each label $y_i \in \{0, 1\}$. The AdaBoost algorithm executes a classifier ' T ' times. After repeated analysis, it is found that the proposed approach led to better results with $T = 10$ and also does not lead to overfitting. The weights of the j^{th} training data is represented by λ_j^b , where b is the iteration count of the weak classifiers. Initially, all the data weights are considered as equal ($\lambda_j^b = 1/N$), where N is the number of training patterns. At the end of each iteration, the hypothesis of the weak classifier, $h_t : \{\vec{x}_1, \dots, \vec{x}_m\} \Rightarrow \{0, 1\}$ is calculated. Finally, the calculated hypothesis is evaluated using the value α^b , where α^b is the reliability of classification by the weak classifier at the b^{th} iteration. After selecting a suitable hypothesis h_t , the weights of the misclassified patterns are increased for the next iteration. This procedure is repeated until a strong classifier as a weighted combination of ' T ' weak classifiers is produced. A logical representation of the AdaBoost algorithm is shown in Figure 4.2. Here, h_t^i represents the hypothesis of the i^{th} weak classifier, which consists of class label of the testing data obtained using (4.28). Similarly, H_t is the hypothesis of the strong classifier, which is obtained as the linear combination of ' T ' weak classifiers. At the end of ' T ' iterations, H_t consists of the final class label of the testing data, which is estimated using (4.32). A brief description about the weak classifier and the boosting algorithm is given in the following subsections.

4.4.1 Weak Classifier

Machine learning algorithms such as k-nearest neighbours, ANN, SVM and DTs can be used as weak classifiers. The authors in [169] have demonstrated the superiority of the SVM algorithm than the ANN based methods for classification problems. This has led to the thought of devising a more efficient tool for training procedure. Therefore, in this chapter, SVM based pattern recognition approach is considered as a weak classifier. It is a widely used pattern recognition approach for both classification and regression problems. In classification process, it determines the decision boundary between two classes, which is far away from any data point in the training set. Initially, the use of SVM has been limited only for two class

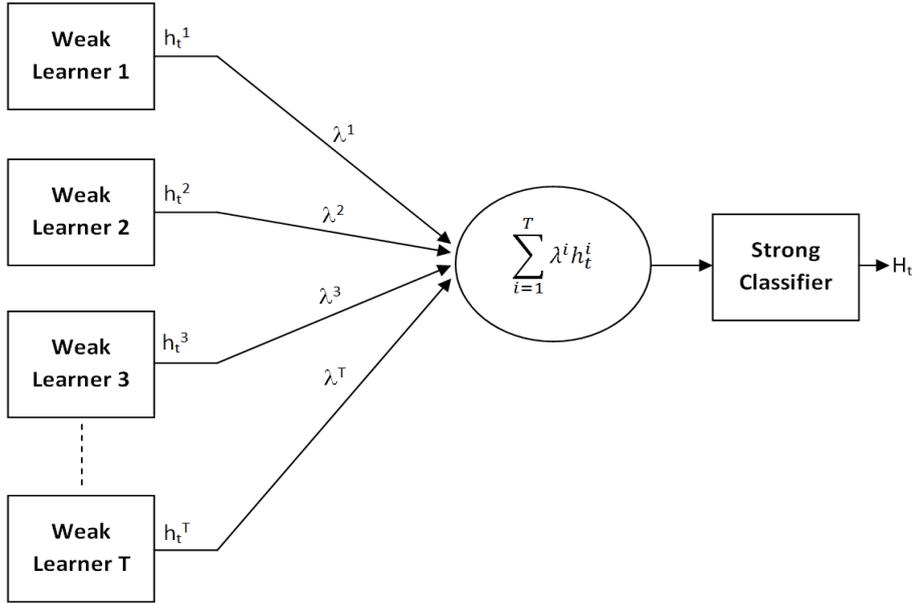


Figure 4.2: Architecture of AdaBoost Algorithm

data sets that are separable by a linear classifier. In 1992, Vapnik et.al., have introduced the concept of kernel mapping, which makes the SVM classifier to perform non-linear classifications even with complex boundaries. Among many kernel mapping functions, radial basis function (gaussian) kernel is the most widely used kernel due to its better capability of handling non-linear data. The detailed explanations about this classifier has been presented in section 4.2.1.

4.4.2 AdaBoosting Algorithm

The detailed steps involved in the design of strong classifier using AdaBoost algorithm are given below.

1. Initialize the number of weak classifiers, T .
2. Set the iteration count, $b=1$.
3. Assign uniform weights for all the training patterns using,

$$\lambda_j^0 = \frac{1}{N}, \quad \forall j \in N \quad (4.25)$$

where, λ_j is the weight assigned to the j^{th} training pattern and N is the total number of training patterns.

4. Train the classifier T (*here, $T = b$*) and predict the security status of the training patterns considering the training set as the testing data.

5. Form a classification probability vector using the training data and its corresponding weights. The elements of this vector at the b^{th} iteration are obtained using,

$$PC_j^b = PC_j^m + \lambda_j^m * E_j^b, \quad \forall j \in N \quad (4.26)$$

where, E_j^b is the estimated class label of the j^{th} training pattern at b^{th} iteration, λ_j^m is the weight of the j^{th} training pattern at the previous iteration. Here, $m = b - 1$ and for initial search (ie. $b=1$), the elements of the class probability vector, PC^m are assumed to be zero.

6. Estimate the security status of the training patterns by assigning patterns corresponding to positive probability to secure class (*class '1'*) and patterns corresponding to negative probability to insecure class (*class '0'*).

$$Y_j = \begin{cases} 1, & \text{if } PC_j^b > 0 \\ 0, & \text{if } PC_j^b < 0 \end{cases} \quad (4.27)$$

7. Find the reliability of the classifier T at the end of b^{th} iteration using,

$$\alpha^b = \frac{1}{2} \log\left(\frac{1 - e_m}{e_m}\right) \quad (4.28)$$

where, e_m is the minimum error obtained using the fuzzy clustering thresholding and minimum error criterion methods (Refer section 4.3.4).

8. The weights of the training patterns at the end of b^{th} iteration are updated using,

$$\lambda_j^b = \frac{\lambda_j^m \exp(-\alpha^b C_j Y_j^b)}{\sum_{j=1}^N (\lambda_j^m \exp(-\alpha^b C_j Y_j^b))}, \quad \forall j \in N \quad (4.29)$$

where, C_j is the original class label of the j^{th} training pattern, Y_j is the predicted class label of the j^{th} training pattern, λ_j^m and λ_j^b are the weights of the j^{th} training pattern before and after the b^{th} iteration respectively.

9. If $b = T$, then go to step 10 else, increment the iteration count as, $b=b+1$ and repeat from step 4.
10. After the learning process is completed, predict the security status of the testing patterns by each of the weak classifiers considered for training purpose.

11. Set the iteration count, $bp=1$.
12. Form a classification probability vector again, whose elements, PC^b at the b^{th} iteration are obtained using,

$$PC_j^{bp} = PC_j^m + \alpha^{bp} * E_j^{bp}, \quad \forall j \in T_e \quad (4.30)$$

where, E_j^{bp} is the predicted class label of the j^{th} testing pattern at bp^{th} iteration, α^b is the reliability of the classifier T and T_e is the total testing patterns.

13. If $bp = T$, then go to step 14 else, increment $bp = bp + 1$ and repeat from step 12. Thus, the final classification probability vector obtained after ' T ' iterations resembles the classification probability of a strong classifier.
14. Finally, estimate the security status of the testing patterns using the classification probability vector as shown below,

$$Y_j = \begin{cases} \text{Secure or Class 1,} & \text{if } PC_j^{bp} > 0 \\ \text{Insecure or Class 0,} & \text{if } PC_j^{bp} < 0 \end{cases} \quad (4.31)$$

4.5 Conclusions

This chapter illustrates the design of intelligent classifiers such as WSVM, CBR and AdaBoost algorithm for the security assessment and monitoring of power systems. This work uses Morlet wavelet as a new kernel mapping function for the design of WSVM for the proposed security assessment. Literature studies revealed that WSVM exhibits high performance accuracy for classification problems than the other kernel based SVM classifiers like l-SVM, q-SVM, p-SVM, m-SVM and r-SVM. Further studies revealed that both CBR and AdaBoost classifiers have also been successfully employed for different classification problems. In order to enhance the generalization capability of these two classifiers, a novel weight updation strategy using fuzzy clustering thresholding technique is proposed.

Chapter 5

Static Security Assessment using Different Machine Learning Techniques

5.1 Introduction

Monitoring of system security is very crucial for a safe and reliable operation of the power system. Security assessment is usually conducted to evaluate the robustness of the system to severe contingencies such as transmission line outage or short circuit faults. During such situations, detection of post-contingency problems in a faster manner is of utmost importance. A system is said to be secure if its operating criteria before and after contingency conditions are within the threshold limits. This implies that security analysis must be performed considering both the constraints viz. thermal constraints (branch line flows) and electrical constraints (bus voltage values) to ensure the static security of power systems.

The traditional approach for security assessment is based on the data provided by Supervisory Control And Data Acquisition (SCADA) systems. But, they typically take 2-10 seconds for providing such measurements across the entire power system. Moreover, the power system parameters changes continuously due to the dynamic nature of loads connected to it. Therefore, the security assessment studies conducted using these measurements may become unrealistic in real time [170]. This may result in significant error in state estimation results. On the other hand, PMUs which provide fast and accurate real time measurements, help in obtaining updated information of the system being monitored at a particular time. Therefore, in recent years, PMUs are widely employed for monitoring and control of power systems.

In the past years, security assessment is usually performed by computing the security

indices through load flow solution, following a disturbance. However, this method is computationally expensive and hence, cannot be used for online security assessment. To overcome this drawback, machine learning techniques have been employed, which make the security assessment computationally more efficient and reliable. Some of these techniques, which have been predominately employed are Artificial Neural Networks (ANNs), Support Vector Machines (SVMs) and Decision Trees (DTs). The authors in [171, 172] have applied DTs to evaluate power system security assessment. But, the use of statistical tools in DTs can often lead to poor classification results [125]. Although ANNs have been considered as a successful tool for security assessment, they are extremely time consuming and require large amount of training data. Therefore, these methods are not suitable for online assessment [173]. Since SVM based pattern recognition approach is found to be effective in handling non-linear classification problems, it has been applied in [174, 175] for power system security assessment and classification. However, its performance is mainly dependent on the choice of kernel and the selection of kernel parameters needs a thorough investigation.

In this chapter, a suitable monitoring framework for static security assessment has been proposed. This framework can predict security status of the system and the violations in terms of either line overload/voltage violation or both. Different machine learning techniques like WSVM, CBR and AdaBoost algorithm described in Chapter 4, have been applied for security assessment. The effectiveness of the proposed Static Security Assessment (SSA) method has been demonstrated on IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus systems and their SSA results are compared with the results obtained using SVM, ANN and k-Nearest Neighbour (kNN) methods.

5.2 Proposed Static Security Index

Security indices, which are usually represented by the out-of-limit voltage or line overload values due to a particular contingency, can be helpful in evaluating the static security of the power system. It also helps the operators to assess the critical information about vulnerability of the power system components and the entire power system. The security indices reported in the literature suffers from masking problem and weighting factor allocation to the power system components. Masking problem is overcome by using higher order performance indices. The weighting factor allocation is a difficult task as different weights has to be considered for different elements based on their importance and power system prac-

tice [176]. In this chapter, a composite Security Index (SI) consisting of both line overload (*LOV*) and bus voltage limit (*VV*) violation vectors is proposed to completely eliminate the masking problem and also the difficult task of weights selection. Mathematically, it is defined as,

$$SI = \left(\frac{VV + LOV}{100} \right)^{(1/2m)} \quad (5.1)$$

where, the value of 'm' is chosen as 2.

The limit violation vectors can be obtained using (5.2) and (5.3),

$$LOV = \begin{cases} \sum_l^{nl} \left(\frac{S_l - S_l^{max}}{\Delta S_l} \right), & \text{if line } l \text{ is overloaded} \\ 0, & \text{Otherwise} \end{cases} \quad (5.2)$$

$$VV = \begin{cases} \sum_i^{nb} \left(\left(\frac{V_i - V_i^{max}}{\Delta V_i^{max}} \right) + \left(\frac{V_i - V_i^{min}}{\Delta V_i^{min}} \right) \right), & \text{if } V_i^{min} > V_i > V_i^{max} \\ 0, & \text{if } V_i^{min} \leq V_i \leq V_i^{max} \end{cases} \quad (5.3)$$

and,

$$\Delta V_i^{max} = V_i^{max} - 1.0 \quad (5.4)$$

$$\Delta S_l = S_l^{max} - S_l^{Admissible} \quad (5.5)$$

$$\Delta V_i^{min} = V_i^{min} - 1.0 \quad (5.6)$$

$$\Delta S_l^{Admissible} = S_l^{max} - 10\% S_l^{max} \quad (5.7)$$

where, *nl* and *nb* are total number of transmission lines and system buses respectively; S_l and S_l^{max} are MVA flow and maximum MVA limit on branch '*l*' respectively; V_i , V_i^{min} and V_i^{max} are bus voltage magnitude, minimum and maximum voltage limits of the *i*th bus respectively.

5.3 Proposed Framework of SSA

Many approaches have been proposed in recent years for power system security assessment and classification using some intelligent classifiers. However, there has been no significant work reported so far that focuses on the prediction of type of violations (either bus voltage/line overload violation or both) causing insecurity. A suitable framework has been developed to effectively monitor system security status as well as type of violations causing insecurity. Performance of machine learning based security assessment is mainly dependent on input data generation and the suitable classifier design.

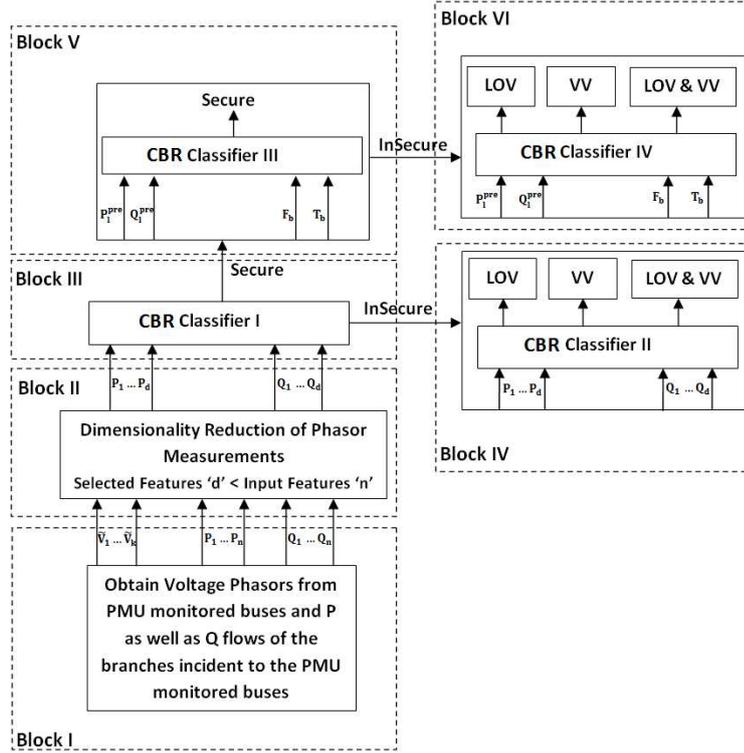


Figure 5.1: Detailed Framework of Static Security Assessment

5.3.1 Design of Monitoring and Security Assessment System

The framework of monitoring and security assessment of power systems using classifiers is shown in Figure 5.1. A large number of data patterns are generated by varying the load randomly at all the buses. The synchronized measurements, which are obtained from the PMUs installed in the system, form the components of the input pattern vector (Block I). These measurements include voltage phasors (\bar{V} and δ) of the buses monitored by PMUs and the power flows (P and Q) of the branches observed by PMUs. In order to reduce the dimensionality of the input features (n) and the training time of the classifier, only relevant features (d), which are obtained using the feature selection technique are considered for the training purpose (Block II). After detailed investigations, it has been found that only real and reactive power flows obtained through the PMUs are identified as relevant features by the feature selection technique. Hence, only these selected features are provided as inputs to the classifiers I and II. Then, the classifier I once trained, predicts the static security status of the system (Block III). In case of any insecure patterns identified by the classifier I, the real and reactive power flows in those insecure patterns are provided as inputs to the classifier II. Then, the classifier II predicts the type of violations in terms of line overload/voltage violation or both in those insecure patterns (Block IV). However, if the system is found to

be secure, then the security of that particular operating condition is assessed with respect to its next contingency using classifier III (Block V). In other words, the classifier III is used to predict the security status of the particular operating condition with respect to all probable N-1 contingencies. For this analysis, the contingency location and its pre-contingent power flows are provided as inputs to the classifiers III and IV. After training, the classifier III can accurately predict the security status of that loading condition with respect to its probable contingency list and the classifier IV predicts the type of violation in terms of line overload/voltage violation or both in those insecure patterns identified by the classifier III (Block VI).

5.3.2 Input Data Generation

The input data base consisting of training and testing sets can be generated by either real time occurrences or through offline simulations. In this chapter, sufficient amount of patterns were generated through offline simulations. This simulation is carried out considering different operating conditions by randomly varying the load at all the buses between 50% and 200% of their base case value. For each operating condition, the steady state variables such as bus voltage magnitudes, bus voltage angles, line currents and power flows which are obtained through load flow solver are considered as synchronized measurements. It is well known that PMUs measure only the voltage phasor of the PMU buses and the current flow through the branches connected to these buses. However, there are some indirect measurements such as the outgoing real and reactive power flows from PMU buses, which can also be easily computed using the bus voltage phasor information obtained from the PMUs. Therefore, both the direct and indirect phasor measurements are considered as input parameters for the proposed static security assessment. The training and testing patterns are then formed separately from the total generated data patterns. Finally, the static security index, as defined in (5.1), is evaluated for each training pattern and is labeled as either secure ($SI = 0$) or insecure ($SI > 0$).

5.3.3 Dimensionality Reduction of Phasor Measurements

The number of available phasor measurements increases with the increase in size of the system. However, all the phasor measurements may not provide useful information required for classification and will increase the complexity as well as the training time of the classifier. Therefore, it is necessary to select only the appropriate features which can provide more

discriminative information for classification problems. In this chapter, a statistical approach based on class separability and correlation coefficient methods [177] have been used to select the appropriate variables for security assessment and classification. The index, F_i which is used for the measure of its class separability with respect to the i^{th} variable is shown below,

$$F_i = \frac{m_i^{(S)} - m_i^{(I)}}{\sigma_i^{(S)2} + \sigma_i^{(I)2}}, \quad \forall i, j \in n \quad (5.8)$$

$$m_i^{(S)} = \frac{1}{N^{(S)}} \sum_{j=1}^{N^{(S)}} x_{ij}^{(S)} \quad (5.9)$$

$$m_i^{(I)} = \frac{1}{N^{(I)}} \sum_{j=1}^{N^{(I)}} x_{ij}^{(I)} \quad (5.10)$$

$$\sigma_i^{(S)2} = \frac{1}{N^{(S)}} \sum_{j=1}^{N^{(S)}} (x_{ij}^{(S)} - m_i^{(S)})^2 \quad (5.11)$$

$$\sigma_i^{(I)2} = \frac{1}{N^{(I)}} \sum_{j=1}^{N^{(I)}} (x_{ij}^{(I)} - m_i^{(I)})^2 \quad (5.12)$$

where, $m_i^{(S)}$ and $m_i^{(I)}$ are the mean values of i^{th} variable corresponding to secure and insecure classes respectively, $\sigma_i^{(S)2}$ and $\sigma_i^{(I)2}$ are the variances of i^{th} variable corresponding to secure and insecure classes respectively, $N^{(S)}$ and $N^{(I)}$ are the number of secure and insecure patterns in the training set respectively, N and n are the total number of training patterns and total number of variables in a training pattern respectively.

However, the variables chosen based on this measure may not provide complete information about the correlation among the other variables. Hence, both the F measure and correlation information have been used for the selection of attributes for the proposed SSA. The correlation coefficient between the i^{th} and j^{th} variable can be calculated using the following equations,

$$C_{ij} = \frac{E(x_i x_j) - E(x_i)E(x_j)}{\sigma_i \sigma_j}, \quad \forall i, j \in n \quad (5.13)$$

and,

$$E(x_i x_j) = \frac{1}{N} \sum_{k=1}^N x_{ik} x_{jk} \quad (5.14)$$

$$E(x_i) = \frac{1}{N} \sum_{k=1}^N x_{ik} \quad (5.15)$$

$$E(x_j) = \frac{1}{N} \sum_{k=1}^N x_{jk} \quad (5.16)$$

$$\sigma_i^2 = \frac{1}{N} \sum_{k=1}^N (x_{ik} - E(x_i))^2 \quad (5.17)$$

$$\sigma_j^2 = \frac{1}{N} \sum_{k=1}^N (x_{jk} - E(x_j))^2 \quad (5.18)$$

The detailed steps involved in the selection of input variables using class separability and

correlation coefficient methods is illustrated below.

1. Determine the ' F' ' index of each variable with respect to other variables using (5.8)-(5.12).
2. Rank the variables in the descending order according to the calculated ' F' ' index.
3. Set a threshold value ' t ' of correlation coefficient (here, $t=0.85$).
4. Initially, consider a variable whose ' F' ' index is highest.
5. Find the correlation coefficient of this variable with respect to other variables using (5.13)-(5.18).
6. Those variables, whose correlation coefficient is less than the threshold value (t) are selected as the appropriate variables.
7. Select the variable which is having the next higher ' F' ' index ranking and repeat from step 5.

This procedure is repeated in a sequential manner for all the variables available in the training pattern. Finally, the variables which contains more information about the class separability and less correlated among the other variables are selected as the relevant features.

5.3.4 Synthetic Minority Oversampling Technique (SMOTE)

Class imbalance is a result of class distribution in which the insecure class are considerably more abundant than the secure class samples. In such situations, the performance of machine learning techniques is highly biased towards the majority class. Usually, random sampling methods viz. undersampling and oversampling are utilized to overcome this class imbalance problem. Undersampling is a method of producing the class balanced training set of smaller size, while simple oversampling is used to increase the amount of minority class samples [178]. However, these sampling methods suffer from overfitting as the same data is repeatedly used for sampling. To overcome this drawback, a Synthetic Minority Oversampling Technique (SMOTE) [179] has been utilized in this work to generate synthetic samples from the minority class samples. The synthetic data samples are generated by combining the minority class sample with its nearest neighbour sample. Considering a minority sample ' q ' with ' k ' neighbours, a SMOTE sample can be generated using,

$$S_i = q_i + u * d_{pq}, \quad \forall i \in n \quad (5.19)$$

In (5.19), the value of 'u' is a random number in the interval [0, 1] for all the variables; d'_{pq} is the Euclidean distance between the minority class sample 'q' and its nearest neighbour sample 'p'; 'p' is a sample randomly selected from the list of 'k' neighbours. The Euclidean distance d'_{pq} is calculated using,

$$d_{pq} = \sqrt{\sum_{i=1}^n (q_i - p_i)^2} \quad (5.20)$$

where n is the total number of variables in a sample.

This procedure of generation of synthetic samples ensures that generated SMOTE sample lies on the line segment joining two original samples used to generate it. An illustration about the generation of synthetic data using SMOTE is shown in Figure 5.2.

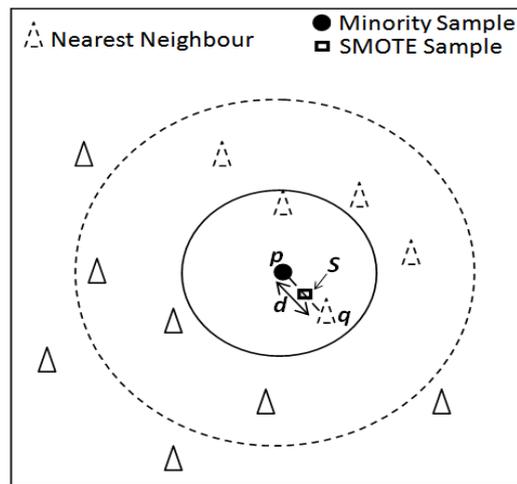


Figure 5.2: Illustration of SMOTE Sample Generation

5.4 Case Studies & Discussions

The effectiveness of the proposed approach has been demonstrated on IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus networks. The minimum and maximum value of voltage magnitude at each bus is considered as 0.9 pu and 1.10 pu respectively. The maximum value of MVA flow across branches is taken as 130% of their base case MVA flow. The input pattern vector consists of synchronized measurements, which are obtained from PMUs installed at locations obtained in Chapter 2 considering normal operation.

5.4.1 Details of Input Data

The details on the number of single line contingencies considered, the number of PMUs and the number of branches measured for the three test systems are shown in Table 5.1 The steady

Table 5.1: Details of the Three Test Systems

Test Systems	IEEE 14 bus	IEEE 30 Bus	Indian 246 Bus
Number of branches	20	41	376
Number of PMUs	3	7	57
Number of contingencies	18	33	339
Number of branches measured	12	24	226
Number of features available	30	62	566
Number of features selected	5	6	96
Dimensionality reduction	83.33 %	90.32 %	80.04 %

state measurements viz., voltage magnitude as well as voltage angle of the PMU buses and the current and power flows of the branches obtained using the PMUs, form the components of the input pattern vector. To reduce the number of features, a detailed analysis using the class separability and correlation coefficient methods has been carried out as mentioned in the earlier section 5.3.3. After calculating the class separability index of all variables, the correlation of each variable with respect to the other variables is also calculated. Finally, only those variables which are less correlated among the other variables and have higher class separability index (or F') are selected as the input features.

Table 5.2 lists the values of F' index calculated for all the 42 variables obtained using PMUs for an IEEE 14 bus system. After detailed investigations, it has been found that only 5 variables (variables 29, 31, 32, 36 and 42) out of 42 variables satisfy the above criterion. Therefore, only these 5 variables are considered as the relevant features for an IEEE 14 bus system. Here, the variables 29, 31, 32, 36 and 42 represent the real power flow on branch 9-10, reactive power flows on branches 1-2, 2-3, 5-6 and 9-14 respectively. Similar analysis has also been carried out on IEEE 30 bus and Indian 246 bus systems. Their results also reveal that only few branch real and reactive power flows obtained using PMUs have less correlation with variables having higher F' index. Hence, only those real and reactive power flows (obtained using the PMUs), which are identified by this technique are provided as inputs to the classifiers I and II. This greatly reduces the dimension of the input training pattern, thereby making the classification task more efficient and reliable. Out of 1000 data patterns, which are generated by varying the load randomly at all the buses, 80% of them are chosen as training set and the remaining 20% as testing set.

Table 5.2: All 42 Variables and their 'F' Indices of IEEE 14 Bus System

Rank	Variable Number	Variable Name	Index F	Rank	Variable Number	Variable Name	Index F	Rank	Variable Number	Variable Name	Index F
1	42	Q9-14	240.21	15	2	V6	78.00	29	6	δ 9	21.36
2	29	P9-10	223.87	16	25	P6-11	74.68	30	22	P2-5	18.18
3	1	V2	180.25	17	4	δ 2	58.43	31	10	I2-5	17.26
4	38	Q6-12	180.06	18	39	Q6-13	55.25	32	24	P5-6	15.04
5	35	Q4-9	169.65	19	37	Q6-11	55.02	33	21	P2-4	13.20
6	17	I9-10	168.96	20	23	P4-9	52.55	34	12	I5-6	12.88
7	41	Q9-10	130.79	21	13	I6-11	45.70	35	9	I2-4	12.58
8	33	Q2-4	111.11	22	11	I4-9	45.58	36	31	Q1-2	11.57
9	34	Q2-5	106.84	23	40	Q7-9	43.84	37	32	Q2-3	9.08
10	3	V9	101.72	24	27	P6-13	37.43	38	20	P2-3	9.05
11	30	P9-14	96.71	25	15	I6-13	31.63	39	8	I2-3	8.79
12	26	P6-12	86.23	26	28	P7-9	28.77	40	7	I1-2	3.50
13	18	I9-14	83.60	27	16	I7-9	22.02	41	19	P1-2	3.34
14	14	I6-12	79.13	28	5	δ 6	21.77	42	36	Q5-6	2.21

V, δ - Voltage magnitude and Phase angle of the PMU buses; I, P, Q - Current, Real and Reactive power flows of the branches measured by the PMUs.

Table 5.3: Details of Data Generation for Classifiers I and III

Test Systems	Classifier I			Classifier III		
	P_{Total}	P_{Secure}	$P_{Insecure}$	P_{Total}	P_{Secure}	$P_{Insecure}$
IEEE 14-bus	1000	369	631	6642	3521	3121
IEEE 30-bus	1000	182	818	6006	9	5997
Indian 246-bus	1000	263	737	24722	21755	2967

P_{Total} - Total Number of Patterns, P_{Secure} - Number of patterns belonging to secure class, $P_{Insecure}$ - Number of patterns belonging to insecure class.

Table 5.3 lists the details of the data generation for classifiers I and III. The number of data patterns belonging to secure and insecure class are also listed in this table. Table 5.4 gives the details regarding the number of training and testing patterns generated for classifiers I and II and similarly, the information regarding the training and testing patterns for classifiers III and IV are given in Table 5.5.

Table 5.4: Details of Training and Testing Data for Classifiers I and II

Test Systems	Classifier I			Classifier II		
	P_{Total}	P_{Train}	P_{Test}	P_{Total}	P_{Train}	P_{Test}
IEEE 14-bus	1000	800	200	631	505	126
IEEE 30-bus	1000	800	200	818	654	164
Indian 246-bus	1000	800	200	737	590	147

P_{Total} - Total Number of Patterns, P_{Train} - Number of training patterns, P_{Test} - Number of testing patterns.

Table 5.5: Details of Training and Testing Data for Classifiers III and IV

Test Systems	Classifier III			Classifier IV		
	P_{Total}	P_{Train}	P_{Test}	P_{Total}	P_{Train}	P_{Test}
IEEE 14-bus	6642	5314	1328	3121	2497	624
IEEE 30-bus	6006	4785	1221	5997	4797	1200
Indian 246-bus	24722	19778	4944	2967	2374	593

Table 5.6 represents the details of the testing patterns for classifiers I, II, III and IV. As mentioned in section 5.3, only insecure patterns identified by the classifiers I and III are provided as inputs to the classifiers II and IV respectively. Further, the testing patterns of classifiers II and IV with line overload and voltage violation are also listed in Table 5.6.

Table 5.6: Details of Testing Patterns for Classifiers I, II, III and IV

Test Systems	Classifier I	Classifier II			Classifier III	Classifier IV		
		Patterns	P_{LOV}	P_{VV}		Patterns	P_{LOV}	P_{VV}
IEEE 14-bus	200	126	126	0	1328	624	624	0
IEEE 30-bus	200	164	164	87	1221	1200	1200	602
Indian 246-bus	200	147	109	147	4944	593	324	327

P_{LOV} & P_{VV} - Number of Patterns with line overload & voltage violation.

5.4.2 Comparison of WSVM, AdaBoost & CBR Algorithm

The results of the proposed SSA using three new classifier models viz. WSVM, CBR and AdaBoost algorithm are shown in Tables 5.7, 5.8 and 5.9 respectively. It is observed that the prediction accuracy of classifiers I and II using WSVM is between 98% - 100% and using Adaboost algorithm, prediction accuracy of about 99% - 100% is obtained. Similarly, the prediction accuracy of classifiers I and II using CBR method is between 95% - 100% for all the three test systems. Static security evaluation is the assessment of power system security by considering single branch outage (N-1) as contingencies for each loading condition. While carrying out this N-1 security assessment for all the loading scenarios, its respective class label is also determined using SI defined in (5.1). However, it is observed that the random loading at all the buses results in the constraint violation in more than 50% of the generated data patterns. Thus, there are 631, 818 and 737 patterns out of 1000 loading scenarios that leads to system insecurity, thus leaving 369, 182 and 263 patterns as secure for the three test systems, respectively. In this work, only the patterns corresponding to secure class are simulated with single branch contingencies. The number of contingencies considered for IEEE 14-bus and IEEE 30-bus systems are 18 and 33, respectively. Thus, a total of 6642 (369*18) and 5940 (182*33) patterns were generated for IEEE 14-bus and IEEE 30-bus systems respectively. However, for Indian 246-bus system, the number of data patterns is extremely large, as the number of single branch contingencies are sufficiently high. This makes the training and the classification tasks more complex and difficult.

Table 5.7: Results of Classifiers I, II, III and IV using WSVM Classifier

Test Systems	Classifier I				Classifier II			Classifier III				Classifier IV			
	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	
IEEE 14-bus	72	128	100	126	100	0	100	777	551	98.19	624	100	0	100	
IEEE 30-bus	47	153	100	164	100	86	98.85	0	1221	99.92	1200	100	58	09.63	
Indian 246-bus	60	140	100	109	100	147	100	4417	527	96.85	317	97.84	303	92.66	

PA - Prediction accuracy of the classifier; P_{LOV} - Number of patterns with line overload violation, P_{VV} - Number of patterns with voltage violation.

Table 5.8: Results of Classifiers I, II, III and IV using AdaBoost Algorithm

Test Systems	Classifier I				Classifier II			Classifier III				Classifier IV			
	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	
IEEE 14-bus	70	130	99	126	100	0	100	749	579	93.67	624	100	0	100	
IEEE 30-bus	46	154	99.5	164	100	86	99.39	0	1221	99.92	1200	100	38	06.31	
Indian 246-bus	61	139	99.5	108	99.32	147	100	4394	550	93.31	312	96.30	302	93.09	

Table 5.9: Results of Classifiers I, II, III and IV using CBR algorithm

Test Systems	Classifier I				Classifier II			Classifier III				Classifier IV			
	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	P_{Secure}	$P_{Insecure}$	PA (%)	P_{LOV}	PA (%)	P_{VV}	PA (%)	
IEEE 14-bus	72	128	100	126	100	0	100	773	555	98.19	624	100	0	100	
IEEE 30-bus	52	148	95.5	164	100	85	97.70	0	1221	99.92	1200	100	268	44.52	
Indian 246-bus	59	141	99.5	108	99.08	147	100	4384	560	97.92	321	99.07	318	97.25	

Therefore, the proposed SI index shown in (5.1) has been used to select only the critical contingencies from a large list of credible contingencies. The particular contingency is identified as critical, if the calculated SI value > 0 , else that contingency is considered as non-critical for that loading condition. In this perspective, a complete analysis has been carried out to identify the list of critical and non-critical contingencies for every loading condition. While performing this simulation, it is identified that those contingencies which lead to violations in a particular loading condition may not necessarily cause violations for another loading condition. At the end of analysis, it is found that 245 contingencies do not lead to violations in any of the loading conditions and, therefore, these contingencies are removed from the critical contingencies list. Hence, only the remaining 94 (339-245) contingencies are selected as critical contingencies affecting the system security. Therefore, only 24722 (263*94) data patterns are generated for Indian 246-bus system. Finally, the data patterns consisting of contingency location (*from bus and to bus*) and its respective pre-contingent power flows are provided as inputs to classifiers III and IV. The classification results of classifiers III and IV obtained using the above classifiers for all the test systems are listed in columns 4 and 5 of Table 5.7 – Table 5.9 respectively.

5.4.3 Computational Requirement for Online Implementation

The simulations are conducted in MATLAB 8.3 running on a pentium core (TM) i7 3.40 GHz processor desktop. In this work, parallel computation technique has been used to enhance the simulation performance of the proposed CBR based classifiers. Thus, the computing resource is shared in parallel among all the available 4 workers on the above multi-core desktop. Table 5.10 shows the average training time and testing time of the proposed CBR classifiers, where the testing time is shown for 1 unseen random loading condition.

Table 5.10: Computation Time (in seconds) of the Proposed CBR Classifiers

Test Systems	Classifier I		Classifier II		Classifier III		Classifier IV	
	T_r	T_e	T_r	T_e	T_r	T_e	T_r	T_e
IEEE 14-bus	0.2340	0.0722	0.1300	0.0791	0.2595	0.0987	0.1526	0.0975
IEEE 30-bus	0.5334	0.0713	0.1298	0.0754	0.1500	0.0905	0.1496	0.0901
Indian 246-bus	0.2811	0.1915	0.2499	0.1713	2.3158	0.1588	0.3400	0.1377

T_r – Training time and T_e – Testing time.

Table 5.11 lists the average training time and testing time of the proposed CBR classifiers

for Indian 246-bus system before and after parallel computation. These results illustrate that

Table 5.11: Computation Time (in seconds) of the Proposed CBR Classifiers for Indian 246-bus System Before and After Parallel Computation

Test Systems	Classifier I		Classifier II		Classifier III		Classifier IV	
	T_r	T_e	T_r	T_e	T_r	T_e	T_r	T_e
Before	1.6532	1.5969	0.7887	0.7575	49.1897	5.4978	0.3341	0.3095
After	0.2811	0.1915	0.2499	0.1713	2.3158	0.1588	0.3400	0.1377

the computation time of the proposed approach after parallel computation is reduced several times than the simulation time obtained before parallel computation. Thus, it is proved that the parallel computation on a single multi-core desktop is effectively significant in optimizing the computation time of the proposed CBR based classifiers. This simulation can be further optimized by using a multi-core desktop on a larger resource such as a computer cluster (ie., distributed computing server). Further, to prove its feasibility for online implementation, the average CPU time taken in evaluating the unforeseen test sample along-with its training time for practical Indian 246-bus system is compared with other classifiers as illustrated in Table 5.12.

Table 5.12: Computation Time (in seconds) of Different Classifiers for Indian 246-bus System

Test Systems	Classifier I		Classifier II		Classifier III		Classifier IV	
	T_r	T_e	T_r	T_e	T_r	T_e	T_r	T_e
SVM	0.2269	0.0145	0.2109	0.0102	12.8472	0.0201	0.5573	0.0171
ANN	0.8194	0.0114	0.6797	0.0113	4.7937	0.0115	0.9320	0.0115
Proposed	0.2811	0.1915	0.2499	0.1713	2.3158	0.1588	0.3400	0.1377

From the above illustrations, it is observed that the proposed CBR classifiers produce better prediction than the traditional classifiers but at an increased computational cost. This illustrates an important trade-off between the speed and the performance, as the increased accuracy is worth than the additional complexity considering the application and the usage of the reasoning system.

5.4.4 Results of SMOTE for Class Imbalance Problem

From the above results shown in Tables 5.7, 5.8 and 5.9, it is also observed that in the case of IEEE 30-bus system, the prediction accuracy of classifier IV for voltage violation

prediction is very less. This is due to the fact that the training of classifiers is biased towards majority (insecure) class due to the presence of class imbalance in the training data. To overcome this class imbalance problem, SMOTE has been utilized in this work.

Table 5.13: Results of Classifier IV (VV Prediction) for IEEE 30 Bus System before and after SMOTE

	Before SMOTE			After SMOTE		
	WSVM	CBR	AdaBoost	WSVM	CBR	AdaBoost
Total Patterns	5997	5997	5997	8739	8739	8739
Majority Class (Class '0')	3255	3255	3255	3255	3255	3255
Minority Class (Class '1')	2742	2742	2742	5484	5484	5484
Training Patterns	4797	4797	4797	7539	7539	7539
Testing Patterns	602	602	602	602	602	602
Minority Class Predicted	58	268	38	602	550	602
Prediction Accuracy	09.63 %	44.52 %	06.31 %	100 %	91.36 %	100 %

Table 5.13 lists the details about the number of synthetic data generated, testing patterns and prediction accuracy of the classifiers before and after SMOTE. The test patterns consists of 602 voltage violation instances in which only 268 instances are predicted correctly by the CBR algorithm. Similarly, the AdaBoost and WSVM classifiers can predict only 38 and 58 instances respectively against 602 instances. Using SMOTE, 1 synthetic sample is generated for each minority sample (patterns with voltage violation). Thus, a total of 2742 synthetic data are generated for all 2742 minority samples. These additional 2742 synthetic samples are then included in the training set and the patterns having only voltage violation are considered for testing. Thus, after inclusion of SMOTE data, the classifiers WSVM and AdaBoost give 100% prediction accuracy with all 602 instances predicted correctly. Similarly, the CBR algorithm can predict 550 instances with a prediction accuracy of about 91.36%. Henceforth, it is concluded that the class imbalance problem in power system measurements can be attenuated with the use of simple oversampling or undersampling techniques. In this work, SMOTE is used as it found to be better than the random sampling methods.

5.4.5 Analysis of the Proposed SSA Results with Existing Methods

Tables 5.14–5.15 list the comparison of the proposed SSA results using WSVM, CBR and AdaBoost classifiers with SVM, ANN and k-NN. The ANN based security assessment [180] have shown extremely good non-linear input-output mapping provided enough number of

neurons are considered in the hidden layer. In this work, two-layer feed forward neural network with 10 neurons in the hidden layer have been considered. However, the major drawback of neural networks is the selection of sufficient number of hidden neurons. When the number of hidden neurons is very less, the training of ANN is impeded and when the ANN is trained with more number of hidden neurons, the performance of the classifier is degraded. A pattern recognition based SVM classifier, which has been extensively used for power system security assessment and classification [174] has also been taken into consideration. The concept of kernel mapping makes the SVM classifiers to perform non-linear classification even with complex boundaries. In this work, radial basis function (gaussian) kernel has been used as the mapping function due to its capability of handling non-linear relation existing between the input data and its class labels. The kNN algorithm which has been used for classification of power system faults [181] has also been considered in this work. This classifier is tested with different values of ' k ' and the model (at $k=2$), which gives higher classification accuracy, is selected as an optimal value. This kNN classifier firstly determines two training patterns that are close to the given test data using euclidean distance criterion. After that, a similarity measure is performed on all neighbours to identify the most similar pattern among the neighbours. Finally, the class label of the most similar pattern is assigned as the target label of the provided test data.

Table 5.14: Performance Analysis of Various Classifiers for IEEE 14-bus and 30-bus systems

Methods	IEEE 14 Bus						IEEE 30 Bus					
	Classifier I	Classifier II		Classifier III	Classifier IV		Classifier I	Classifier II		Classifier III	Classifier IV	
		P_{LOV}	P_{VV}		P_{LOV}	P_{VV}		P_{LOV}	P_{VV}		P_{LOV}	P_{VV}
ANN	100	100	100	88.63	100	100	100	100	97.75	99.92	100	94.68
SVM	97.5	86.51	86.51	96.69	94.55	94.87	97.51	95.12	96.67	88.28	96.92	100
kNN	100	100	100	99.70	100	100	100	100	98.78	99.92	100	43.69
Proposed WSVM	100	100	100	98.19	100	100	100	100	98.85	99.32	100	100
Proposed CBR	100	100	100	98.19	100	100	95.5	100	97.70	99.92	100	91.36
Proposed AdaBoost	99	100	100	93.67	100	100	99.5	100	99.39	99.92	100	100

Table 5.15: Performance Analysis of SSA Results Obtained using Various Classifiers for Indian 246-bus System

Methods	Indian 246 Bus					
	Classifier I	Classifier II		Classifier III	Classifier IV	
		P_{LOV}	P_{VV}		P_{LOV}	P_{VV}
ANN	100	100	100	95.29	94.94	94.09
SVM	99.5	98.17	97.28	90.13	94.14	90.21
kNN	99.5	98.17	100	98.85	96.29	97.30
Proposed WSVM	100	100	100	96.85	97.84	92.66
Proposed CBR	99.50	99.08	100	97.92	99.07	97.25
Proposed AdaBoost	99.5	99.32	100	93.31	96.30	93.09

Further, it has been observed that the proposed method of input data generation leads to class imbalance problem in an IEEE 30 bus system. This problem may adversely affect the performance of the classifiers. In order to overcome that, the SMOTE data has also been included in the training set of classifier IV for the prediction of insecure patterns with voltage violation. From the classification results, it is found that the SMOTE is beneficial where power system measurements have class imbalance data. However, the classification accuracy of classifier IV using k-NN classifier is only 43.69% even after considering SMOTE data. Hence, it is understood that the sampling methods have the least effect on the performance of the k-NN classifier. The above results show that the proposed approach gives better prediction results than the SVM based pattern recognition approaches. In addition to that, it is also found that ANNs and k-NN based security assessment methods have a similar performance as that of the proposed AdaBoost classifiers based security assessment. In spite of their widespread use for power system security assessment, these traditional classifiers have some drawbacks stated as follows - (1) The training of the neural networks for larger systems such as Indian 246 bus system would be time consuming, as the number of connection weights and neurons would be extremely large due to the mapping of large input data to the output nodes. (2) The selection of ' k ' in the nearest neighbour classifier is a difficult task, as smaller values of ' k ' leads to overfitting and its higher values results in the longer simulation time. This increases the computational complexity of this algorithm with larger systems, owing to huge training data. (3) The choice of kernel and the selection of kernel parameters in a SVM classifier is a complex task, which requires thorough investigation.

Based on the above observations, it is concluded that the performance of the existing machine learning techniques is greatly impacted by the selection of suitable input parameters and the complexities involved in training due to large input data. Since these methods are mainly dependent on the input training data, they can often lead to high misclassification rate, if the underlying information in the training data is not known. To overcome this drawback, WSVM, CBR and AdaBoost based classifiers proposed for SSA give better performance than the traditional classifiers in terms of classification accuracy. Thus, it is realized that security assessment results can be further enhanced with the usage of classifiers having better generalization capability than the traditional ones. Moreover, it is also observed that both WSVM and AdaBoost classifiers provide similar performance in most of the cases. Although CBR performs better than the traditional classifiers, training of CBR is very complex and

may require additional computational infrastructure. However, in terms of performance and less complexity involved in classifier design, it is concluded that both WSVM and AdaBoost classifiers can enhance the monitoring and security assessment of power systems.

5.5 Conclusions

This chapter presents the application of various intelligent classifiers with different generalization capability for static security assessment of power systems using phasor measurements. This study provides the vital information needed to study the operational security of systems with high level of prediction accuracy. Traditionally, security indices are used to classify the training patterns into secure or insecure class, but they suffer from masking problem and weight factor allocation problem. Therefore, a composite security index, consisting of both power flows and bus voltage limit violations is proposed in this chapter to classify the training patterns into secure or insecure classes. The dimensionality of the input phasor measurements which increases with the increase in system size, further complicates the complexity and the training time of the classifiers. Hence, a statistical approach based on class separability and correlation coefficient indices has been used in this chapter to identify only the relevant phasor measurements. Studies conducted on IEEE 14 bus, IEEE 30 bus and a practical Indian 246 bus systems reveal the following.

1. The proposed framework predicts the static security status as well as the type of violations that causes insecurity of power systems.
2. The security assessment and monitoring is further enhanced with the usage of new classifiers with higher generalization capability. These classifiers viz. WSVM, CBR and AdaBoost algorithm provide better classification performance than the traditional machine learning techniques used for security assessment.
3. Although WSVM, CBR and AdaBoost algorithm is found to give better prediction than the existing classifiers, the training of CBR involves complex learning algorithms and hence require advanced computational infrastructure. Therefore, in terms of performance and complexity, it is concluded that both WSVM and AdaBoost classifiers can be considered as the best tool for the proposed security assessment.
4. Class imbalance in the input data generated for an IEEE 30-bus system significantly affects the overall performance of the classifiers. Hence, SMOTE technique is used to overcome this problem.

Chapter 6

Transient Security Assessment using Machine Learning Techniques

6.1 Introduction

Power system security is frequently affected by some of the severe contingencies like faults, generator tripping, line switching and load shedding. These events may subsequently cause considerable separation in generator rotor angles of a large interconnected power system. Transient Security Assessment (TSA) is used to determine whether the system oscillations, following the occurrence of a fault, will result in loss of synchronism among the generators [182]. There have been many methods reported to predict the system security status during the occurrence of large disturbances. The authors in [183, 184] have proposed an ANN based method utilizing synchronized measurements for the prediction of transient security of power systems. In [185], SVM based method has been proposed for real time transient security assessment. The synchronized measurements such as rotor angles, voltage magnitudes and speeds obtained using PMUs are provided as inputs to the SVM classifier. Similar approach using DTs has been proposed in [186, 187] for real time prediction of transient instability in power systems. Since past few years, these methods have been successfully applied for predicting the transient security of power systems. But these studies have not considered the status of the individual machine losing synchronism from transient stability point of view. Hence, no information about the severity of disturbance is obtained. Further studies have revealed that asynchronous or out-of-step operation of one or more system generators with the rest of the power system is one of the primary reasons for system blackout [188]. The out-

of-step operation of system generators often result in damage to generator-turbine shaft due to pulsating torques and torsional resonance. Therefore, it is important to determine the out-of-step operation of system generators. This can be achieved by having a suitable mechanism that can effectively predict the machine synchronism status of each system generators. This information has become vital in identifying the magnitude and severity of each disturbance and thereby an appropriate counter measure can be initiated.

System islanding becomes inevitable in case of large disturbances and in such situations, the information about the number of generators in each coherent group is very important to initiate appropriate controlled islanding strategies. Generator coherency is defined as the group of generators that exhibit similar dynamic behavior following a disturbance. In the past, various schemes have been proposed to determine the coherent group of generators following a large disturbance [189–193]. The most commonly used method to determine the generator group coherency is by observing their swing curves during fault and post-fault periods. However, this scheme based on time-domain simulation is an offline process. There have been only few studies reported so far on the determination of generator coherency in real time [192,193]. Thus, there has been a strong requisite to determine the coherency status of generators in a faster manner for initiating real-time control actions.

In this chapter, a new approach has been proposed for enhanced monitoring and assessment of transient security of power systems utilizing synchronized measurements has been proposed. The proposed approach can predict the transient security status, individual machine synchronization status as well as the coherent group of generators. The rotor angle of generators obtained using PMUs are used as inputs for all predictions. A new synchronism status index is formulated using these phasor measurements to identify the machine synchronism status in each training pattern. AdaBoost classifiers have been used in the proposed framework due to their high generalization capability than the existing classifiers including CBR algorithm. This TSA framework consists of three classifier models in which classifier I predicts the transient security status and classifier II is used to determine the generator coherency. Classifier III is a hybrid classifier, which determines the individual generator synchronism state for a given operating condition. This hybrid classifier consists of an array of parallel classifiers, where one classifier is assigned to each generating unit of the power system. The proposed approach is implemented and tested on standard benchmark systems such as IEEE 14-bus, IEEE 30-bus and on a practical Indian 246-bus networks. Results indicate

that the proposed approach can enhance the overall monitoring and security assessment of power systems.

6.2 Data Generation & Rotor Trajectory Index

In this thesis, sufficient amount of patterns were generated through offline time domain simulations by randomly varying the load at all the buses between 50% and 200% of their base case to obtain different loading conditions. For each loading scenario, a three phase fault is simulated at 0.1 s on each bus and the fault is cleared after 5 cycles by opening of a transmission line connected to that bus. Similar evaluation has been carried out considering outage of all transmission lines, one at a time, connected to that faulted bus. Then, the generator rotor angles obtained using PMUs are utilized to compute the transient security status of each outage scenario. The training and testing patterns are formed from the total generated data patterns. Finally, the Rotor Trajectory Index (RTI) proposed in [194] is evaluated for each training pattern. This index is used to find the severity of a contingency based on rotor angle trajectory of each generating unit following a disturbance. It is mathematically defined as follows,

$$RTI = 1 - \frac{360^\circ - (\Delta\delta_{i,COI})_{max}}{360^\circ + (\Delta\delta_{i,COI})_{max}} \quad (6.1)$$

where, $(\Delta\delta_{i,COI})_{max}$ is the maximum relative rotor angle difference of i^{th} generator with respect to Center Of Inertia (COI) in the post fault period. For any generating machine, if the maximum value of RTI crosses the threshold ζ , the system leads to transiently insecure, else the system remains transiently secure. Here, the value of ζ is taken as 0.5. Thus, if $(RTI < 0.5)$, then the pattern is secure else, it belongs to insecure class.

The relative rotor angle of i^{th} generator with respect to COI can be calculated using,

$$\Delta\delta_{i,COI} = |\delta_i - \delta_{COI}| \leq \delta_{max} \quad \forall i \in N_G \quad (6.2)$$

$$\delta_{COI} = \frac{\sum_{i=1}^{N_G} M_i \delta_i}{\sum_{i=1}^{N_G} M_i} \quad (6.3)$$

$$M_i = \frac{2H_i}{\omega_s} \quad (6.4)$$

where, δ_i is the rotor angle of the i^{th} generator; δ_{COI} is the angle of center of inertia; δ_{max} is the maximum allowable relative angle difference for secure operation ($\delta_{max} = 120^\circ$); M_i is the mass of the i^{th} generator; N_G is the number of system generators; H_i is the inertia constant

of the i^{th} generator; ω_s is the synchronous speed ($\omega_s = 2\pi f_s$).

6.3 Proposed Synchronism Status Index

The rotor angle δ of the generators, measured by PMUs after the clearance of fault, contain sufficient information for the prediction of transient security status of power systems [184, 195]. Hence, the generator angles at the time of fault (or Fault Application time (f_a)), at the Fault Clearing Time (FCT) and consecutive 5 cycles after FCT (such as FCT+1, FCT+2, FCT+3, FCT+4 and FCT+5) are also recorded. Since it is convenient to represent the transient behaviour of power systems in COI framework, the measured generators angles at FCT and consecutive 5 cycles after FCT are converted with respect to COI coordinates. Then, a new Synchronism Status Index (SSI) has been proposed to classify the synchronism status of each generator in terms of either 0 (Not Synchronized) or 1 (Synchronized), following a disturbance. The proposed SSI is defined as,

$$SSI = \begin{cases} 0, & \text{if } \delta_i^{final} > \xi \text{ (in radians)} \\ 1, & \text{otherwise} \end{cases} \quad (6.5)$$

where, $\delta_i^{final} = [abs(\delta_{i,COI}^{FCT} - \delta_{i,COI}^{FCT+1}) + abs(\delta_{i,COI}^{FCT+1} - \delta_{i,COI}^{FCT+2}) + abs(\delta_{i,COI}^{FCT+2} - \delta_{i,COI}^{FCT+3}) + abs(\delta_{i,COI}^{FCT+3} - \delta_{i,COI}^{FCT+4}) + abs(\delta_{i,COI}^{FCT+4} - \delta_{i,COI}^{FCT+5})]$

Here, the value of ξ is taken as 0.2618 (15°). The smaller or higher values of δ_i^{final} represents the generator 'i' with least or more chance of loosing synchronism with the rest of the system.

6.4 Proposed Framework of TSA

The detailed framework of monitoring and transient security assessment of power systems is shown in Figure 6.1. This framework has three major functions like transient security prediction, coherent generator group prediction and determination of synchronism status of each generating unit. For this purpose, three classifier models have been utilized with each classifier performing one important function. The vectors X_1, X_2, \dots, X_m , which represent the rotor angle measurements corresponding to generating units G_1, G_2, \dots, G_m respectively are provided as inputs to all the classifier models. In particular, input X_m is the vector of rotor angle measurements of m^{th} generator taken at fault application time (δ_m^{fa}), at FCT (δ_m^{FCT}), and their angle in the COI framework at FCT ($\delta_{m,COI}^{FCT}$) and consecutive 5 cycles after FCT ($\delta_{m,COI}^{FCT+1}, \delta_{m,COI}^{FCT+2}, \delta_{m,COI}^{FCT+3}, \delta_{m,COI}^{FCT+4}, \delta_{m,COI}^{FCT+5}$). Thus, eight inputs are required for

one generating unit thereby making the total inputs as $8 * m$ for a system with ' m ' generating units.

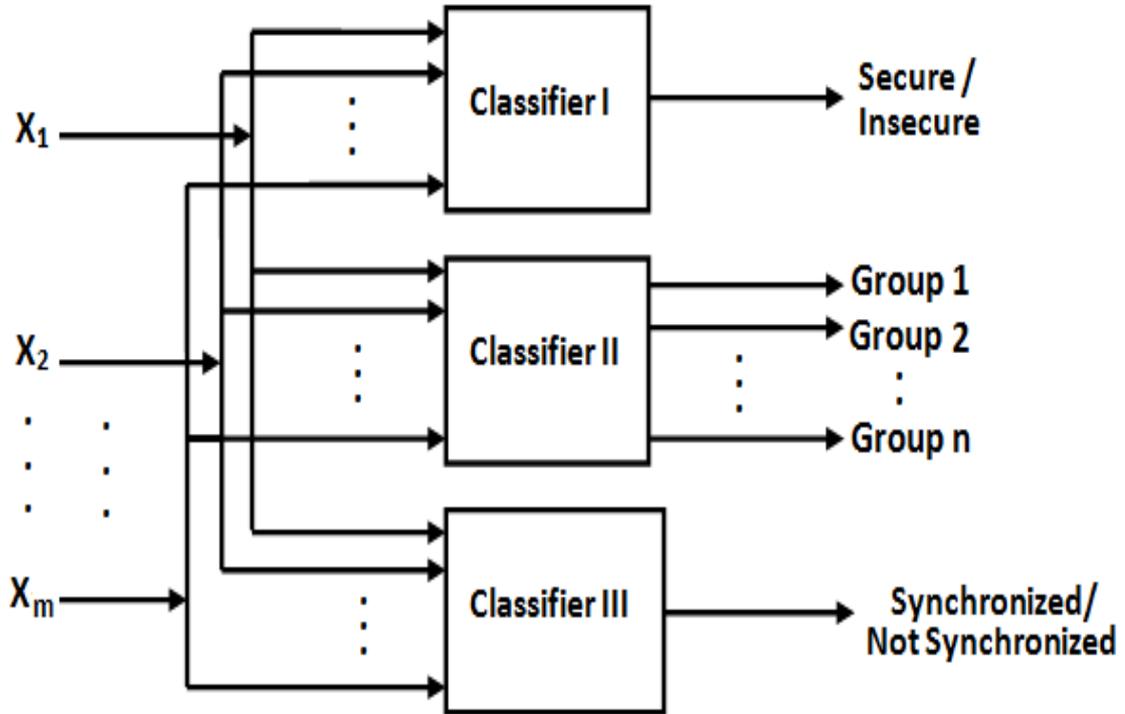


Figure 6.1: Proposed Framework of Transient Security Assessment

Classifier I is designed using AdaBoost algorithm to classify the transient security status of power systems. The training patterns are classified into secure or insecure based on the RTI defined in (6.1). Finally, the classifier I once trained, can accurately classify the transient security status of the unforeseen testing patterns. Classifier II uses a multiclass SVM to determine the coherent group of generators for the provided test data. Since the generator coherent group is a multi-class classification problem and AdaBoost classifier described in Chapter 4 is designed to give only binary class of outputs viz. either 0 or 1, a multiclass SVM has been utilized for this purpose. Prior to coherency determination using classifier II, the coherent group of generators for each training pattern is determined by observing their swing curves obtained during fault and post fault periods. For a given fault, the generator ' i ' can be considered coherent with respect to the slack generator within a tolerance ξ , if they have similar rotor angles response during fault and post-fault periods. It is represented by the following equation.

$$\Delta\delta_{io}(t) = \text{abs}(\delta_i(t) - \delta_o(t)) \leq \xi, \quad \forall i \in N_G \quad (6.6)$$

where, δ_i is the rotor angle of the generator 'i' in degrees and δ_o is the rotor angle of the slack generator. The rotor angles, δ_i (for $i=1$ to N_G , $N_G \neq$ slack generator) of all the generators are noted after 54 cycles of FCT and subsequently classified into six different coherent generator groups as shown in Table 6.1. For this study, ξ is taken as 15° .

Table 6.1: Coherent Group Classification

Group	Range of $\Delta\delta_{io}$ at FCT+54 cycles
1	$> 120^\circ$ Most Advanced
2	$90 - 120^\circ$
3	$60 - 90^\circ$
4	$30 - 60^\circ$
5	$15 - 30^\circ$
6	$< 15^\circ$ Least Advanced

Thus, after training, classifier II can classify the coherent group of generators for the test patterns effectively. Classifier III is a hybrid classifier, which consists of an array of Adaboost SVM classifiers. The structure of this hybrid classifier is illustrated in Figure 6.2. Here, the classifier array consists of 'm' parallel classifiers such that each classifier is as-

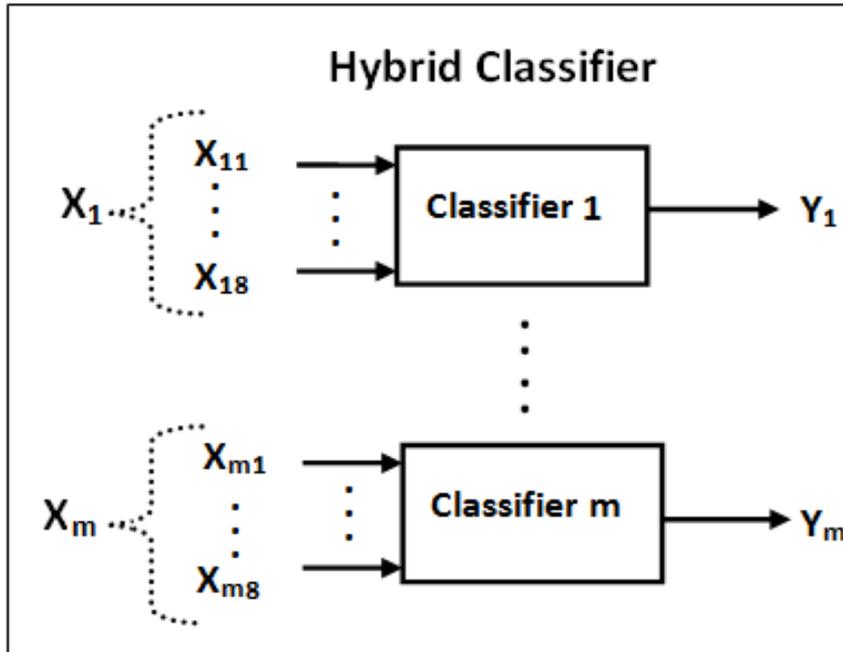


Figure 6.2: Proposed Structure of Hybrid Classifier for Synchronism Status Detection

signed to each generating unit. Initially, for each training pattern, the synchronism status of generating units are determined using (6.5). Then, the classifier III after training, can determine the synchronism status of all the generating units. Thus, for any unforeseen operating

condition, the information about the out-of-step operation of generators can be determined using Y_1, Y_2, \dots, Y_m .

6.5 Case Studies

The proposed TSA has been demonstrated on IEEE 14-bus, IEEE 30-bus and Indian 246-bus systems. The base case operating condition and dynamic data of the above test systems are provided in Appendices B, C and D respectively. The inputs to the proposed approach are the rotor angle measurements of all generating units, which are obtained using PMUs at fault application time, at FCT and their angle in the COI framework at FCT and consecutive five cycles after FCT. Table 6.2 lists the number of PMUs, number of generators and the total number of features available for the three test systems. The total number of contingencies considered for each loading scenario and the total number of testing patterns for the three test systems are also listed in Table 6.2.

Table 6.2: Details about Various Parameters in the Test Systems

Details	IEEE 14	IEEE 30	Indian 246
Number of PMUs	3	7	57
Number of Generators	5	6	42
Number of contingencies possible	40	82	752
Number of contingencies selected	40	82	117
Number of features	40	48	336
Number of input patterns	4040	8282	11817
Number of testing patterns	808	1656	1693

The time domain simulation is performed by simulating a three phase fault on each bus at 0.1 s and the fault is cleared after 5 cycles by tripping of a transmission line connected to that faulted bus. This analysis has been carried out considering outage of all transmission lines connected to the faulted bus. As mentioned in section 6.2, thus there are about 40 and 82 contingencies possible for IEEE 14-bus and IEEE 30-bus systems. Besides that, load of each bus is randomly varied between 50%–200% to generate 101 different loading scenarios. Thus, a total of 4040 (101*40) and 8282 (101*82) patterns were generated for the two test systems, respectively. Similarly, there are 752 contingencies for an Indian 246-bus system. This considerably increases the amount of input data patterns and thus, also the complexity and time associated with the training of classifiers. To reduce the training

patterns, the RTI defined in (6.1) has been used to select only the critical contingencies from the large list of credible contingencies. The particular contingency is identified as critical, if the calculated RTI value > 0.5 , else that contingency is considered as non-critical for that loading condition. This analysis has been carried out to identify the list of critical and non-critical contingencies for every loading condition. Then the contingency, which is found to be critical in most of the loading conditions is given the top priority and the remaining contingencies are ranked accordingly. At the end of this analysis, it is found that nearly 635 contingencies are found to be non-critical in most of the loading conditions. Thus, only top 117 out of 752 contingencies are selected as the probable contingencies. Therefore, $101 \times 117 = 11817$ operating conditions are generated to assess the security status of the Indian 246-bus system. Out of entire patterns generated, 80% of them are given as training data and remaining 20% as testing data. The details of time domain simulation performed for

Table 6.3: Details about time domain simulation for Test Systems

Fault Details	60 Hz	50 Hz
Fault application time, f_a	0.1s	0.1s
Fault clearing time, f_c	0.183s	0.2s
Fault duration	90ms	100ms
Total transient analysis	2s	2s

Table 6.4: Security Assessment (Classifier I) of the Testing Patterns using the Proposed Approach

Test Systems	Testing Patterns	Using RTI			Proposed Approach			PA (%)
		P_{Secure}	$P_{Insecure}$	T_e	P_{Secure}	$P_{Insecure}$	T_e	
IEEE 14-bus	808	716	92	1.0950	700	109	0.0235	97.90
IEEE 30-bus	1656	1374	282	1.0880	1343	313	0.0694	98.13
Indian 246-bus	1693	1682	11	7.7625	1693	0	0.9394	99.35

PA - Prediction accuracy of the classifier; T_e - Average testing time of classifier in seconds.

standard test systems (60Hz systems) and Indian 246-bus system (50Hz system) are given in Table 6.3.

Table 6.4 shows the results of transient security prediction (classifier I) using AdaBoost algorithm for IEEE 14-bus, IEEE 30-bus and Indian 246-bus systems. The proposed approach gives a prediction accuracy of about 97.90%, 98.13% and 99.35% for the three test systems, comprising of 5, 6 and 42 generating units, respectively. Further, to prove its fea-

sibility for online implementation, the average CPU time taken in evaluating the unforeseen test sample for the three test systems are compared with the traditional method as illustrated in Table 6.4. Traditionally, the generator coherency is determined by observing their swing curves during fault and post fault periods. Then, the rotor angle trajectory of all generators obtained after 54 cycles of FCT are utilized to classify the generating units into different coherent groups as shown in Table 6.1. The results obtained using classifier II for the three test systems are compared with those obtained using traditional method in Tables 6.5, 6.6 and 6.7. These tables depict the total number of testing patterns and the number of patterns correctly predicted by classifier II alongwith its prediction accuracy for the three test systems. For IEEE 14-bus system, classifier II gives a prediction accuracy of above 89% for all its generating units. Similarly, classifier II has a prediction accuracy of about 86.72%–96.50% for IEEE 30-bus system. In case of Indian 246-bus system, there are 42 generating units and the classifier II gives similar prediction with an accuracy of about 82.46%–92.56% in most of the generating units. Therefore, the simulation results obtained for first 8 generators (except slack generator) are shown in Table 6.7.

Table 6.5: Coherent Generator Group Prediction (Classifier II) for IEEE 14-bus System

Generating Units	$Test_{tt}$	Traditional Method						Proposed Approach						$Test_{cp}$	PA (%)
		Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6	Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6		
G_2	808	56	3	7	155	393	194	62	5	6	179	338	218	731	90.47
G_3	808	73	8	18	173	294	242	83	4	21	118	288	231	750	92.82
G_4	808	84	25	264	401	26	8	94	26	269	377	35	7	746	92.33
G_5	808	97	4	27	272	272	136	103	10	30	285	138	142	723	89.48

$Gr_1, Gr_2, Gr_3, Gr_4, Gr_5$ and Gr_6 - Group1, Group2, Group3, Group4, Group5 and Group6, respectively; $Test_{tt}$ and $Test_{cp}$ - Total Testing Patterns and Total Testing Patterns Correctly Predicted, respectively.

Table 6.6: Coherent Generator Group Prediction (Classifier II) for IEEE 30-bus System

Generating Units	$Test_{tt}$	Traditional Method						Proposed Approach						$Test_{cp}$	PA (%)
		Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6	Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6		
G_2	1656	14	2	13	34	357	1236	13	3	13	47	376	1204	1598	96.50
G_3	1656	17	8	7	113	447	1064	16	9	9	159	411	1052	1564	94.44
G_4	1656	17	2	21	165	569	882	17	2	58	186	527	866	1499	90.52
G_5	1656	299	22	36	668	320	311	319	16	30	665	315	311	1558	94.08
G_6	1656	35	15	61	224	860	461	38	26	100	280	720	492	1436	86.72

Table 6.7: Coherent Generator Group Prediction (Classifier II) for Indian 246-bus System

Generating Units	$Test_{tt}$	Traditional Method						Proposed Approach						$Test_{cp}$	PA (%)
		Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6	Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6		
G_2	1693	1229	102	139	106	0	117	1376	47	102	72	0	96	1406	83.05
G_3	1693	1295	123	123	65	6	81	1385	109	143	10	0	46	1463	86.41
G_4	1693	1251	118	130	82	23	89	1375	83	128	12	0	95	1397	82.52
G_5	1693	1235	126	161	56	18	97	1366	98	129	5	95	0	1396	82.46
G_6	1693	1233	105	174	64	11	106	1376	83	133	0	101	0	1395	82.40
G_7	1693	1118	135	218	45	15	162	1196	102	198	7	63	127	1567	92.56
G_8	1693	1090	191	165	102	32	113	1263	174	161	12	0	83	1520	89.78
G_9	1693	1243	112	154	72	28	84	1292	101	145	6	115	34	1557	91.97

Table 6.8: Synchronism Status Prediction (Classifier III) for IEEE 14-bus System

Generating Units	$Test_{tt}$	Synchronized		Not Synchronized		$Test_{cp}$	PA (%)
		Using SSI	Proposed	Using SSI	Proposed		
G_1	808	664	645	144	163	789	97.65
G_2	808	808	804	0	4	804	99.51
G_3	808	657	643	151	165	794	98.27
G_4	808	327	325	481	483	800	99.01
G_5	808	655	648	153	160	801	99.13

Table 6.9: Synchronism Status Prediction (Classifier III) for IEEE 30-bus System

Generating Units	$Test_{tt}$	Synchronized		Not Synchronized		$Test_{cp}$	PA (%)
		Using SSI	Proposed	Using SSI	Proposed		
G_1	1656	1510	1505	146	151	1651	99.70
G_2	1656	1656	1656	0	0	1656	100
G_3	1656	1655	1652	1	4	1653	99.82
G_4	1656	1650	1649	6	7	1655	99.94
G_5	1656	1090	1071	566	585	1635	98.73
G_6	1656	1617	1608	39	48	1647	99.46

As mentioned in section 6.4, classifier III is a hybrid classifier consisting of an array of AdaBoost classifiers in such a manner that each AdaBoost classifier is assigned to each generating unit. Therefore, the proposed classifier III model in the framework shown in Figure 6.1 requires 5, 6 and 42 AdaBoost classifiers for the three test systems, respectively. These results, which are obtained for all the testing patterns are then compared with the results obtained using traditional method. Tables 6.8, 6.9 and 6.10 show the comparison of synchronism status of generating units obtained using the proposed and traditional methods for the three test system, respectively. Classifier III has a prediction accuracy of about 97.65%–99.51% for IEEE 14-bus system and has prediction accuracy of above 99% for IEEE 30-bus system. These results also reveal that all the generating units in IEEE 14-bus and IEEE 30-bus systems are synchronized with the rest of the system in most of the testing patterns. The Indian 246-bus system requires 42 AdaBoost classifiers to predict the synchronism status of each generating unit. The results obtained for randomly selected 14 generating units are shown in Table 6.10. The classifier III precisely determines the synchronism status of these 14 generating units with a prediction accuracy of about 84.11%–97.58%.

Table 6.10: Synchronism Status Prediction (Classifier III) for Indian 246-bus System (of 14 Random Generators)

Generating Units	$Test_{tt}$	Synchronized		Not Synchronized		$Test_{cp}$	PA (%)
		Using SSI	Proposed	Using SSI	Proposed		
G_2	1693	1172	1217	521	476	1628	96.16
G_5	1693	609	838	1084	855	1464	86.47
G_7	1693	1027	862	666	831	1516	89.55
G_{11}	1693	1155	1187	538	506	1569	92.67
G_{14}	1693	1304	1376	389	317	1619	95.63
G_{17}	1693	134	226	1559	1467	1465	86.53
G_{21}	1693	168	240	1525	1453	1465	86.53
G_{25}	1693	1268	1007	425	686	1424	84.11
G_{28}	1693	1340	1375	353	318	1652	97.58
G_{31}	1693	1444	1493	249	200	1604	94.74
G_{34}	1693	1238	1113	455	580	1564	92.38
G_{37}	1693	1335	1118	358	575	1460	86.24
G_{40}	1693	119	174	1574	1519	1488	87.89
G_{42}	1693	1428	1438	265	255	1623	95.87

Tables 6.11 and 6.12 list the TSA results of Indian 246-bus system obtained using the traditional and proposed methods at different loading levels such as 50%, 125%, 150% and 185%. The number of generating units in each coherent group and the number of synchronized as well as non-synchronized generating units in each loading pattern are also shown in Table 6.11. The three loading patterns, which are identified as secure are correctly predicted by classifier I, thus giving a prediction accuracy of about 100%. Similarly, classifier II accurately predicts the list of generating units in each coherent group with a accuracy of about 100% for the first two loading scenarios. It is revealed that all the 41 generating units (except slack generator) are in same coherent group (least variation among the generators rotor angle trajectories) at 50% and 125% of system loading. And as the loading increases, few generators move into different coherent groups depending on the their rotor trajectories. For the remaining two loading patterns, classifier II gives an accuracy of about 85.37% and 80.49%, respectively. Finally, classifier III is utilized to determine the synchronization status of each generating units at each loading scenario. The last column of Table 6.12 lists the number of synchronized and non-synchronized generating units identified by classifier III alongwith its prediction accuracy.

Table 6.11: TSA of Indian 246-bus System at Different Loading Levels using the Traditional Method

Pattern	Loading(%)	Faulted Bus	Contingency	Security Status	Generator Coherency Status						Synchronism Status of Generators	
					Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6	Synchronized	Not Synchronized
7931	50	21	21-37	Secure (1)	-	-	-	-	-	41	30	12
8242	125	7	7-65	Secure (1)	-	-	-	-	-	41	17	25
6873	150	34	136-34	Secure (1)	2	-	1	5	2	31	27	15
7350	185	18	18-134	Insecure (0)	1	-	4	2	7	27	29	13

Table 6.12: TSA of Indian 246-bus System at Different Loading Levels using the Proposed Approach

Pattern	Classifier I		Classifier II						Classifier III			
	TSA	PA(%)	Gr_1	Gr_2	Gr_3	Gr_4	Gr_5	Gr_6	PA(%)	Synchronized	Not Synchronized	PA (%)
7931	Secure (1)	100	-	-	-	-	-	41	100	26	16	86.67
8242	Secure (1)	100	-	-	-	-	-	41	100	17	25	100
6873	Secure (1)	100	1	-	0	2	3	35	85.37	25	17	92.59
7350	Insecure (0)	100	0	-	1	1	4	35	80.49	33	9	87.88

6.6 Conclusions

This chapter presented a new approach utilizing the synchronized measurements for enhancing the TSA of power systems. The proposed approach can determine the system security status, individual machine synchronism state and the coherent group of generators. The synchronized measurements consisting of generator rotor angles obtained using PMUs at during fault and post fault periods are provided as inputs to the proposed method. To identify the machine synchronism status in each training pattern, a new Synchronism Status Index (SSI) has also been proposed. The proposed TSA framework consists of three classifier models. Classifier I, which uses AdaBoost classifier accurately predicts the transient security status with a prediction accuracy of about 97.90 % – 99.35 % for the three test systems. Classifier II determines the coherent group of generators using multiclass SVM classifier and classifier III is a hybrid classifier consisting of an array of AdaBoost classifiers. Each AdaBoost classifier determines the synchronism status of each generating unit. Finally, the effectiveness of the proposed approach is tested on standard benchmark systems such as IEEE 14-bus, IEEE 30-bus and on a practical Indian 246-bus networks. The comparison of the simulation results obtained using the proposed approach with the results obtained using classical time domain simulations reveal the following. The existing time domain simulations cannot be effectively applied for post fault assessment of power systems under real time conditions because of their computational complexity and complex modelling. The average testing time of the proposed method for transient security evaluation is found to be less than 0.1 second for all the three test systems in comparison to the longer simulation time obtained using traditional approach. The effectiveness of the proposed TSA approach makes it more suitable for online implementation.

Chapter 7

Conclusions

7.1 Discussion and Conclusions of the Work

The main focus of this thesis is to improve the overall monitoring and security assessment by utilizing synchronized measurements, obtained from Phasor Measurement Units (PMUs). An intelligent search technique based PMU placement method has been proposed to ensure complete system observability with a lesser number of PMUs than the existing methods. The proposed placement scheme is designed to provide complete system observability during all operating scenarios viz. normal operation as well as during cascaded failures. Then, a new framework for Static Security Assessment (SSA) has been proposed to predict the security status and the type of violations causing insecurity in the system. Different machine learning techniques with higher generalization ability has been explored in this thesis to improve power system monitoring. Finally, a novel framework for Transient Security Assessment (TSA) is also proposed, which can predict the transient security status, individual machine synchronism state and coherent group of generators. The effectiveness and suitability of the proposed security framework has been investigated on different test systems such as IEEE 14-bus, IEEE 30-bus and a practical Indian 246-bus systems.

Chapter 1 discusses the various operating states of power system and major components of security assessment. The importance of phasor measurements based security assessment has been highlighted alongwith the review of various techniques proposed for optimal placement of PMUs in power system. The final part of this chapter presents the motivation behind the research work carried out in this thesis.

In Chapter 2, a new method based on intelligent search technique has been proposed for

the optimal placement of PMUs to make the power system topologically observable. The proposed method works in two stages. Stage I is used to find the sub-optimal locations of PMUs using Best First Search (BFS), which is an intelligent search algorithm with an ability to change its search path from the current node to the most promising node. These results obtained in stage I are then given to stage II to remove the redundant PMU locations using pruning. The proposed method is further extended to incorporate the presence of conventional flow measurements in the system. The proposed placement method is also found to be effective in handling both single as well as multiple flow measurements connected to a bus. The proposed method is applied on all test systems under different operating scenarios viz. normal operation as well as during single line loss and single PMU loss. Simulation results demonstrate that the proposed method is more effective than the existing methods, especially for larger systems. The proposed method is also found to be computationally efficient as its simulation time is less than 2 seconds for all the systems.

Chapter 3 proposes a suitable Optimal PMU Placement (OPP) scheme to determine the optimal locations of PMUs for maintaining complete system observability during cascaded failures. Both the islanding and the non-islanding cases were generated for the test cases following the cascaded failures. To identify whether a particular cascaded failure leads to islanding condition, a topology based approach has also been proposed. In addition to cascaded failures, additional contingencies such as single line and single PMU loss have also been considered. In this chapter, measurement redundancy is also incorporated in the proposed method to enhance the state estimation process. Simulation results reveal that the proposed redundant observability method offers better results than the two stage method proposed in Chapter 2 by providing increased redundancy with the same number of PMUs. Another important aspect is that the proposed redundancy method offers multiple PMU placement solutions having different levels of redundancy for the same number of PMUs.

Three intelligent classifiers such as Wavelet Support Vector Machine (WSVM), Case Based Reasoning (CBR) and AdaBoost algorithm, which possess a huge potential for enhancing the security assessment of power systems are discussed in Chapter 4. The WSVM uses a Morlet wavelet as its new kernel mapping function and the review results revealed that the WSVM exhibits better performance than the other kernel based SVM classifiers like linear SVM, quadratic SVM, polynomial SVM, multi-layer perceptron SVM and radial basis function (Gaussian) SVM for classification problems. Further, to enhance the generalization

capability of CBR and AdaBoost classifiers, a novel weight updation strategy using fuzzy clustering thresholding technique has also been proposed.

Chapter 5 presents the application of various intelligent classifiers with different generalization capability for Static Security Assessment (SSA) of power systems using phasor measurements. This chapter also proposes a new framework that can predict the static security status as well as the type of violations that causes insecurity of power systems. Existing security indices which are used to classify the training patterns into secure or insecure class, suffer from masking and weight allocation problems. Therefore, in this chapter, a composite Security Index (SI), consisting of both the line power flows and the bus voltage limit violations is proposed to classify the training patterns into secure or insecure class. The synchronized measurements such as voltage magnitude and voltage angle of the buses, current and the power flows of the branches measured by the PMUs, form the components of the input training pattern. Then, a statistical approach based on class separability and correlation coefficient indices has been used to select only the most important features, which further reduces the training time and complexity of classifiers. Synthetic Minority Oversampling Technique (SMOTE) has been used to overcome the class imbalance in the input data generated. The proposed approach has been implemented on IEEE 14-bus, IEEE 30-bus and practical Indian 246-bus systems. These results obtained using WSVM, CBR and AdaBoost classifiers are comparatively better than the existing techniques in terms of classification accuracy. Among these three classifier models, WSVM and AdaBoost algorithm have been found to be more suitable for security assessment, since they provide better prediction than the existing classifiers including CBR algorithm.

In Chapter 6, a new approach utilizing the synchronized measurements has been proposed to have an improved monitoring and Transient Security Assessment (TSA) of power systems. For this analysis, the measured rotor angles of the generators are used as inputs to the proposed TSA framework consisting of different classifiers. This TSA framework, which is designed using AdaBoost classifiers accurately predicts the transient security status with a prediction accuracy of about 97.90 % – 99.35 % for the three test systems. In addition to transient security prediction, the proposed approach also determines the synchronism status of the generating units as well as the coherent group of generators. Finally, the proposed approach is implemented and tested on standard benchmark systems such as IEEE 14 bus and IEEE 30 bus systems and on a practical Indian 246 bus network.

7.2 Major Contributions of the Work

This dissertation has the following novel and significant contributions, which are summarized as follows.

- A new intelligent search technique has been developed to optimally place the PMUs for maintaining complete system observability during all operating scenarios viz. normal operation as well as during cascaded failures. The proposed placement method is also incorporated with measurement redundancy to improve the state estimation process.
- A new framework for SSA has been proposed to classify the system security status and the type of violations (bus voltage deviation and line flow overloads) that causes insecurity of power systems.
- Development of a suitable approach for improving the monitoring and assessment of transient security of power systems. In addition to transient security status, the proposed approach can also determine the individual machine synchronism state and the coherent group of generators.
- Applications of different machine learning techniques with better generalization capability for enhancing the overall monitoring and security assessment of power systems.

7.3 Future Scope

As a consequence of this research carried out in this thesis, the following aspects are identified for future research in this area.

- The proposed framework can also be extended to incorporate voltage security monitoring of power systems.
- Investigations can be carried out for the security assessment under multiple line outage, generator outage and various network topology conditions.
- A new approach based on hybrid CBR models can be designed using decision trees, fuzzy algorithms, etc., along-with the CBR classifier to reduce the computation burden of CBR classifiers, while at the same time improving the classification accuracy.
- PMU data-driven framework for classification of faults/events in distribution systems may be developed due to the proliferation of advanced metering devices with high sampling rates.
- This work can be further extended to investigate the impact of external topology errors on security assessment.
- In order to handle streaming big data received from power grid sensors like PMUs, smart meters, etc, a framework can be developed for big data analysis.

References

- [1] T. E. D. Liacco, "The adaptive reliability control system," *IEEE Trans. Power Apparatus & Syst.*, no. 5, pp. 517–531, 1967.
- [2] S. C. Srivastava, A. Velayutham, K. Agrawal, and A. Bakshi, "Report of the Enquiry Committee on Grid Disturbance in Northern Region on 30th July 2012 and in Northern, Eastern & North-eastern Region on 31st July 2012," *Enquiry Committee, New Delhi.*, Aug. 2012.
- [3] L. Pereira, "Cascade to black [system blackouts]," *IEEE Power & Energy Magazine*, vol. 2, no. 3, pp. 54–57, 2004.
- [4] A. G. Phadke, J. S. Thorp, and M. G. Adamiak, "A new measurement technique for tracking voltage phasors, local system frequency, and rate of change of frequency," *IEEE Trans. Power Apparatus & Syst.*, no. 5, pp. 1025–1038, 1983.
- [5] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*, 2008, vol. 1.
- [6] A. Phadke and R. M. de Moraes, "The wide world of wide-area measurement," *IEEE Power & Energy Magazine*, vol. 6, no. 5, 2008.
- [7] S. Skok, I. Ivankovic, and Z. Cerina, "Applications based on pmu technology for improved power system utilization," in *In Proc. IEEE Power Engg. Soc. General Meeting*, 2007, pp. 1–8.
- [8] D. Novosel, V. Madani, B. Bhargave, K. Vu, and J. Cole, "Dawn of the grid synchronization," *IEEE Power & Energy Magazine*, vol. 6, no. 1, pp. 49–60, 2008.
- [9] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.
- [10] A. Ekwue, "A review of automatic contingency selection algorithms for online security analysis," in *In Proc. IEEE Conf. Power Syst. Monitoring & Control*, 1991, pp. 152–155.
- [11] R. Allan and A. Adraktas, "Terminal effects and protection system failures in composite system reliability evaluation," *IEEE Trans. Power Apparatus & Syst.*, no. 12, pp. 4557–4562, 1982.
- [12] R. Billinton and T. Medicherla, "Station originated multiple outages in the reliability analysis of a composite generation and transmission system," *IEEE Trans. Power Apparatus & Syst.*, no. 8, pp. 3870–3878, 1981.

- [13] Q. Chen and J. D. McCalley, "Identifying high risk nk contingencies for online security assessment," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 823–834, 2005.
- [14] A. Phadke, B. Pickett, M. Adamiak, M. Begovic, G. Benmouyal, R. Burnett, T. Cease, J. Goossens, D. Hansen, M. Kezunovic *et al.*, "Synchronized sampling and phasor measurements for relaying and control," *IEEE Trans. Power Del.*, vol. 9, no. 1, pp. 442–452, 1994.
- [15] A. G. Phadke, "Synchronized phasor measurements in power systems," *IEEE Computer Appl. Power*, vol. 6, no. 2, pp. 10–15, 1993.
- [16] L. Breiman, J. Friedman, C. J. Stone, and R. A. Olshen, *Classification and regression trees*. CRC press, 1984.
- [17] L. Wehenkel, "Machine learning approaches to power-system security assessment," *IEEE Expert*, vol. 12, no. 5, pp. 60–72, 1997.
- [18] L. Wehenkel, T. Van Cutsem, and M. Ribbens-Pavella, "An artificial intelligence framework for online transient stability assessment of power systems," *IEEE Trans. Power Syst.*, vol. 4, no. 2, pp. 789–800, 1989.
- [19] L. Wehenkel and M. Pavella, "Decision trees and transient stability of electric power systems," *Int. J. Automatica*, vol. 27, no. 1, pp. 115–134, 1991.
- [20] L. Wehenkel, M. Pavella, E. Euxibie, and B. Heilbronn, "Decision tree based transient stability method a case study," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 459–469, 1994.
- [21] C. Liu, Z. H. Rather, Z. Chen, and C. L. Bak, "An overview of decision tree applied to power systems," *Int. J. Smart Grid & Clean Energy*, vol. 2, no. 3, pp. 413–419, 2013.
- [22] A. Navada, A. N. Ansari, S. Patil, and B. A. Sonkamble, "Overview of use of decision tree algorithms in machine learning," in *In Proc. IEEE Control & Syst. Graduate Res. Colloquium (ICSGRC)*, 2011, pp. 37–42.
- [23] P. K. Simpson, "Fuzzy min-max neural networks. i. classification," *IEEE Trans. Neural Networks*, vol. 3, no. 5, pp. 776–786, 1992.
- [24] D. Niebur and A. J. Germond, "Power system static security assessment using the kohonen neural network classifier," *IEEE Trans. Power Syst.*, vol. 7, no. 2, pp. 865–872, 1992.
- [25] T. Baldwin, L. Mili, M. Boisen Jr, and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Trans. Power Syst.*, vol. 8(2), no. 2, pp. 707–715, 1993.
- [26] R. Sodhi, S. Srivastava, and S. Singh, "Multi-criteria decision-making approach for multi-stage optimal placement of phasor measurement units," *IET Gen. Transm. & Distrib.*, vol. 5, no. 2, pp. 181–190, 2011.
- [27] N. P. Theodorakatos, N. M. Manousakis, and G. N. Korres, "Optimal placement of phasor measurement units with linear and non-linear models," *Electric Power Components & Syst.*, vol. 43, no. 4, pp. 357–373, 2015.

- [28] F. Aminifar, A. Khodaei, M. Fotuhi-Firuzabad, and M. Shahidehpour, "Contingency-constrained PMU placement in power networks," *IEEE Trans. Power Syst.*, vol. 25(1), no. 1, pp. 516–523, 2010.
- [29] O. Gómez and M. A. Ríos, "ILP-based multistage placement of PMUs with dynamic monitoring constraints," *Int. J. Electric. Power & Energy Syst.*, vol. 53, pp. 95–105, 2013.
- [30] X. Tai, D. Marelli, E. Rohr, and M. Fu, "Optimal PMU placement for power system state estimation with random component outages," *Int. J. Electric. Power & Energy Syst.*, vol. 51, pp. 35–42, 2013.
- [31] M. Korkali and A. Abur, "Placement of PMUs with channel limits," in *In Proc. IEEE Power & Energy Soc. General Meeting*, 2009, pp. 1–4.
- [32] E. Abiri, F. Rashidi, T. Niknam, and M. R. Salehi, "Optimal PMU placement method for complete topological observability of power system under various contingencies," *Int. J. Electric. Power & Energy Syst.*, vol. 61, pp. 585–593, 2014.
- [33] F. Rashidi, E. Abiri, T. Niknam, and M. R. Salehi, "Optimal placement of PMUs with limited number of channels for complete topological observability of power systems under various contingencies," *Int. J. Electric. Power & Energy Syst.*, vol. 67, pp. 125–137, 2015.
- [34] F. Marin, F. Garcia-Lagos, G. Joya, and F. Sandoval, "Genetic algorithms for optimal placement of phasor measurement units in electrical networks," *Electronics Letters*, vol. 39, no. 19, pp. 1403–1405, 2003.
- [35] B. Milosevic and M. Begovic, "Nondominated sorting genetic algorithm for optimal phasor measurement placement," *IEEE Trans. Power Syst.*, vol. 18(1), no. 1, pp. 69–75, 2003.
- [36] R. F. Nuqui and A. G. Phadke, "Phasor measurement unit placement techniques for complete and incomplete observability," *IEEE Trans. Power Del.*, vol. 20(4), no. 4, pp. 2381–2388, 2005.
- [37] A. B. Antonio, J. R. Torreao, and M. B. Do Coutto Filho, "Meter placement for power system state estimation using simulated annealing," in *In Proc. IEEE Conf. Power Tech.*, vol. 3, 2001, pp. 1–5.
- [38] J. Peng, Y. Sun, and H. Wang, "Optimal PMU placement for full network observability using Tabu search algorithm," *Int. J. Electric. Power & Energy Syst.*, vol. 28(4), no. 4, pp. 223–231, 2006.
- [39] H. Mori and Y. Sone, "Tabu search based meter placement for topological observability in power system state estimation," in *In Proc. IEEE Conf. Transm. & Distrib.*, vol. 1, 1999, pp. 172–177.
- [40] R. Babu and B. Bhattacharyya, "Optimal allocation of phasor measurement unit for full observability of the connected power network," *Int. J. Electric. Power & Energy Syst.*, vol. 79, pp. 89–97, 2016.

- [41] S. Chakrabarti, G. K. Venayagamoorthy, and E. Kyriakides, "PMU placement for power system observability using binary particle swarm optimization," in *In Proc. IEEE Australasian Universities Power Engg. Conf. (AUPEC)*, 2008, pp. 1–5.
- [42] A. A. Saleh, A. S. Adail, and A. A. Wadoud, "Optimal phasor measurement units placement for full observability of power system using improved particle swarm optimisation," *IET Gen. Transm. & Distrib.*, vol. 11, no. 7, pp. 1794–1800, 2017.
- [43] K. Arul jeyaraj, V. Rajasekaran, S. Nandha Kumar, and K. Chandrasekaran, "A multi-objective placement of phasor measurement units using fuzzified artificial bee colony algorithm, considering system observability and voltage stability," *Int. J. Experimental & Theoretical Artificial Intell.*, vol. 28, no. 1-2, pp. 113–136, 2016.
- [44] B. Ramachandran and G. Thomas Bellarmine, "Improving observability using optimal placement of phasor measurement units," *Int. J. Electric. Power & Energy Syst.*, vol. 56, pp. 55–63, 2014.
- [45] N. M. Manousakis and G. N. Korres, "Optimal pmu placement for numerical observability considering fixed channel capacity semidefinite programming approach," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3328–3329, 2016.
- [46] N. Manousakis and G. Korres, "An advanced measurement placement method for power system observability using semidefinite programming," *IEEE Syst. Journal*, 2017.
- [47] R. Sodhi, S. Srivastava, and S. Singh, "Optimal pmu placement method for complete topological and numerical observability of power system," *Electric Power Syst. Res.*, vol. 80, no. 9, pp. 1154–1159, 2010.
- [48] N. Manousakis and G. Korres, "Optimal allocation of pmus in the presence of conventional measurements considering contingencies," *IEEE Trans. Power Del.*, 2016.
- [49] M. Dehghani, L. Goel, and W. Li, "Pmu based observability reliability evaluation in electric power systems," *Electric Power Syst. Res.*, vol. 116, pp. 347–354, 2014.
- [50] S. Chakrabarti, E. Kyriakides, G. Valverde, and V. Terzija, "State estimation including synchronized measurements," in *In Proc. IEEE Conf. PowerTech.*, 2009, pp. 1–5.
- [51] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including pmu and scada measurements," *Electric Power Syst. Res.*, vol. 81, no. 7, pp. 1514–1524, 2011.
- [52] Z. Huang, K. Schneider, and J. Nieplocha, "Feasibility studies of applying kalman filter techniques to power system dynamic state estimation," in *In Proc. IEEE Conf. Power Engg.*, 2007, pp. 376–382.
- [53] Y. Sun, P. Du, Z. Huang, and et.al., "Pmu placement for dynamic state tracking of power systems," in *In Proc. North American Power Symposium (NAPS)*, 2011, pp. 1–7.
- [54] J. Qi, K. Sun, and W. Kang, "Optimal pmu placement for power system dynamic state estimation by using empirical observability gramian," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2041–2054, 2015.

- [55] J. James, A. Y. Lam, D. J. Hill, and V. O. Li, "A unified framework for wide area measurement system planning," *Int. J. Electric. Power & Energy Syst.*, vol. 96, pp. 43–51, 2018.
- [56] M. B. Mohammadi, R.-A. Hooshmand, and F. H. Fesharaki, "A new approach for optimal placement of pmus and their required communication infrastructure in order to minimize the cost of the wams," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 84–93, 2016.
- [57] J. Aghaei, A. Baharvandi, A. Rabiee, and M.-A. Akbari, "Probabilistic pmu placement in electric power networks: an milp-based multiobjective model," *IEEE Trans. Industrial Inform.*, vol. 11, no. 2, pp. 332–341, 2015.
- [58] J. Qi, K. Sun, and W. Kang, "Optimal pmu placement for power system dynamic state estimation by using empirical observability gramian," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 2041–2054, 2015.
- [59] U. D. of Electricity, "Synchrophasor technologies and their deployment in the recovery act smart grid programs," 2013.
- [60] S. Zhu, L. Wu, S. Mousavian, and J. H. Roh, "An optimal joint placement of pmus and flow measurements for ensuring power system observability under n-2 transmission contingencies," *Int. J. Electric. Power & Energy Syst.*, vol. 95, pp. 254–265, 2018.
- [61] R. Kavasseri and S. K. Srinivasan, "Joint placement of phasor and power flow measurements for observability of power systems," *IEEE Trans. Power Syst.*, vol. 26(4), no. 4, pp. 1929–1936, 2011.
- [62] K. D. Jones, E. B. Cano, H. K. Chen, and et.al., "Strategies for success with synchrophasors: Poised to shine in the eastern region of the united states," *IEEE Power & Energy Magazine*, vol. 13, no. 5, pp. 29–35, 2015.
- [63] S. Samantaray, I. Kamwa, and G. Joos, "Ensemble decision trees for phasor measurement unit-based wide-area security assessment in the operations time frame," *IET Gen. Transm. & Distrib.*, vol. 4, no. 12, pp. 1334–1348, 2010.
- [64] X. Liu, X. Zhang *et al.*, "Distributed voltage security monitoring in large power systems using synchrophasors," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 982–991, 2016.
- [65] R. Diao, K. Sun, V. Vittal, and et.al., "Decision tree-based online voltage security assessment using pmu measurements," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 832–839, 2009.
- [66] A. Tiwari and V. Ajjarapu, "Event identification and contingency assessment for voltage stability via pmu," in *In Proc. North American Power Symposium*, 2007, pp. 413–420.
- [67] A. Iravani, M. Karrari, and S. Karrari, "A suitable dynamic stability index for power systems using pmu data," in *In Proc. IEEE Mediterranean Electrotechnical Conf.*, 2012, pp. 1113–1116.

- [68] J. M. Lim and C. L. DeMarco, "Model-free voltage stability assessments via singular value analysis of pmu data," in *In Proc. Symposium on Bulk Power Syst. Dynamics & Control-IX Optimization, Security & Control of Emerging Power Grid*, 2013, pp. 1–10.
- [69] V. Venkatasubramanian, X. Liu, G. Liu, Q. Zhang, and M. Sherwood, "Overview of wide-area stability monitoring algorithms in power systems using synchrophasors," in *In Proc. IEEE American Control Conf.*, 2011, pp. 4172–4176.
- [70] J. W. Simpson-Porco and F. Bullo, "Distributed monitoring of voltage collapse sensitivity indices," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1979–1988, 2016.
- [71] S. S. Biswas and A. K. Srivastava, "A novel method for distributed real time voltage stability monitoring using synchrophasor measurements," in *In Proc. Symposium on Bulk Power Syst. Dynamics & Control-IX Optimization, Security & Control of Emerging Power Grid*, 2013, pp. 1–6.
- [72] X. Ancheng, L. Ruihuang, L. Mingkai, J. H. Chow, B. Tianshu, Y. Ting, and P. Tianjiao, "On-line voltage stability index based on the voltage equation of transmission lines," *IET Gen. Transm. & Distrib.*, vol. 10, no. 14, pp. 3441–3448, 2016.
- [73] C. D. Vournas, C. Lambrou, and P. Mandoulidis, "Voltage stability monitoring from a transmission bus pmu," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3266–3274, 2017.
- [74] H. Jiang, Y. Zhang, J. J. Zhang, and E. Muljadi, "Pmu-aided voltage security assessment for a wind power plant," in *In Proc. IEEE Power & Energy Soc. General Meeting*, 2015, pp. 1–5.
- [75] N. Hatziargyriou, G. Contaxis, and N. Sideris, "A decision tree method for on-line steady state security assessment," *IEEE Trans. Power Syst.*, vol. 9, no. 2, pp. 1052–1061, 1994.
- [76] Z. Li and W. Wu, "Phasor measurements-aided decision trees for power system security assessment," in *In Proc. IEEE Conf. Information & Computing Sci.*, vol. 1, 2009, pp. 358–361.
- [77] K. Swarup, R. Mastakar, and K. P. Reddy, "Decision tree for steady state security assessment and evaluation of power systems," in *In Proc. IEEE Conf. Intell. Sensing & Information Process.*, 2005, pp. 211–216.
- [78] I. Saeh and A. Khairuddin, "Decision tree for static security assessment classification," in *In Proc. Int. Conf. Future Computer & Communication*, 2009, pp. 681–684.
- [79] I. Genc, R. Diao, V. Vittal, S. Kolluri, and S. Mandal, "Decision tree-based preventive and corrective control applications for dynamic security enhancement in power systems," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1611–1619, 2010.
- [80] R. Diao, V. Vittal, and N. Logic, "Design of a real-time security assessment tool for situational awareness enhancement in modern power systems," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 957–965, 2010.

- [81] M. He, J. Zhang, and V. Vittal, "Robust online dynamic security assessment using adaptive ensemble decision-tree learning," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4089–4098, 2013.
- [82] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wong, "A reliable intelligent system for real-time dynamic security assessment of power systems," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, 2012.
- [83] P. Sekhar and S. Mohanty, "An online power system static security assessment module using multi-layer perceptron and radial basis function network," *Int. J. Electric. Power & Energy Syst.*, vol. 76, pp. 165–173, 2016.
- [84] R. Sunitha, S. K. Kumar, and A. T. Mathew, "Online static security assessment module using artificial neural networks," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4328–4335, 2013.
- [85] C. F. Kucuktezcan and V. I. Genc, "A new dynamic security enhancement method via genetic algorithms integrated with neural network based tools," *Electric Power Syst. Res.*, vol. 83, no. 1, pp. 1–8, 2012.
- [86] R. Sunitha, R. K. Sreerama, and A. T. Mathew, "A composite security index for on-line steady-state security evaluation," *Electric Power Components & Syst.*, vol. 39, no. 1, pp. 1–14, 2011.
- [87] N. Amjady, "Dynamic voltage security assessment by a neural network based method," *Electric Power Syst. Res.*, vol. 66, no. 3, pp. 215–226, 2003.
- [88] S. Singh, L. Srivastava, and J. Sharma, "Fast voltage contingency screening and ranking using cascade neural network," *Electric Power Syst. Res.*, vol. 53, no. 3, pp. 197–205, 2000.
- [89] L. Srivastava, S. Singh, and J. Sharma, "A hybrid neural network model for fast voltage contingency screening and ranking," *Int. J. Electric. Power & Energy Syst.*, vol. 22, no. 1, pp. 35–42, 2000.
- [90] R. Singh and L. Srivastava, "Line flow contingency selection and ranking using cascade neural network," *Int. J. Neurocomputing*, vol. 70, no. 16, pp. 2645–2650, 2007.
- [91] K. Lo, L. Peng, J. Macqueen, A. Ekwue, and D. Cheng, "Fast real power contingency ranking using a counterpropagation network," *IEEE Trans. Power Syst.*, vol. 13, no. 4, pp. 1259–1264, 1998.
- [92] S. Chauhan, "Fast real power contingency ranking using counter propagation network: feature selection by neuro-fuzzy model," *Electric power Syst. Res.*, vol. 73, no. 3, pp. 343–352, 2005.
- [93] M. Pandit, L. Srivastava, and J. Sharma, "Fast voltage contingency selection using fuzzy parallel self-organizing hierarchical neural network," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 657–664, 2003.
- [94] S. Kalyani and K. S. Swarup, "Classification and assessment of power system security using multiclass svm," *IEEE Trans. Syst., Man, & Cybern. C Appl. & Rev.*, vol. 41, no. 5, pp. 753–758, 2011.

- [95] J. Geeganage, U. Annakkage, T. Weekes, and B. A. Archer, "Application of energy-based power system features for dynamic security assessment," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 1957–1965, 2015.
- [96] L. Wehenkel, "Machine learning approaches to power-system security assessment," *IEEE Expert*, vol. 12, no. 5, pp. 60–72, 1997.
- [97] C. Singh, X. Luo, and H. Kim, "Power system adequacy and security calculations using monte carlo simulation incorporating intelligent system methodology," in *In Proc. IEEE Conf. Probabilistic Methods Applied to Power Syst.*, 2006, pp. 1–9.
- [98] L. H. Hassan, M. Moghavvemi, H. A. Almurib, and O. Steinmayer, "Current state of neural networks applications in power system monitoring and control," *Int. J. Electric. Power & Energy Syst.*, vol. 51, pp. 134–144, 2013.
- [99] V. S. S. Vankayala and N. D. Rao, "Artificial neural networks and their applications to power systemsa bibliographical survey," *Electric Power Syst. Res.*, vol. 28, no. 1, pp. 67–79, 1993.
- [100] K. S. Swarup and P. B. Corthis, "Ann approach assesses system security," *IEEE Computer Appl. in Power*, vol. 15, no. 3, pp. 32–38, 2002.
- [101] T. S. Sidhu and L. Cui, "Contingency screening for steady-state security analysis by using fft and artificial neural networks," *IEEE Trans. Power Syst.*, vol. 15, no. 1, pp. 421–426, 2000.
- [102] N. M. Manousakis, G. N. Korres, and P. S. Georgilakis, "Taxonomy of pmu placement methodologies," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 1070–1077, 2012.
- [103] J. London, S. A. R. Piereti, R. Benedito, and N. Bretas, "Redundancy and observability analysis of conventional and pmu measurements," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1629–1630, 2009.
- [104] P. Gopakumar, M. J. B. Reddy, and D. K. Mohanta, "Transmission line fault detection and localisation methodology using pmu measurements," *IET Gen. Transm. & Distrib.*, vol. 9, no. 11, pp. 1033–1042, 2015.
- [105] E. Kumar, *Artificial Intelligence*. I.K.International Pvt Ltd, New Delhi, India, 2008.
- [106] M. Esmaili, K. Gharani, and H. A. Shayanfar, "Redundant observability PMU placement in the presence of flow measurements considering contingencies," *IEEE Trans. Power Syst.*, vol. 28(4), no. 4, pp. 3765–3773, 2013.
- [107] G. F. Luger and W. Stubblefield, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*. Pearson Education, Harlow, UK, 2002.
- [108] D. Dua, S. Dambhare, R. K. Gajbhiye, and S. Soman, "Optimal multistage scheduling of PMU placement: An ILP approach," *IEEE Transactions on Power Delivery*, vol. 23(4), no. 4, pp. 1812–1820, 2008.
- [109] S. Chakrabarti, E. Kyriakides, and D. G. Eliades, "Placement of synchronized measurements for power system observability," *IEEE Transactions on Power Delivery*, vol. 24(1), no. 1, pp. 12–19, 2009.

- [110] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Transactions on Power Systems*, vol. 23(3), no. 3, pp. 1433–1440, 2008.
- [111] B. Xu and A. Abur, "Optimal placement of phasor measurement units for state estimation," *PSERC Final Project Report*, pp. 05–58, 2005.
- [112] A. Enshae, R. A. Hooshmand, and F. H. Fesharaki, "A new method for optimal placement of phasor measurement units to maintain full network observability under various contingencies," *Electric Power Systems Research*, vol. 89, pp. 1–10, 2012.
- [113] R. Sodhi, S. Srivastava, and S. Singh, "Optimal PMU placement to ensure system observability under contingencies," in *In Proc. IEEE Power & Energy Soc. General Meeting*, 2009, pp. 1–6.
- [114] M. R. Aghamohammadi and A. Shahmohammadi, "Intentional islanding using a new algorithm based on ant search mechanism," *Int. J. Elect. Power Energy Syst.*, vol. 35, no. 1, pp. 138–147, 2012.
- [115] F.-S. Pai and S.-J. Huang, "A detection algorithm for islanding-prevention of dispersed consumer-owned storage and generating units," *IEEE Trans. Energy Convers.*, vol. 16, no. 4, pp. 346–351, 2001.
- [116] N. Senroy, G. T. Heydt, and V. Vittal, "Decision tree assisted controlled islanding," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1790–1797, 2006.
- [117] G. Xu, V. Vittal, A. Meklin, and J. E. Thalmann, "Controlled islanding demonstrations on the WECC system," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 334–343, 2011.
- [118] L. Ding, F. M. Gonzalez-Longatt, P. Wall, and V. Terzija, "Two-step spectral clustering controlled islanding algorithm," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 75–84, 2013.
- [119] S. S. Ahmed, N. C. Sarker, A. B. Khairuddin, M. A. Ghani, and H. Ahmad, "A scheme for controlled islanding to prevent subsequent blackout," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 136–143, 2003.
- [120] K. Sun, D.-Z. Zheng, and Q. Lu, "Splitting strategies for islanding operation of large-scale power systems using obdd-based methods," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 912–923, 2003.
- [121] P. Trodden, W. Bukhsh, A. Grothey, and K. McKinnon, "Milp formulation for controlled islanding of power networks," *Int. J. Electric. Power & Energy Syst.*, vol. 45, no. 1, pp. 501–508, 2013.
- [122] S. Nezam-Sarmadi, S. Nouri-Zadeh, A. Ranjbar, and M. Pishvaie, "An islanding algorithm to restore a pmu installed power system," in *In Proc: IEEE Asia-Pacific Power & Energy Engg. Conf. (APPEEC)*, 2010, pp. 1–4.
- [123] B. Pradhan, K. H. Reddy, D. S. Roy, and D. K. Mohanta, "Intentional islanding of electric power systems in a grid computing framework: a graph-theoretic approach," in *In Proc: IEEE Int. Conf. Recent Trends in Information Syst. (ReTIS)*, 2011, pp. 156–160.

REFERENCES

- [124] L. Huang, Y. Sun, J. Xu, W. Gao, J. Zhang, and Z. Wu, "Optimal PMU placement considering controlled islanding of power system," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 742–755, 2014.
- [125] T. Venkatesh and T. Jain, "AdaBoost Classifiers for Phasor Measurements based Security Assessment of Power Systems," *IET Gen. Transm. & Distrib. (in press)*, pp. 1–8, 2018.
- [126] L. Zhang, W. Zhou *et al.*, "Wavelet support vector machine," *IEEE Trans. Syst. Man Cybern. B Cybern.*, vol. 34, no. 1, pp. 34–39, 2004.
- [127] D. Kivanc, G. Li, and H. Liu, "Computationally efficient bandwidth allocation and power control for ofdma," *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1150–1158, 2003.
- [128] J. Zeng and W. Qiao, "Short-term wind power prediction using a wavelet support vector machine," *IEEE Trans. Sustainable Energy*, vol. 3, no. 2, pp. 255–264, 2012.
- [129] A. Widodo and B.-S. Yang, "Wavelet support vector machine for induction machine fault diagnosis based on transient current signal," *Expert Syst. Appl.*, vol. 35, no. 1, pp. 307–316, 2008.
- [130] S.-H. Chen, R. C. Guido, T.-K. Truong, and Y. Chang, "Improved voice activity detection algorithm using wavelet and support vector machine," *Comp. Speech & Language*, vol. 24, no. 3, pp. 531–543, 2010.
- [131] J. Vilhena, H. Vicente, M. R. Martins, J. M. Grañeda, F. Caldeira, R. Gusmão, J. Neves, and J. Neves, "A Case-Based Reasoning View of Thrombophilia Risk," *Int. J. Biomedical Informatics*, vol. 62, pp. 265–275, 2016.
- [132] H. Gómez-Vallejo, B. Uriel-Latorre, M. Sande-Meijide, B. Villamarín-Bello, R. Pavón, F. Fdez-Riverola, and D. Glez-Peña, "A case-based reasoning system for aiding detection and classification of nosocomial infections," *Decision Support Syst.*, vol. 84, pp. 104–116, 2016.
- [133] T. W. Liao, "An investigation of a hybrid CBR method for failure mechanisms identification," *Eng. Appl. Artificial Intell.*, vol. 17, no. 1, pp. 123–134, 2004.
- [134] R. Saraiva, M. Perkusich, L. Silva, H. Almeida, C. Siebra, and A. Perkusich, "Early diagnosis of gastrointestinal cancer by using case-based and rule-based reasoning," *Expert Syst. Appl.*, vol. 61, pp. 192–202, 2016.
- [135] S. Begum, S. Barua, R. Filla, and M. U. Ahmed, "Classification of physiological signals for wheel loader operators using multi-scale entropy analysis and case-based reasoning," *Expert Syst. Appl.*, vol. 41, no. 2, pp. 295–305, 2014.
- [136] M. T. Rezvan, A. Z. Hamadani, and A. Shalbfazadeh, "Case-based reasoning for classification in the mixed data sets employing the compound distance methods," *Eng. Appl. Artificial Intell.*, vol. 26, no. 9, pp. 2001–2009, 2013.
- [137] Y. Shen, J. Colloc, A. Jacquet-Andrieu, and K. Lei, "Emerging medical informatics with case-based reasoning for aiding clinical decision in multi-agent system," *Int. J. biomedical informatics*, vol. 56, pp. 307–317, 2015.

- [138] A. Sene, B. Kamsu-Foguem, and P. Rumeau, "Telemedicine framework using case-based reasoning with evidences," *Comp. Methods and Programs in biomedicine*, vol. 121, no. 1, pp. 21–35, 2015.
- [139] S. K. Biswas, N. Sinha, B. Purakayastha, and L. Marbaniang, "Hybrid expert system using case based reasoning and neural network for classification," *Int. J. Biologically Inspired Cognitive Architectures*, vol. 9, pp. 57–70, 2014.
- [140] W. L. Yeow, R. Mahmud, and R. G. Raj, "An application of case-based reasoning with machine learning for forensic autopsy," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3497–3505, 2014.
- [141] K. H. Im and S. C. Park, "Case-based reasoning and neural network based expert system for personalization," *Expert Syst. Appl.*, vol. 32, no. 1, pp. 77–85, 2007.
- [142] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proc. IEEE Computer Vision and Pattern Recognition Conf.*, 2001, pp. 511–518.
- [143] J. Ruan and J. Yin, "Multi-Pose Face Detection Using Facial Features and AdaBoost Algorithm," in *Proc. IEEE 2nd Int. Work. Computer Sci. and Engg.*, 2009, pp. 31–34.
- [144] M. Yang, J. Crenshaw, B. Augustine, R. Mareachen, and Y. Wu, "Adaboost-based face detection for embedded systems," *Computer Vision and Image Understanding*, vol. 114, no. 11, pp. 1116–1125, 2010.
- [145] C. Shan, S. Gong, and P. W. McOwan, "Facial expression recognition based on local binary patterns: A comprehensive study," *Image and Vision Computing*, vol. 27, no. 6, pp. 803–816, 2009.
- [146] E. Owusu, Y. Zhan, and Q. R. Mao, "A neural-AdaBoost based facial expression recognition system," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3383–3390, 2014.
- [147] P. Ramzi, F. Samadzadegan, and P. Reinartz, "Classification of hyperspectral data using an AdaBoostSVM technique applied on band clusters," *IEEE J. Selected Topics Applied Earth Observations & Remote Sensing*, vol. 7, no. 6, pp. 2066–2079, 2014.
- [148] A. Broggi, E. Cardarelli, S. Cattani, P. Medici, and M. Sabbatelli, "Vehicle Detection for Autonomous Parking using a Soft-Cascade AdaBoost Classifier," in *Proc. IEEE Intelligent Vehicles Conf. and Symp.*, 2014, pp. 912–917.
- [149] H. Doğan and O. Akay, "Using AdaBoost classifiers in a hierarchical framework for classifying surface images of marble slabs," *Expert Syst. Appl.*, vol. 37, no. 12, pp. 8814–8821, 2010.
- [150] T. Chen and S. Lu, "Accurate and Efficient Traffic Sign Detection Using Discriminative Adaboost and Support Vector Regression," *IEEE Trans. Vehicular Techn.*, vol. 65, no. 6, pp. 4006–4015, 2016.
- [151] H. Shao, X. Deng, and F. Cui, "Short-term Wind Speed Forecasting using the Wavelet Decomposition and AdaBoost Technique in Wind Farm of East China," *IET Gen. Transm. & Distrib.*, vol. 10, no. 11, pp. 2585–2592, 2016.

- [152] L. Guo, P.-S. Ge, M.-H. Zhang, L.-H. Li, and Y.-B. Zhao, "Pedestrian detection for intelligent transportation systems combining AdaBoost algorithm and support vector machine," *Expert Syst. Appl.*, vol. 39, no. 4, pp. 4274–4286, 2012.
- [153] W.-C. Cheng and D.-M. Jhan, "A self-constructing cascade classifier with AdaBoost and SVM for pedestriandetection," *Engineering Appl. Artificial Intell.*, vol. 26, no. 3, pp. 1016–1028, 2013.
- [154] M. V. Reddy and R. Sodhi, "A rule-based S-Transform and AdaBoost based approach for power quality assessment," *Electric Power Syst. Res.*, vol. 134, pp. 66–79, 2016.
- [155] J. Wang, X. Xiong, N. Zhou, Z. Li, and W. Wang, "Early warning method for transmission line galloping based on SVM and AdaBoost bi-level classifiers," *IET Gen. Transm. & Distrib.*, vol. 10, no. 14, pp. 3499–3507, 2016.
- [156] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning*, vol. 20, no. 3, pp. 273–297, 1995.
- [157] J. Mercer, "Functions of positive and negative type, and their connection with the theory of integral equations," *Philosophical Trans. Royal Society London. A*, vol. 209, pp. 415–446, 1909.
- [158] Q. Zhang and A. Benveniste, "Wavelet networks," *IEEE Trans. Neural Netw.*, vol. 3, no. 6, pp. 889–898, 1992.
- [159] I. Daubechies, "The wavelet transform, time-frequency localization and signal analysis," *IEEE Trans. Infomation Theory*, vol. 36, no. 5, pp. 961–1005, 1990.
- [160] H. H. Szu, B. A. Telfer, and S. L. Kadambe, "Neural network adaptive wavelets for signal representation and classification," *Int. J. Opt. Engg.*, vol. 31, no. 9, pp. 1907–1916, 1992.
- [161] A. Aamodt and E. Plaza, "Case-based reasoning: Foundational issues, methodological variations, and system approaches," *AI communications*, vol. 7, no. 1, pp. 39–59, 1994.
- [162] N. Patidar and J. Sharma, "Case-Based Reasoning Approach to Voltage Security Assessment of Power Systems," in *Proc. IEEE Int. Conf. Industrial Techn.*, 2006, pp. 2768–2772.
- [163] C.-G. Chang, J.-J. Cui, D.-W. Wang, and K.-Y. Hu, "Research on case adaptation techniques in case-based reasoning," in *Proc. IEEE Int. Conf. Machine Learning Cybern.*, 2004, pp. 2128–2133.
- [164] I. Watson and F. Marir, "Case-based reasoning: A review," *J. Knowledge Eng. Review*, vol. 9, no. 4, pp. 327–354, 1994.
- [165] J. G. Carbonell, R. S. Michalski, and T. M. Mitchell, "An overview of machine learning," *Machine learning*, vol. I, pp. 3–23, 1983.
- [166] K. M. Gupta and A. Montezemi, "Empirical evaluation of retrieval in case-based reasoning systems using modified cosine matching function," *IEEE Trans. Syst. Man Cybern. A Syst. Humans*, vol. 27, no. 5, pp. 601–612, 1997.

- [167] T. Chaira and A. K. Ray, “Fuzzy image processing and applications with matlab,” *CRC Press*, pp. 72–77, 2009.
- [168] J. Kittler and J. Illingworth, “On threshold selection using clustering criteria,” *IEEE Trans. Syst., Man Cyber.*, vol. 15, no. 5, pp. 652–655, 1985.
- [169] Y. Karimi, S. Prasher, R. Patel, and S. Kim, “Application of support vector machine technology for weed and nitrogen stress detection in corn,” *Computers & Electronics in Agriculture*, vol. 51, no. 1-2, pp. 99–109, 2006.
- [170] R. Diao, K. Sun, V. Vittal, R. J. O’Keefe, M. R. Richardson, N. Bhatt, D. Stradford, and S. K. Sarawgi, “Decision Tree-Based Online Voltage Security Assessment Using PMU Measurements,” *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 832–839, 2009.
- [171] R. Diao, V. Vittal, and N. Logic, “Design of a Real-Time Security Assessment Tool for Situational Awareness Enhancement in Modern Power Systems,” *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 957–965, 2010.
- [172] M. He, J. Zhang, and V. Vittal, “Robust online dynamic security assessment using adaptive ensemble decision-tree learning,” *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4089–4098, 2013.
- [173] D. Niebur and A. J. Germond, “Power system static security assessment using the kohonen neural network classifier,” *IEEE Trans. Power Syst.*, vol. 7, no. 2, pp. 865–872, 1992.
- [174] S. Kalyani and K. S. Swarup, “Classification and Assessment of Power System Security Using Multiclass SVM,” *IEEE Trans. Syst. Man Cybern. C Appl. Rev.*, vol. 41, no. 5, pp. 753–758, 2011.
- [175] J. Geeganage, U. Annakkage, T. Weekes, and B. A. Archer, “Application of energy-based power system features for dynamic security assessment,” *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 1957–1965, 2015.
- [176] H. Song and M. Kezunovic, “Static Vulnerability and Security Margin of the Power System,” in *In Proc. IEEE/PES Transm. & Distrib. & Expo.*, 2006, pp. 147–152.
- [177] K. Lo, L. Peng, J. Macqueen, A. Ekwue, and D. Cheng, “Fast real power contingency ranking using a counterpropagation network,” *IEEE Trans. Power Syst.*, vol. 13, no. 4, pp. 1259–1264, 1998.
- [178] L. Lusa and R. Blagus, “Class prediction for high-dimensional class-imbalanced data,” *BMC bioinformatics*, vol. 11, no. 523, pp. 1–17, 2010.
- [179] N. Chawla, K. Bowyer, L. Hall, and W. Kegelmeyer, “SMOTE: synthetic minority over-sampling technique,” *J. Artif. Intell. Res.*, pp. 321–357, 2002.
- [180] R. Sunitha, R. S. Kumar, and A. T. Mathew, “Online Static Security Assessment Module Using Artificial Neural Networks,” *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4328–4335, 2013.

- [181] A. Recioui, B. Benseghier, and H. Khalfallah, "Power System Fault Detection, Classification and Location Using the K-Nearest Neighbors," in *In Proc. IEEE Int. Conf. Electrical Engg.* IEEE, 2015, pp. 1–6.
- [182] N. Amjady and S. Banihashemi, "Transient stability prediction of power systems by a new synchronism status index and hybrid classifier," *IET Gen. Transm. & Distrib.*, vol. 4, no. 4, pp. 509–518, 2010.
- [183] F. Hashiesh, H. E. Mostafa, A.-R. Khatib, I. Helal, and M. M. Mansour, "An intelligent wide area synchrophasor based system for predicting and mitigating transient instabilities," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 645–652, 2012.
- [184] C.-W. Liu, M.-C. Su, S.-S. Tsay, and Y.-J. Wang, "Application of a novel fuzzy neural network to real-time transient stability swings prediction based on synchronized phasor measurements," *IEEE Trans. Power Syst.*, vol. 14, no. 2, pp. 685–692, 1999.
- [185] F. R. Gomez, A. D. Rajapakse, U. D. Annakkage, and I. T. Fernando, "Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1474–1483, 2011.
- [186] S. Rovnyak, S. Kretsinger, J. Thorp, and D. Brown, "Decision trees for real-time transient stability prediction," *IEEE Trans. Power Syst.*, vol. 9, no. 3, pp. 1417–1426, 1994.
- [187] Y. Xu, Z. Dong, K. Meng, R. Zhang, and K. Wong, "Real-time transient stability assessment model using extreme learning machine," *IET Gen. Transm. & Distrib.*, vol. 5, no. 3, pp. 314–322, 2011.
- [188] K. Al-Tallaq and E. Feilat, "Online detection of out-of-step operation based on prony analysis-impedance relaying," in *In Proc. 5th WSEAS Int. Conf. Power Syst. & Electromagnetic Compatibility*, 2005, pp. 55–60.
- [189] E. De Tuglie, S. Iannone, and F. Torelli, "A coherency-based method to increase dynamic security in power systems," *Electr. Power Syst. Res.*, vol. 78, no. 8, pp. 1425–1436, 2008.
- [190] T. Hiyama, "Identification of coherent generators using frequency response," in *IEE Proceedings C (Gen. Transm. & Distrib.)*, vol. 128, no. 5, 1981, pp. 262–268.
- [191] W. Li and A. Bose, "A coherency based rescheduling method for dynamic security," *IEEE Trans. Power Syst.*, vol. 13, no. 3, pp. 810–815, 1998.
- [192] M. Ariff and B. C. Pal, "Coherency identification in interconnected power systeman independent component analysis approach," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1747–1755, 2013.
- [193] H. A. Alsafih and R. Dunn, "Determination of coherent clusters in a multi-machine power system based on wide-area signal measurements," in *In Proc. IEEE Power & Energy Soc. General Meeting*, 2010, pp. 1–8.

REFERENCES

- [194] K. Verma and K. Niazi, "A coherency based generator rescheduling for preventive control of transient stability in power systems," *Electr. Power & Energy Syst.*, vol. 45, pp. 10–18, 2013.
- [195] N. Amjady, "A framework of reliability assessment with consideration effect of transient and voltage stabilities," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 1005–1014, 2004.