Assessment and Enhancement of Power System Security using Soft Computing and Data Mining Approaches

Dissertation submitted to the

National Institute of Technology Rourkela

in partial fulfillment of the requirements

of the degree of

Doctor of Philosophy

in

Electrical Engineering

by

Pudi Sekhar

(Roll Number: 512EE1018)

under the supervision of

Prof. Sanjeeb Mohanty

January, 2016

Department of Electrical Engineering

National Institute of Technology Rourkela

Electrical Engineering
National Institute of Technology Rourkela

Prof./Dr. Sanjeeb Mohanty
Assistant Professor

January 29, 2016

Supervisor's Certificate

This is to certify that the work presented in this dissertation entitled "*Assessment and Enhancement of Power System Security using Soft Computing and Data Mining Approaches" by "Pudi Sekhar"*, Roll Number 512EE1018, is a record of original research carried out by him under my *supervision* and guidance in partial fulfillment of the requirements of the degree of *Doctor of Philosophy* in *Electrical Engineering*. Neither this dissertation nor any part of it has been submitted for any degree or diploma to any institute or university in India or abroad.

Sanjeeb Mohanty

Dedicated

To

My Parents

…Pudi Sekhar

Declaration of Originality

I, Pudi Sekhar, Roll Number 512EE1018 hereby declare that this dissertation entitled *"Assessment and Enhancement of Power System Security using Soft Computing and Data Mining Approaches"* represents my original work carried out as a doctoral student of NIT Rourkela and, to the best of my knowledge, it contains no material previously published or written by another person, nor any material presented for the award of any other degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the section "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

January 29, 2016
NIT Rourkela *Pudi Sekhar*

Acknowledgement

It has been a pleasure for me to work on this dissertation. I hope the reader will find it not only interesting and useful, but also comfortable to read.

The research reported here has been carried out in the **Dept. of Electrical Engineering, National Institute of Technology Rourkela at the Soft computing Laboratory.** I am greatly indebted to many persons for helping me complete this dissertation.

First and foremost, I would like to express my sense of gratitude and indebtedness to my supervisor **Prof. Sanjeeb Mohanty,** Asst. Professor, Department of Electrical Engineering, for his inspiring guidance, encouragement, and untiring effort throughout the course of this work. His timely help and painstaking efforts made it possible to present the work contained in this thesis. I consider myself fortunate to have worked under his guidance. Also, I am indebted to him for providing all official and laboratory facilities.

I am grateful to Director, **Prof. S.K. Sarangi** and **Prof. Jitendriya Kumar Satpathy**, Head of Electrical Engineering Department, National Institute of Technology, Rourkela, for their kind support and concern regarding my academic requirements.

I am grateful to my Doctoral Scrutiny Committee members, **Prof. A. K. Panda**, **Prof. S. Karmakar, Prof. P. K. Ray** and **Prof. A. K. Sahoo,** for their valuable suggestions and comments during this research period. I express my thankfulness to the faculty and staff members of the Electrical Engineering Department for their continuous encouragement and suggestions.

I express my heartfelt thanks to the **International Journal Reviewers** for giving their valuable comments on the published papers in different International Journals, which helps to carry the research work in a right direction. I also thank to the **International Conference Organizers** for intensely reviewing the published papers.

I am especially indebted to my colleagues in the power systems group. First, I would like to thank **Ms. S. Upadhyaya** and **Mr. G. V. Subramanyam**, who helped me in my research work. We shared each other a lot of knowledge in the field of power systems. I would like to thank my seniors **Dr. N. Rajendra Prasad** and **Mr. T. Ramesh,** for their help and support throughout my research work.

I would also like to thank my friends, **Mr. Muralidhar Killi, Mr. Rajendra K Khadanga, Mr. Amit Kumar, Mr. K. Vinay Sagar**, **Mr. S. Shiva Kumar**, **Mr. G. Kiran Kumar** and **Mr. D. Ravi Kumar** for extending their technical and personal support.

I express my deep sense of gratitude and reverence to my beloved Mother **Smt. Vara Lakshmi**, father **Sri. Brahmalinga Swamy,** my sister **Smt. Naga Seshu,** my uncles **Sri. Suri Babu** and **Sri. Ramanajee** who supported and encouraged me all the time, no matter what difficulties I encountered. I would like to express my love and affection on my nephews **Rithvik Durgesh** and **Kashvik simhesh**. I would like to express my greatest admiration to **all my family members** for their positive encouragement that they showered on me throughout this research work. Without my family's sacrifice and support, this research work would not have been possible. It is a great pleasure for me to acknowledge and express my appreciation to all **my well wishers** for their understanding, relentless supports, and encouragement during my research work. Last but not the least, I wish to express my sincere thanks to all those who helped me directly or indirectly at various stages of this work.

This section would remain incomplete without remembering my Grandmother **B. Narayanamma** and Grandfather **P. Narayana murthy,** who left their souls. I would like to express my love and respect for their everlasting affection and support.

Above all, I would like to thank **The Almighty God** for the wisdom and perseverance that he has been bestowed upon me during this research work, and indeed, throughout my life.

January 29, 2016 *Pudi Sekhar*

NIT Rourkela Roll Number: 512EE1018

Abstract

The power system is a complex network with numerous equipment's interconnected for it's reliable operation. These power system networks are forced to operate under highly stressed conditions closer to their limits. One of the key objective of the power system operators is to provide safe, economic and reliable power to it's consumers. However, such network experiences perturbations due to many factors. These perturbations may lead to system collapse or even black out, which impacts the reliability of the system. Thus, one of the major aspect for the secure operation of the system can be achieved through security assessment. In this context, the power system static security assessment is necessary to evaluate the security status under contingency scenario. One of the approach for the security assessment is by contingency ranking, where the severity of a specific contingency is computed and ranked with highest severity to the lowest one. Initially, this approach is implemented using several load flow methods in order to identify the limit violations. However, these approaches are complex, time consuming and not feasible for real time implementation. These approaches are applied to a specific system operating condition. Thus in this context, this thesis focusses to implement soft computing and data mining approaches for security assessment by contingency ranking and classification approach. Along with the security assessment, this thesis also focusses on a control mechanism approach for the security enhancement under contingency scenario using evolutionary computing techniques.

In this thesis, the various aspects of the power system security such as it's assessment, and it's enhancement are studied. The conventional contingency ranking approach by NRLF method is presented for the security assessment. In order to predict the system severity, a ranking module is designed with two neural network models namely, MFNN and RBFN for security assessment under different load conditions. Both neural network models are quite accurate in predicting the performance indices in less time.

Another aspect of power system static security assessment is by classification approach, where the security states are classified into secure, critically secure, insecure and highly insecure. This approach helps in proper security monitoring. Thus, this thesis also presents the design and implementation of two security pattern classifier models namely the decision tree and the random forest classifiers. The classifiers are trained and tested with several security patterns generated in an offline mode. The proposed models are compared with

MLP, RBFN and SVM classifier models in order to prove their efficiency in classifying the security levels.

Further, this thesis work also focusses on a control mechanism for security enhancement under N-1 line outage contingency scenario. Initially contingency analysis is carried out under N-1 line outage case and critical contingencies are identified. The objective is to reschedule the generators with minimum fuel cost in such a way that the overloaded lines are relieved from stress. In order to enhance the power system security, an evolutionary computing algorithm, namely an enhanced cuckoo search algorithm is proposed for the contingency constrained economic load dispatch. To study the robustness and effectiveness of the proposed algorithm, the results are compared with CS, BA and PSO algorithms.

Keywords*: *Artificial Neural Network; Contingency Ranking; Classifier; Decision Tree; Evolutionary Algorithms; Power System Control; Security Assessment; Random Forest.

Contents

List of Figures

List of Tables

Abbreviations

ANN	Artificial Neural Networks
API	Active Power Performance Index
BA	Bat Algorithm
BPA	Back Propagation Algorithm
CA	Classification Accuracy
CART	Classification And Regression Tree
CCELD	Contingency Constrained Economic Load Dispatch
CNN	Cascade Neural Network
CS	Cuckoo Search
DE	Differential Evolution
DT	Decision Tree
ECS	Enhanced Cuckoo Search
EP	Evolutionary Programming
FACTS	Flexible AC Transmission Systems
FCSR	Fixed Centers Selected at Random
FD	Fast Decoupled
GA	Genetic Algorithm
GS	Gauss Seidal
HVDC	High Voltage Direct Current
IEEE	Institute of Electrical and Electronics Engineers
KCL	Kirchhoff's Current Law
LMS	Least Mean Square
LOI	Line Overload Index
MATLAB	Matrix Laboratory
MFNN	Multi-Layer Feedforward Neural Network

MLP	Multi-Layer Perceptron
MR	Misclassification Rate
NR	Newton-Raphson
NRLF	Newton-Raphson Load Flow
OPF	Optimal Power Flow
PC	Personal Computer
PE	Processing Elements
PI	Performance Index
PR	Pattern Recognition
PSSSA	Power System Static Security Assessment
PSO	Particle Swarm Optimization
RAM	Random Access Memory
RBFN	Radial Basis Function Network
RF	Random Forest
RLS	Recursive Least Squares
SC	Soft Computing
SI	Severity Index
SPS	System Protection Schemes
SSA	Static Security Assessment
SSI	Static Severity Index
SVM	Support Vector Machine
UFLS	Under frequency load shedding
UVLS	Under voltage load shedding
VDI	Voltage Deviation Index
VPI	Voltage Performance Index

List of Notations

a	Attribute
a_i, b_i, c_i	Fuel cost coefficients of generator i
C_i	Class label
C_k	Vote of the k^{th} tree to a specific class
D	Dimension of the problem
d_{max}	Maximum distance between the chosen centres
$e_1(m)$	Error at the m^{th} iteration
gn	Generation number
J_1, J_2, J_3, J_4	Jacobian Matrices
k	Number of overloaded transmission lines
L_o	Set of overloaded transmission lines
m	Number of iterations
m_1	Number of chosen centres
n	exponent of penalty function
N_B, N_b	Number of buses in the system
N_L, N_l	Number of transmission lines in the system
N_g	Number of generators
N_h	Number of hidden neurons
N_k	Number of neurons in the output layer
N_i	Number of inputs to the network
N_p	Number of patterns in the training set
NI	Maximum number of iterations
NP	Number of population
n_t	Number of trees
$P_{a\ min}$	Minimum value of the probability

$P_{a\ max}$	Maximum value of the probability
P_D	Total load demand
P_{gi}	Active power output of the generator *i*
P_{gi}^{min}	Minimum limit of the active power of generator *i*
P_{gi}^{max}	Maximum limit of the active power of generator *i*
P_i	Computed real power for bus *i*
P_i^{net}	Specified real power for bus *i*
P_L	System losses
P_l	Active power flow in line *l*
P_l^{max}	MW capacity of line *l*
P_s	Slack bus power
Q_i	Computed reactive power for bus *i*
Q_i^{net}	Specified reactive power for bus *i*
s	Child node
$S_b\,(j)$	Output from the hidden layer
$S_a(i)$	Output from the first layer
S_{pq}	Power flow in branch p-q (MVA)
S_{pq}^{max}	Maximum power flow limit in branch p-q (MVA)
S_{Gp}	Power generation of the p^{th} bus (MVA)
S_l	Apparent Power flow in transmission line
S_l^{max}	Rating of line *l* (MVA)
S_{Lp}	Load of the p^{th} bus (MVA)
T	Set of cases
T_r,*TS*	Training set
T_r^*	Data sample from the training set
$\|V_i\|$	voltage magnitude at bus i
V_i^{sp}	Rated voltage magnitude at bus *i*
ΔV_i^{lim}	Upper and lower voltage limits by regulation

V_i^{min}	Minimum voltage limit at the load bus *i*
V_i^{max}	Maximum voltage limit at the load bus *i*
$\|V_p^{min}\|$	Minimum voltage limit of the p^{th} bus
$\|V_p^{max}\|$	Maximum voltage limit of the p^{th} bus
$\|V_p\|$	Voltage magnitude of the p^{th} bus
W	Real non-negative weighting factor
W_{aj}	Weight between the hidden layer and output layer
X_{best}	Current best solution
$X_{i\ min}$	Minimum value of the problem parameter *i*
$X_{i\ max}$	Maximum value of the problem parameter *i*
X_{1p}	Actual value
X_{2p}	Estimated value after m^{th} iteration
X_1	The input pattern
X_2	The co-ordinates of the centre
$\|\|X_1\text{-}X_2\|\|$	Euclidean distance between X_1 andX_2
$\delta_k(m)$	Error for the k^{th} output at the m^{th} iteration
$\delta_j(m)$	Error for the j^{th} output after the m^{th} iteration
η_1	The learning rate
θ, δ	Voltage angle at a bus
Φ_k	Random vector of the k^{th} tree
α	Step size
α_{min}	Minimum value of the step size
α_{max}	Maximum value of the step size

Chapter 1

Introduction and Literature Survey

1.1 Introduction

Since 1920s, the power system security has gained importance in the planning, design and at the operational stages. The fundamental goal of the power system is to supply uninterrupted, quality power, economically to its consumers. The power system is a complex network, where its security plays a major role for its reliable operation. The power system networks are compelled to operate under stressed operating conditions closer to their stability limits. When such systems experience any perturbation, it will lead to system collapse or even black out, affecting the system security. This raises the reliability issue of the system. Thus, there is a need to develop a powerful and robust online security monitoring system in order to assess the system security level and forewarn the operational engineers to take necessary preventive and control actions. Also, apart from the security monitoring and assessment, there exists the need for necessary control action, such that the system regains the secure state from the insecure one. In this context, it is necessary to develop an efficient and economical control scheme in order to enhance the system security under the contingency scenario.

This chapter is organized as follows: Section 1.2 presents an overview of the power system security, Section 1.3 discuss the concept of security monitoring, assessment and control framework, Section 1.4 explains the theoretical background of security analysis. The Section 1.5 discusses the basic approaches for the security assessment. The Section 1.6 discuss the importance and background of soft computing, whereas, the Section 1.7 presents the explanation of machine learning and data mining. The Section 1.8 explains the literature

survey on the security assessment and the enhancement, whereas Section 1.9 bring out the motivation points for the present work. The dissertation objectives are explained in Section 1.10. Finally, dissertation outline is presented in section 1.11.

1.2 An Overview of Power System Security

With the increasing trend of power demand, the size and complexity of the power system has been increased, which consists of several equipment's such as the generators, the transformers, the transmission lines, the switch gear equipment's etc. The key goal of the operational engineers is to provide reliable power to the consumers without interruption and damage to the consumer appliances. Also, the utility company's goal is economic operation of the power system. But such a power system network is also prone to several perturbations like the transmission line outage, the generator outage, the sudden increase in load demand, the loss of a transformer, etc. which are known as the contingencies. Thus, an important factor in the operation of a power system is the desire to maintain the system security. The system security comprise of practices that are well designed to maintain the system operation when component fails. Apart from the economic operation, the power system must be operationally "secure". An operationally secure system is defined as the one with low probability of system black out. The above aspects need security constrained power system optimization.

From the security point of view, an *outage* can be defined as a temporary suspension of operation. Therefore, the *contingency* is defined as a future event (outage) or circumstance that is possible but cannot be predicted with certainty. The contingency analysis is performed to assess the impact of a contingency on a power system for a specific state. However, the increasing complexity of the modern real time power systems makes the security assessment challenging. For instance, the day-to-day monitoring of a power system requires a quick sensitivity analysis to recognize the parameters influencing the security and the recommendations on control aspect to improve the level of system security [1]. Another influencing factor is the economic and environmental factors, increasing the complexity of the security and the economy, forcing the operators to operate the power system closer to the limits [1]. Usually the security of the system is assessed for severe changes which have high impact of system conditions. Such conditions are usually encountered because of contingencies. These contingencies arises because of the faulty operation of the relay's which

are installed to protect the power system network from faults and abnormal conditions. The faulty operation of the relay may lead to loss of a transmission line, transformer, generator or a primary load. Thus, for the secure operation of the power system, there is a pressing need to monitor the system security to take necessary control actions and to avoid the system from black out. In this context, the security assessment has emerged as a requirement in the operational stage of the power system.

1.2.1 Power System Security: Definition

The *Power system security* is defined as, the ability of the system to withstand unexpected failures (contingencies) and continue to operate without interruption of supply to consumers [2]. The security assessment is the key aspect in the planning and operational stages of a power system. The *security assessment* is also called as the *security evaluation*, which investigates the robustness of the system security level to a set of preselected contingencies in its present or future state.

The *power system security assessment* is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation [3].

1.3 Security Monitoring, Assessment and Control

The *static security* is defined as the ability of the system to reach a steady state within the specified secure region (defined by boundary limits) following a contingency [4].

The power system security can be divided into three key functions that are carried out in an energy control centre.

1) System monitoring: It identifies whether the system operating state is secure or not, based on the real-time system measurements. It provides the power system operators with the latest information of the operating condition of the system, with the change in load and generation.

2) Contingency analysis: The contingency analysis is carried out to study the outage events and alert the operators to any potential overloads or serious voltage violations. This approach

helps the system operational engineers to locate protective operating states in such a way that no single contingency event will generate overloads or voltage violations.

3) Corrective action analysis (Security constrained optimal power flow): This stage includes the necessary control actions in order to restore the system security. If the system experiences serious problem in the event of an outage, it allows the operator to change the operation of the power system. Thus this function cater as preventive and post-contingency control. An example of corrective action is rescheduling of generators which result in change in power flows, which in turn cause a change in loading on overloaded lines. These three security functions helps to maintain the secure operation of the power system.

1.3.1 Power System Operating States

The control strategies alleviating the dangerous phenomena and maintaining the power system in a secure state are primarily based on the classification of the power system operating states [5], which are explained below:

1) Normal: In this state, all the system variables are within the operating limits and no equipment is overloaded. The system is said to be secure, which has the capability to withstand a contingency without violating the system constraints.

2) Alert: In this state, all the system variables are within the operating limits with all the constraints satisfied. But, the system security level is degraded, where a contingency may overload the equipment. This puts the system in an emergency state.

3) Emergency: In this state, some of the system variables violates the operating limits (for ex. overloaded lines, low voltages etc.). If proper control strategies are not followed, the system may advance towards In Extremis.

4) In Extremis: In this state, the cascading spread of the system component outages takes place which leads to partial or complete black out.

5) Restoration: The power system disturbance, based on its nature, can lead the power systems to a blackout or a brownout state. In the blackout state, the entire load is separated from the generators, through either the tripping of the generators or the transmission lines. No load is supplied. In the brownout state, the partial load is supplied through the

transmission network. The blackout state is more severe than the brownout state and requires several stages for restoring it back to the normal operating state. After the disturbance has occurred, the operator tries to bring back the power system to normal operating state through measures known as restorative strategies. In this process the generators and lines which have tripped will be bought back to service through a sequence of steps known as the restorative measures. At this state, the control actions (for ex. energizing of the system or its parts and reconnection and resynchronization of system parts) must be strong and effective in order to bring back to the normal operating state.

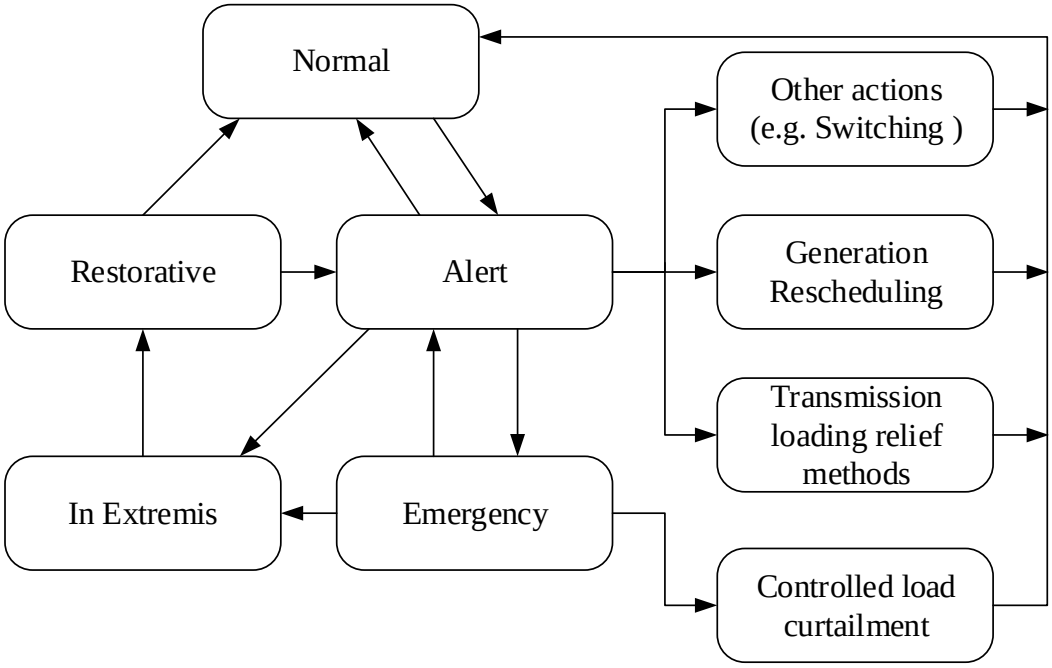

Figure 1.1: Power system security operating states and control actions

The Figure 1.1 shows the associated relations and possible transitions between the operating states and the typical control strategies. With reference to the discussed classification of the operating states, the control strategies or the approaches required to keep the power system secure are generally applied in two distinct stages.

1) Normal and preventive control: This control mechanism is implemented in normal and alert stages. The main goal is to be in the present state or restoration to the normal state.
The typical control actions in this stage are:

- Hierarchical automatic control:
  - Frequency control
  - Voltage control
- Centralized manual control:
  - Contingency screening
  - Operator judgement

The control strategies usually employed are:

- Active power generation rescheduling
- Change of reference points of flow controlling devices such as the FACTS
- Start-up of generating units
- Change of voltage set points of generators and Static VAR compensators
- Switching of shunt elements such as the capacitors and the reactors
- Change of substation configuration

2) Emergency control: This control mechanism is usually implemented in emergency or In Extremis state in order to prevent the momentum of the failures and to restore the system to the normal or the alert state.

The typical control actions in this stage are:

- Protection based systems:
  - Under frequency load shedding (UFLS) schemes
  - Under voltage load shedding (UVLS) schemes
  - System Protection Schemes (SPS)

The emergency control measures may include:

- Tripping of generators
- Fast generation reduction through fast-valving or water diversion
- Fast HVDC power transfer control
- Load shedding
- Controlled opening of interconnection to neighboring systems to prevent spreading of frequency problems
- Controlled islanding of local system into separate areas with matching generation and load

- Blocking of tap changer of transformers
- Insertion of a braking resistor

For the secure operation of the power system, the manual involvement is needed in the form of an operator. In this control action, the key objective is to maintain the system secure under N-1 criteria. Which means that the outage of any one element should not develop any undesirable stress on other system components. In such a case, usually the security assessment is carried out in most power systems. The operator analyzes the result of a possible outage and its impact on other components.

1.4 Security Analysis

The system security can be classified into two major functions that are carried out in an operations control centre.

1) Security assessment: The security assessment provides the security level of the power system for a specific operating condition. The static security level of a power system provides limit violations in its pre-contingency operating state or post-contingency operating states. The power system security assessment is the approach by which any such violations are detected.

Security assessment involves two functions: (i) System monitoring and (ii) Contingency analysis.

In System monitoring, the power system operator will receive the up to date information of the current operating condition of the power system. The next function is the contingency analysis, which plays a crucial role in the security assessment.

Contingency definition: It comprises of a set of possible contingencies that might occur in a power system. The process consists of creating the contingencies list.

Contingency selection: It is the process of selecting severe contingencies from the list that leads to the bus voltage and the power limit violations. Therefore this process minimizes the contingency list by eliminating least severe contingencies. It uses an index calculation in order to find out the severity of the contingencies. In order to check the unacceptable system stress, the use of static methods is sufficient.

Contingency evaluation: In the evaluation stage, all the credible contingencies are ranked in decreasing order of severity.

Thus, the idea behind the contingency analysis is to identify the list of contingencies that may occur, which would disturb the system operating state by violating the operating limits.

2) Security control: In the event of a contingency, security control permits the operator to adjust the power system operation to regain the system security. In this security function, a contingency analysis is carried out along with the combination of optimal power flow. In this process, a change in optimal dispatch of generation is made in such a way that, when a security analysis is carried out, it should not result in violations. Usually, security control objective is accomplished through security constrained optimization program.

However, there is still considerable scope and potential to improve the power system security control. Improved problem formulations, theory, computer solution methods and application techniques are required.

1.5 Approaches for the Static Security Assessment

The assessment of security is performed based on different approaches. The usage of specific approach depends on the requirements of the system security. The widely used approaches for security assessment are 1) contingency ranking approach and 2) classification approach, as shown in Figure 1.2.

In the ranking approach, the contingencies are ranked in descending order based on the severity in order to evaluate the security status. In the classification approach, the system security is either classified into secure or insecure. For the better security evaluation, the classification of the security can be further extended to multi-class such as secure, critically secure, insecure or highly insecure.

In order to evaluate the security by these approaches, it is necessary to compute the stress experienced by the system for a specific contingency which is termed as the severity. The severity is basically computed using the violations of the line flows, the voltages etc. Over the years, the severity is referred with different names such as the performance indices, the composite indices, the overall performance indices, the severity index etc. Though the names appear different, they all compute the severity of the contingencies, but by considering

different violations or by combining two severities. The Table 1.1 shows the indices which are used to compute the severity.

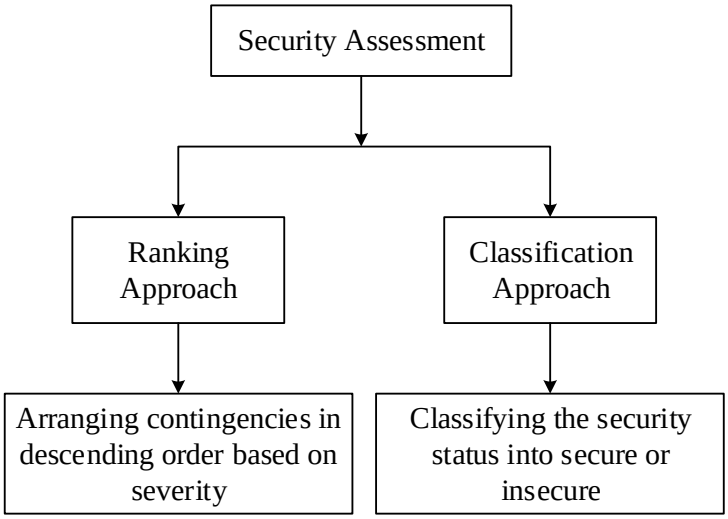

Figure 1.2: Classification of security assessment approaches

Table 1.1: Indices to compute the severity of a contingency

S. No.	Indices	Comment
1.	Active power performance index	This index computes the active power line flow violation
2.	Voltage performance index	This index computes the voltage violations at buses
3.	Composite performance index	This index computes the line flow and voltage violations as a single value
4.	Static Severity index	This index computes the line flow and voltage violations in terms of percentage
5.	Severity Index	This index computes the MVA line flow violations

The literature reveals the indices with the same name but a variation in the formulation in order to compute the severity based on the specific application. The most widely used indices are the active power and the voltage performance indices.

1.6 Soft Computing

Over the years, the soft computing techniques has gained importance because of its applicability in various fields of research, specifically in engineering problems. The SC techniques are useful in solving complex problems, which cannot be achieved by classical numerical methods. In view of its demonstrated quality and strength, SC is still a topic of interest amongst researchers in different fields of science and engineering.

The term "soft computing" [6] was proposed by Lotfi A. Zadeh. According to him, Soft computing is a collection of methodologies that aim to exploit the tolerance for imprecision and uncertainty to achieve tractability, robustness, and low solution cost. Its principal constituents are fuzzy logic, neuro computing and probabilistic reasoning. SC is a combination of strategies intended to model and obtain solutions to real time problems.

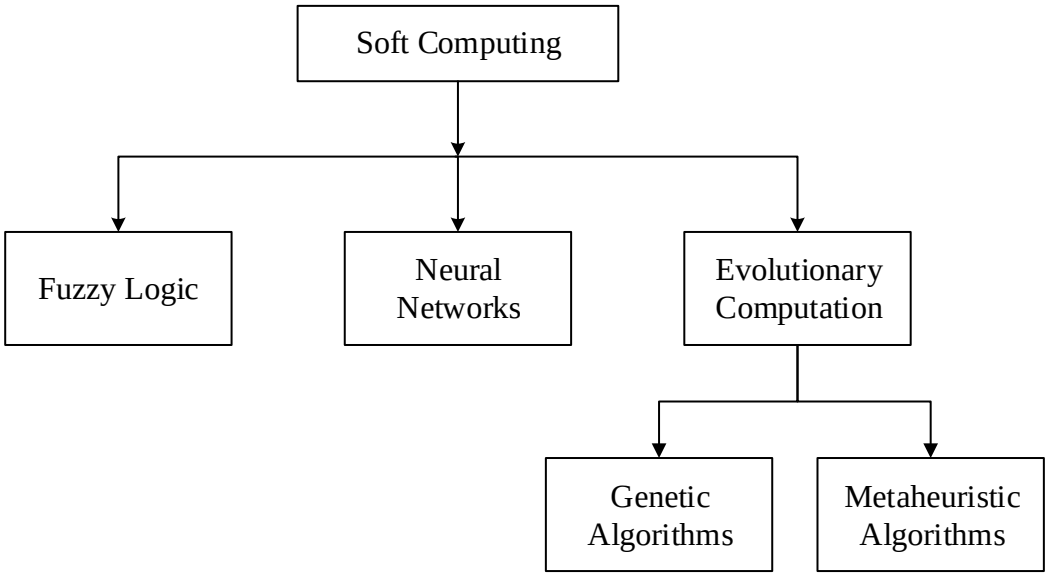

Figure 1.3: Components of Soft Computing

The Figure 1.3 shows the components of soft computing techniques. The SC comprises of definite approach and methodology with a goal to solve real world problems. These issues result from the truth that our world seems to be imprecise, uncertain and difficult to categorize. The key methods of SC include fuzzy logic; neural networks and genetic algorithms. Fuzzy logic is essentially related to imprecision and knowledge representation, whereas neural networks for learning and adaptation and probabilistic reasoning to

uncertainty. These methodologies have the following features:

- Nonlinear
- Capable to deal with non-linearities
- Uses human mind like processing
- self-learning
- Robust in nature

The application of SC techniques is found in many areas such as, signal processing, pattern recognition, quality assurance and industrial inspection, business forecasting, speech processing, credit rating, adaptive process control, robotics control, natural language understanding, etc.

1.7 Machine Learning and Data Mining

Machine learning is a branch of computer science that emerged from the investigation of pattern recognition and computational learning hypothesis in artificial intelligence. Machine learning is defined as, "Field of study that gives computers the ability to learn without being explicitly programmed". A better formal definition [7] is given by T.M Mitchell as "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E".

Machine learning spotlights on the development of system programs, which grow by learning by itself and act accordingly when it experiences an unknown information. The machine learning is a very interesting research field, from which self-driving cars, speech recognition etc. has been developed in the recent years.

Machine learning is broadly classified as:

1) *Supervised learning:* In this method, the system is provided with the sample input data and the corresponding desired outputs. The aim of this approach is to learn the principle of behavior, mapping the input-output sample data.

2) *Unsupervised learning:* In this method, the system needs to learn by itself by discovering the pattern structure in the input data.

3) *Reinforced learning:* In this method, the system is employed in a dynamic conditions to achieve a specific goal, without the help of a teacher.

The machine learning and data mining are very closely related and uses the same methodology. Both approaches search for data patterns, however data mining extract data for human interpretation, whereas, in machine learning, it utilizes the data to develop the system program itself.

- *Machine learning:* It identifies (by learning) the known properties from the training data and focuses on prediction.

- *Data mining:* It focuses on the discovery of unknown properties in the data.

Data mining utilizes various machine learning approaches, with distinct target in mind. Whereas, machine learning utilizes the data mining learning method such as unsupervised learning. Data mining is defined as extracting information or knowledge from the huge data sets. It is also defined as exploration and analysis, by automatic or semi-automatic means, of large quantities of data in order to discover meaningful patterns. Bases on the type of data to be mined, the tasks of data mining are divided into two categories [8]:

1) Prediction Methods
   a. Classification [Predictive]
   b. Regression [Predictive]
   c. Deviation Detection [Predictive]

2) Description Methods: The descriptive function deals with the general properties of data in the database.
   a. Clustering [Descriptive]
   b. Association Rule Discovery [Descriptive]
   c. Sequential Pattern Discovery [Descriptive]

Classification is the procedure of discovering a model that depicts the data classes. The use of this model is to predict the class of attributes whose class label is unknown. The designed model is based on the investigation or analysis carried on the training data set. In this thesis work, the data mining approach is implemented for power system security assessment.

1.8 Review of Literature

In this section, a literature survey corresponding to the power system security assessment and enhancement is presented. In the area of the power system static security assessment, the contingency analysis plays a vital role, the importance of which is discussed in [9, 10]. The contingency analysis gives the security state of the power system under a contingency. In order to perform the contingency analysis, the several load flow methods such as the Gauss-Seidal (GS), the Newton-Raphson (NR) and the fast decoupled (FD) methods [11] were used. These methods are very useful in order to obtain the load flow solutions under the contingency scenario, which aids to compute the system severity. The application of the AC load flow in order to solve the outage cases with respect to the reactive power and voltage magnitudes are discussed in [12-16]. In [17, 18], the accurate methods are proposed in order to calculate the distribution factors based on the decoupled and the Newton-Raphson load flow using network sensitivities. The obtained factors are used to compute the post-outage reactive power flows and the voltage magnitudes following a transmission line or a generator outage.

The AC load flow needs to be solved for each contingency case in order to evaluate the limit violations. However, it is not feasible to perform online, because of the computational barrier. In order to overcome the barrier various approximate methods have been developed. There exists two techniques namely the explicit and the implicit techniques. The explicit methods [l9-24] are the ranking methods, where the contingencies are ranked based on the order of severity using a scalar performance index (PI), which measures the system stress. Higher severity is ranked first and going down the list with the least severity. Whereas, implicit methods use the network solutions in order to recognize the system violations and rank the severity for the various outages [25-31]. A partial system solution approach in [25-27] and an approximate approach in [28, 30], were used to improve the computational speed. The method of concentric relaxation is introduced for the security monitoring. In this approach the system is treated as electrically rigid and gradually relaxed the results to compute the actual flexibility of the transmission. These approaches consider only part of the system network in order to identify the branch flow violations. However, obtaining the voltage violation is very complex. Thus, the authors in [32] have proposed complete bounding method to identify the line flow violations and the voltage violations. This method reduces the number of line flow computations and limits checking. The zero mismatch method [33] is proposed for quick power flow solutions by exploiting the difference in the

convergence rate of individual nodes.

However, an ideal approach for the static security assessment is by contingency ranking. The concept of the contingency ranking was introduced by Ejebe and Wollenberg, in which the contingencies are arranged in descending order by considering the performance index [19]. The majority of the research work in automatic contingency selection focused mostly on implementing algorithms in order to rank the contingencies based on the impact on active power flows [19, 20, 21, 34, 35, 36] and then extending the algorithms to rank the contingencies based on its impact on bus voltages. The selection of the weighting coefficients for the performance indices for contingency ranking has been presented in [37]. A set-theoretic approach is used to obtain the PI, from which the weighting coefficients are obtained. The authors in [38] have discussed the methods available for the contingency screening and ranking for the voltage stability, namely continuation power flow method, multiple load flow method, test function method and V-Q curve fitting method. The combination of the linear sensitivities and the Eigen value analysis for the voltage contingency ranking has been presented in [39] for the voltage stability status under the contingency scenario. The use of an iterative method in order to calculate the Eigen values under outage condition for the contingency ranking is presented in [40]. Yilang chen et al. in [41], have proposed direct ranking method, in which the performance index for a contingency case do not require post contingency voltages at each bus for ranking. In [42] the authors have used the decoupled load flow and the compensation method in order to obtain post outage voltages, and the ranking is given based on performance index. The research in this area has been carried out extensively in the past few years, which includes contingency ranking or screening methods for the security assessment. The most ranking methods are based on the evaluation by means of the performance indices (PI), which is the measure of the system stress. In this approach, the contingencies are ranked based on the severity obtained from network variables and are directly assessed. The static security assessment inspect the severity under post contingency scenario, which includes solving various load flow methods for the base case under N-1 line outage conditions. However, these methods are highly complex and time consuming for online implementation. Also, the system operating conditions vary from time to time, which makes the conventional methods infeasible for real time implementation. Thus, there is a need to develop efficient online tool (which monitor the system security under variable system conditions) for the power system security assessment to ensure safe operation of the power system [43]. The deregulation has compelled the utilities to function their systems closer to their security limits, which demands

quick and efficient approach for security assessment [44].

Conventionally, the contingency ranking approach is performed based on the performance indices (PI) obtained after solving the load flow solutions. However, the accuracy and the speed of the security evaluation depends on the type of methodology used for the ranking approach. Thus in the recent years, the literature revealed the application of the artificial neural networks (ANN) to power system static security assessment, indicate that this is a very promising research field. The importance and the applicability of the neural networks for the power system security assessment and control are discussed by the authors in [45-48]. The computation speed and generalization capability of ANN makes it feasible for the modern power systems for the security monitoring [49]. The combination of ANN and divergence algorithm for the feature selection have been used for security assessment in [50]. The authors in [51-53] have investigated a cascade neural network (CNN), in which the filter and the ranking module are incorporated with a forward network, for quick line flow contingency screening and ranking. In [54, 55], the authors have investigated the application of pattern recognition technique with forward only counter propagation network for the active power contingency ranking. A parallel self-organizing hierarchical neural network is investigated in [56, 57] for the voltage contingency ranking. In this approach, the loadability margin to voltage collapse has been used to rank the contingencies. The efficient performance of the ANN is observed because of the suitable selection of training features which covers the entire operating states of the power system.

Another aspect of static security assessment is by classification approach. For the security evaluation, the authors in [58] have used the kohonen neural network classifier in order to classify the power system operating states. The classifier maps an N-dimensional vector space to a two dimensional neural net in a nonlinear fashion, maintaining the topological order of the input vectors. Thus, the secure operating point vectors inside the boundaries of the secure domain, are mapped to a different region of the neural map than insecure operating points. However, the use of pattern recognition techniques has gained importance for the power system security evaluation [59]. The authors in [59], have proposed the combination of pattern recognition and ANN for the power system security assessment through classification approach. There exists several algorithms (linear programming, least squares etc.,) to design a classifier, however they suffer from poor classification accuracy and high misclassification rate.

As discussed in the previous sections, the key stages of the security includes monitoring,

assessment and the control actions. The security assessment is the task of ascertaining whether the system operating under normal condition can withstand the contingencies (outage of transmission lines, generators etc.) or not without violating the operating limits. If the current operating state is found insecure under contingency, then necessary control steps must be taken in order to avoid limit violation. In such a case, re-routing of power flows will relieve the transmission lines from overload. The authors in [60] have used the linearized relationship between power flows in the overloaded transmission lines and the generated power in order to reschedule the power generation. An efficient straight forward algorithm has been modeled in [61] in order to reduce the moderate overloaded lines by automatic rearrangement of the generator outputs. In order to relieve the overload, the authors in [62] have proposed the concept of fuzzy-set-theory- based approach for active power generation rescheduling. Here, the overloading of lines and the sensitivity of controlling variables are translated into fuzzy set notations in order to formulate the relation between the overloading of line and the controlling ability of generation scheduling. Further, the optimization techniques have been developed in order to obtain the solution of optimal power flow (OPF) problem, such as the gradient method [63], the newton method [64], the decoupling technique [65] and the interior point method [66]. However, the gradient method has poor convergence characteristics, whereas the Newton method is bounded to continuity of the problem definition and constraints. The interior point method is time consuming and converges to local optima. Thus, these methods suffers from several drawbacks in order to obtain the OPF solution.

In view of the drawbacks of the classical methods, the research has focused on the application of evolutionary programming (EP) [67], genetic algorithm (GA) [68, 69], particle swarm optimization (PSO) [70], differential evolution (DE) [71] and many other meta-heuristic algorithms to solve the OPF problem. From these literatures, it can be the observed that the heuristic search algorithms are well-suited to solve the OPF problem. However, research has also revealed the premature convergence of some of these algorithms, which reduces the performance of these algorithms. To improve the performance, the modification of some parameters of these existing algorithms were implemented. However, the several new heuristic search algorithms are also developed in order to solve the drawbacks. Thus, the heuristic search algorithms are well- suited for solving the OPF problem and can also be extended for the application under contingency scenario for the security enhancement.

A phase shifter based OPF for the security enhancement by alleviating the line over load is proposed by the authors in [72]. The ranking of phase shifter locations is conducted based

on the contingency analysis and the sensitivity analysis. The best phase shifter sites are identified and selected into a rule-based system accordingly. Devaraj et al have introduced the genetic algorithm (GA) concept for the OPF based security enhancement [73]. In this, approach, the overloaded lines are alleviated by generator rescheduling and regulation of phase shifting transformer. The GA algorithm is used to obtain the optimal values of generator active-power output and the angle of the phase-shifting transformer. The locations of the phase shifters are selected based on the sensitivity analysis. The evolutionary programming (EP) and the PSO algorithms are applied to security constrained economic load dispatch in [74, 75]. However, though PSO has certain advantages it also suffers from several drawbacks as discussed in [76].

From the above research background, it is observed that for security assessment ANN methods have advantage when compared to classical method. Thus, there is a scope for modeling neural networks for the prediction of severity of a contingency for security assessment by contingency ranking approach. Further, for classification based assessment, it is necessary to design a security pattern classifier system with high classification accuracy and least misclassification rate. Similarly, the literature review for the control mechanism shows the use of many meta-heuristic algorithms for the optimal power flow and the generation rescheduling. But the important aspect comes into picture in the control scenario is the cost incurred to perform the task by considering security aspect. This factor motivated to develop an efficient algorithm, which can reschedule the generators with minimum fuel cost, considering its security aspect under contingency scenario.

1.9 Motivation

The power system is a complex network which consists of several equipment, namely the transmission lines, the generators, the transformers etc. A power system network is said to be reliable, if it supplies quality power to consumers without interruption. Any disturbance will influence the system condition affecting the power supply or even damage the consumer appliances. Thus, the power system security has become a major concern for the operational engineers.

The conventional method of security assessment involves solving the set of nonlinear load flow equations. But the complexity and computation time makes them infeasible for real time security assessment of large power system networks. However, the accuracy and the

speed of the security evaluation depends on the type of methodology used for the ranking approach. This necessitates the need for an efficient approach to assess the security status in short period of time. Thus it is necessary to design an effective security assessment model. This factor motivated to design a quick and efficient model that predict the system severity for the power system security assessment by contingency ranking approach. Further, an attempt was made to use pattern recognition technique for the security assessment problem by classification approach, but the drawback is the design of a powerful pattern recognition system with good input features and classifier model. These factors motivated in search of the quick and efficient pattern classifier techniques with high classification accuracy for the power system security assessment through the classification approach.

Further, the power system security not only includes the assessment part, but also the control strategy as discussed in previous sections. From the literature survey it is observed that generation rescheduling in one of the control strategy for security enhancement. Research shows the application of several meta-heuristic algorithms to perform the economic load dispatch. However, the key factor in scheduling the generators is the fuel cost incurred in the approach. The objective of security enhancement by rescheduling the generators with minimum fuel cost can be achieved with the design of an efficient algorithm. This factor motivated to develop an efficient algorithm for contingency constrained economic load dispatch for security enhancement.

From the above discussion, it is clear that for the security assessment and the enhancement, there is a need and scope to develop fast and efficient algorithmic techniques. The application of different algorithmic techniques for solving different aspects of power system security is the main source of motivation for the present work. In this context, the following contributions are made in this thesis.

1.10 Research Objectives and Scope

From the preceding discussion, the dissertation objective are as follows:

- To explore the contingency ranking approach using the conventional Newton-Raphson load flow analysis.
- To design and implement the neural network models, in order to predict the system

severity for the security assessment by contingency ranking approach.

- To design and implement efficient pattern classifier system for the security assessment by classification approach.
- To develop and implement an efficient algorithm for the contingency constrained economic load dispatch for security enhancement.

The scope of the present work is limited to static security assessment and security enhancement, performed using different severity indices for each approach. The list of contingency factors considered for the simulation study in the present work involves change in load condition and N-1 single line outages.

1.11 Dissertation Outline

The remaining chapters of this thesis are organized as follows:

The chapter 2 gives an overview of the Newton-Raphson load flow method, which is used for the contingency analysis. In this chapter, the security assessment by contingency ranking approach is presented by considering two performance indices in order to compute the severity of the specific contingency under the base load and variable load condition. Then the contingencies are ranked to assess the system security. The results obtained in this chapter are used to validate and compare the prediction results obtained from the neural network models in chapter-3.

The chapter 3 presents the design of ranking module using multi-layer feedforward neural network and radial basis function network for security assessment. The two neural network models are designed and trained for different operating conditions to predict the performance indices. In the testing phase, the two neural network models are provided with the same input data set, which was used to carry out the NRLF based contingency ranking in chapter 2. To study the accuracy of the models, the results obtained using MFNN and RBFN models are compared with the results obtained by NRLF based ranking approach.

The chapter 4 presents the design and the application of the data mining technique known as the decision tree classifier for security assessment by classification approach. The static severity index is used to compute the severity of the contingency. The severity is designed as

a multiclass security problem, by assigning the severity into four security states. The decision tree is trained and tested for different operating conditions in order to classify the security patterns for security evaluation. The efficiency of the DT classifier is compared with multilayer perceptron, radial basis function and support vector machine classifier models.

The chapter 5 presents the design and application of the data mining technique known as the random forest classifier model for the security assessment by the classification approach. The RF model is the extended version of the DT, in which the performance is improved by using multiple decision trees. The RF is trained and tested for different operating conditions in order to classify the security status for the security evaluation. The efficiency of the proposed RF classifier is compared with the DT, the MLP, the RBF and SVM classifier models.

The chapter 6 has focused on the control strategy in order to minimize the severity of the system under N-1 line outage contingency. This chapter presents the design and implementation of enhanced cuckoo search algorithm for the contingency constrained economic load dispatch. The contingency analysis is carried out in order to obtain the critical contingencies identified using the severity index, which computes the severity of the overloaded transmission lines. Thus, the ECS algorithm is implemented in order to reschedule the generators with minimum fuel cost such that the severity is minimized. In order to identify the efficiency of the proposed ECS algorithm, the results obtained are compared with the cuckoo search (CS), the particle swarm optimization (PSO) and the Bat algorithm (BA).

Finally, the chapter 7 presents the conclusions and scope for future work. This chapter summarizes the entire work done and concludes the present study. It explains the effectiveness and robustness of the approaches presented in this thesis. Further, possible suggestions are made for future research.

Chapter 2

Contingency Ranking Approach for Power System Security Assessment using NRLF Method

2.1 Introduction

In chapter 1, the overview of power system security is discussed. It presents the different stages and approaches for the power system security assessment and control. It has also focused on different indices used to compute the system stress. A brief introduction to soft computing and machine learning techniques is also explained in chapter 1. Further, a detailed literature review is discussed.

As discussed in chapter 1, one of the approach for the security assessment is by contingency ranking. Thus, the chapter 2 presents the contingency ranking approach for the power system static security assessment using Newton-Raphson load flow method. In this approach, two performance indices namely, the active power performance index and the voltage performance index are used to obtain the system stress under N-1 line outage contingency. To obtain the system parameters, NRLF analysis is performed under N-1 line outage contingency scenario. The obtained system parameters are used to compute the system severity. Based on the severity, the contingencies are ranked in descending order to analyze the system security. The approach is investigated on the standard IEEE-30 and IEEE-57 bus test system in MATLAB environment. The simulation results demonstrate the

contingency ranking approach for security assessment.

This chapter is organized as follows: Section 2.2 presents the basic idea of contingency ranking approach, Section 2.3 explains the Newton-Raphson load flow method for contingency analysis. The Section 2.4 presents the performance indices used to obtain the system severity under contingency scenario and Section 2.5 presents the algorithmic steps involved for contingency ranking. Whereas, Section 2.6 presents the simulation results and discussion. Finally in section 2.7, the concluding remarks are provided.

2.2 Contingency Ranking Approach

The power system static security can be analyzed by ranking the contingencies based on the contingency severity. The ranking method involves solving the full ac load flow to obtain the system parameters. The contingency analysis involves the simulation of the individual N-1 line outage contingency for the power system model. In order to make the analysis easier, it consists of three basic steps:

Contingency creation: It comprises of a set of possible contingencies that might occur in a power system. The process consists of creating the contingencies list.

Contingency selection: It is the process of selecting severe contingencies from the list that leads to the bus voltage and the power limit violations. Therefore this process minimizes the contingency list by eliminating least severe contingencies. It uses the index calculation to find out the severity of the contingencies.

Contingency evaluation: It involves the necessary security actions needed to be taken or necessary control action in order to mitigate the effect of the contingency.

Thus one of the major tasks of the power system planning and the operational engineers is to study the effect of the outages in terms of their severity for security assessment. The contingency ranking approach utilizes the performance indices (PI) to quantify the severity. In order to obtain the system parameters under contingency case, Newton-Raphson load flow method [8] is used. The NRLF method is also used in chapter-2 to chapter-6 for contingency analysis and to generate security patterns. Thus, the NRLF method is explained in section 2.3.

2.3 NRLF Method for Contingency Analysis

The Figure 2.1 shows the typical bus of a power system. The relation between voltage and current is obtained by the application of KCL to this bus.

$$I_i = V_i \sum_{j=0}^{n} y_{ij} - \sum_{j=1}^{n} y_{ij} V_j \qquad j \neq i \tag{2.1}$$

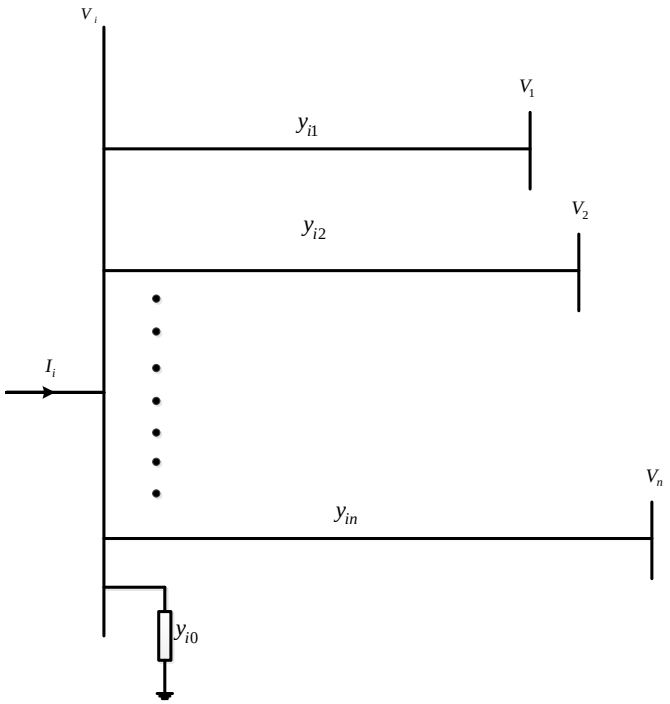

Figure 2.1: A typical bus of the power system

The real and reactive power at bus *i* is given by the equation (2.2)

$$P_i + jQ_i = V_i I_i^* \tag{2.2}$$

$$I_i = \frac{P_i + jQ_i}{V_i^*} \tag{2.3}$$

Substituting I_i in (2.1) will yield,

$$\frac{P_i + jQ_i}{V_i^*} = V_i \sum_{j=0}^{n} y_{ij} - \sum_{j=1}^{n} y_{ij} V_j \qquad j \neq i \tag{2.4}$$

From equation (2.4), a power flow problem is formulated, which results in a set of nonlinear equations, which is solved by using iterative technique known as Newton-Raphson method. The quadratic convergence nature of the Newton-Raphson method is computationally superior and it has minimum divergence characteristics. Thus, the NR method is found to be more efficient and practical for large power systems. Thus for the contingency analysis NR method is used, which is explained below.

The bus admittance matrix is given by the equation (2.5).

$$I_i = \sum_{j=1}^{n} Y_{ij} V_j \tag{2.5}$$

Representing the equation (2.5) in polar form,

$$I_i = \sum_{j=1}^{n} |Y_{ij}||V_j| \underline{\theta_{ij}} + \delta_j \tag{2.6}$$

The complex power at bus *i* is given by,

$$P_i - jQ_i = V_i^* I_i \tag{2.7}$$

Substituting equation (2.6) in (2.7),

$$P_i - jQ_i = |V_i| \underline{-\delta_i} \sum_{j=1}^{n} |Y_{ij}||V_{ij}| \underline{\theta_{ij}} + \delta_j \tag{2.8}$$

The real and imaginary parts of the equation (2.8) is given as,

$$P_i = \sum_{j=1}^{n} |V_i||V_j||Y_{ij}| \cos\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.9}$$

$$Q_i = -\sum_{j=1}^{n} |V_i||V_j||Y_{ij}| \sin\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.10}$$

Equations (2.9) and (2.10) form a set of nonlinear algebraic equations in terms of independent variables. Here, two equations for each load bus given by equations (2.9) and (2.10), and one equation for each voltage-controlled bus given by equation (2.9). Expanding equations (2.9) and (2.10) in Taylor's series, results in set of linear equations as given below.

$$\begin{pmatrix} \Delta P_2^{(k)} \\ \vdots \\ \Delta P_n^{(k)} \\ \Delta Q_2^{(k)} \\ \vdots \\ \Delta Q_n^{(k)} \end{pmatrix} = \left(\begin{array}{ccc|ccc} \frac{\partial P_2^{(k)}}{\partial \delta_2} & \cdots & \frac{\partial P_2^{(k)}}{\partial \delta_n} & \frac{\partial P_2^{(k)}}{\partial |V_2|} & \cdots & \frac{\partial P_2^{(k)}}{\partial |V_n|} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial P_n^{(k)}}{\partial \delta_2} & \cdots & \frac{\partial P_n^{(k)}}{\partial \delta_n} & \frac{\partial P_n^{(k)}}{\partial |V_2|} & \cdots & \frac{\partial P_n^{(k)}}{\partial |V_n|} \\ \hline \frac{\partial Q_2^{(k)}}{\partial \delta_2} & \cdots & \frac{\partial Q_2^{(k)}}{\partial \delta_n} & \frac{\partial Q_2^{(k)}}{\partial |V_2|} & \cdots & \frac{\partial Q_2^{(k)}}{\partial |V_n|} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial Q_n^{(k)}}{\partial \delta_2} & \cdots & \frac{\partial Q_n^{(k)}}{\partial \delta_n} & \frac{\partial Q_n^{(k)}}{\partial |V_2|} & \cdots & \frac{\partial Q_n^{(k)}}{\partial |V_n|} \end{array}\right) \begin{pmatrix} \Delta \delta_2^{(k)} \\ \vdots \\ \Delta \delta_n^{(k)} \\ \Delta |V_2^{(k)}| \\ \vdots \\ \Delta |V_n^{(k)}| \end{pmatrix} \tag{2.11}$$

The Jacobian matrix gives the linearized relationship between small changes in the voltage angle $\Delta\delta_i^{(k)}$ and voltage magnitude $\Delta|V_i^{(k)}|$ with the small changes in real and reactive power $\Delta P_i^{(k)}$ and $\Delta Q_i^{(k)}$. The equation (2.11) can be written in short form as given in equation (2.12).

$$\begin{pmatrix} \Delta P \\ \Delta Q \end{pmatrix} = \begin{pmatrix} J_1 & J_2 \\ J_3 & J_4 \end{pmatrix} \begin{pmatrix} \Delta \delta \\ \Delta |V| \end{pmatrix} \tag{2.12}$$

The diagonal and off diagonal elements of J_1 are

$$\frac{\partial P_i}{\partial \delta_i} = \sum_{j \neq i} |V_i||V_j||Y_{ij}| \sin\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.13}$$

$$\frac{\partial P_i}{\partial \delta_j} = -|V_i||V_j||Y_{ij}| \sin\left(\theta_{ij} - \delta_i + \delta_j\right) \quad j \neq i \tag{2.14}$$

The diagonal and off diagonal elements of J_2 are

$$\frac{\partial P_i}{\partial |V_i|} = 2|V_i||Y_{ii}|\cos\theta_{ii} + \sum_{j\neq i}|V_j||Y_{ij}|\cos\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.15}$$

$$\frac{\partial P_i}{\partial |V_j|} = |V_i||Y_{ij}|\cos\left(\theta_{ij} - \delta_i + \delta_j\right) \quad j \neq i \tag{2.16}$$

The diagonal and off diagonal elements of J_3 are

$$\frac{\partial Q_i}{\partial \delta_i} = \sum_{j\neq i}|V_i||V_j||Y_{ij}|\cos\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.17}$$

$$\frac{\partial Q_i}{\partial \delta_j} = -|V_i||V_j||Y_{ij}|\cos\left(\theta_{ij} - \delta_i + \delta_j\right) \quad j \neq i \tag{2.18}$$

The diagonal and off diagonal elements of J_4 are

$$\frac{\partial Q_i}{\partial |V_i|} = -2|V_i||Y_{ii}|\sin\theta_{ii} - \sum_{j\neq i}|V_j||Y_{ij}|\sin\left(\theta_{ij} - \delta_i + \delta_j\right) \tag{2.19}$$

$$\frac{\partial Q_i}{\partial |V_j|} = -|V_i||Y_{ij}|\sin\left(\theta_{ij} - \delta_i + \delta_j\right) \quad j \neq i \tag{2.20}$$

The terms $\Delta P_i^{(k)}$ and $\Delta Q_i^{(k)}$ are the difference between the scheduled and calculated values, known as power residuals, given by

$$\Delta P_i^{(k)} = P_i^{sch} - P_i^{(k)} \tag{2.21}$$

$$\Delta Q_i^{(k)} = Q_i^{sch} - Q_i^{(k)} \tag{2.22}$$

The new estimates for bus voltages are

$$\delta_i^{(k+1)} = \delta_i^{(k)} + \Delta\delta_i^{(k)} \tag{2.23}$$

$$|V_i^{(k+1)}| = |V_i^{(k)}| + |\Delta V_i^{(k)}| \tag{2.24}$$

The procedure for power flow solution by Newton-Raphson method is as follows:

1) For load buses, P_i^{sch} and Q_i^{sch} are specified. Whereas voltage magnitudes and phase angles are set equal to the slack bus values, or $\left|V_i^{(0)}\right|$ =1.0 and $\delta_i^{(0)}$=0. For voltage-regulated buses, where, $\left|V_i\right|$ and P_i^{sch} are specified, phase angles are set to the slack bus angle or $\delta_i^{(0)}$=0.

2) For load buses, $P_i^{(k)}$ and $Q_i^{(k)}$ are calculated from (2.9) and (2.10) and $\Delta P_i^{(k)}$ and $\Delta Q_i^{(k)}$ are calculated from (2.21) and (2.22).

3) For voltage-controlled buses, $P_i^{(k)}$ and $Q_i^{(k)}$ are calculated from (2.9) and (2.21).

4) The elements of the Jacobian matrix (J_1, J_2, J_3 and J_4) are calculated from (2.13)-(2.20).

5) The linear simultaneous equation (2.12) is solved directly by optimally ordered triangular factorization and Gaussian elimination.

6) The new voltage magnitudes and phase angles are computed from (2.23) and (2.24)

7) The process is continued until the residuals $\Delta P_i^{(k)}$ and $\Delta Q_i^{(k)}$ is less than the specified accuracy.

$$\left|\Delta P_i^{(k)}\right| \le \varepsilon \tag{2.25}$$

$$\left|\Delta Q_i^{(k)}\right| \le \varepsilon \tag{2.26}$$

The above approach is used for contingency analysis under N-1 line outage contingency scenario.

2.4 Performance Indices for the Contingency Analysis

In this work, to assess the system security, two performance indices are used which defines the system stress (severity) in terms of active power and voltage limit violations. The performance indices which are used to obtain the contingency severity are:

Active Power performance index (PI_P): This is the index which determines the extent of line over loading which is given by equation (2.27).

$$PI_P = \sum_{l=1}^{N_L} \left(\frac{W}{2n} \right) \left(\frac{P_l}{P_l^{\max}} \right)^{2n} \tag{2.27}$$

Voltage performance index (PI_V): This is the index which determines the extent of bus voltage limit violations which is given by equation (2.28).

$$PI_V = \sum_{i=1}^{N_B} \left(\frac{W}{2n} \right) \left(\frac{\left(|V_i| - |V_i^{sp}| \right)}{\Delta V_i^{\lim}} \right) \tag{2.28}$$

Here, the minimum and maximum voltage limits are taken as, V_{min}=0.95 pu and V_{max}=1.05 pu. Greater the value of the indices, higher the system insecure. Thus, when assessing security, higher value of index is given first priority in contingency ranking. The system parameters are obtained by performing load flow solution under N-1 line outage contingency.

2.5 Power System Contingency Ranking Algorithm

The contingency ranking approach using the NRLF method is explained in the following algorithm.

Step-1: Read the system bus data and line data
Step-2: Perform the load flow analysis for the base case without contingency
Step-3: Simulate N-1 line outage and proceed to next step
Step-4: Perform load flow analysis for the outage, calculate the active power flow and P^{max}
Step-5: Find the active power performance index (PI_P) using equation (2.27), which gives the active power limit violation
Step-6: Following the contingency, calculate the voltages of all the load buses.
Step-7: Calculate the voltage performance index (PI_V) using equation (2.28), which gives the voltage limit violation at all the load buses due to contingency
Step-8: Repeat steps 3 to 7 for all the transmission lines
Step-9: The contingencies are ranked based on the severity of the contingency.

The flow chart for the contingency ranking approach is shown in Figure 2.2. Once the ranking is achieved, it is easy to analyze the outage severity and necessary control actions

need to be taken to avoid system blackout.

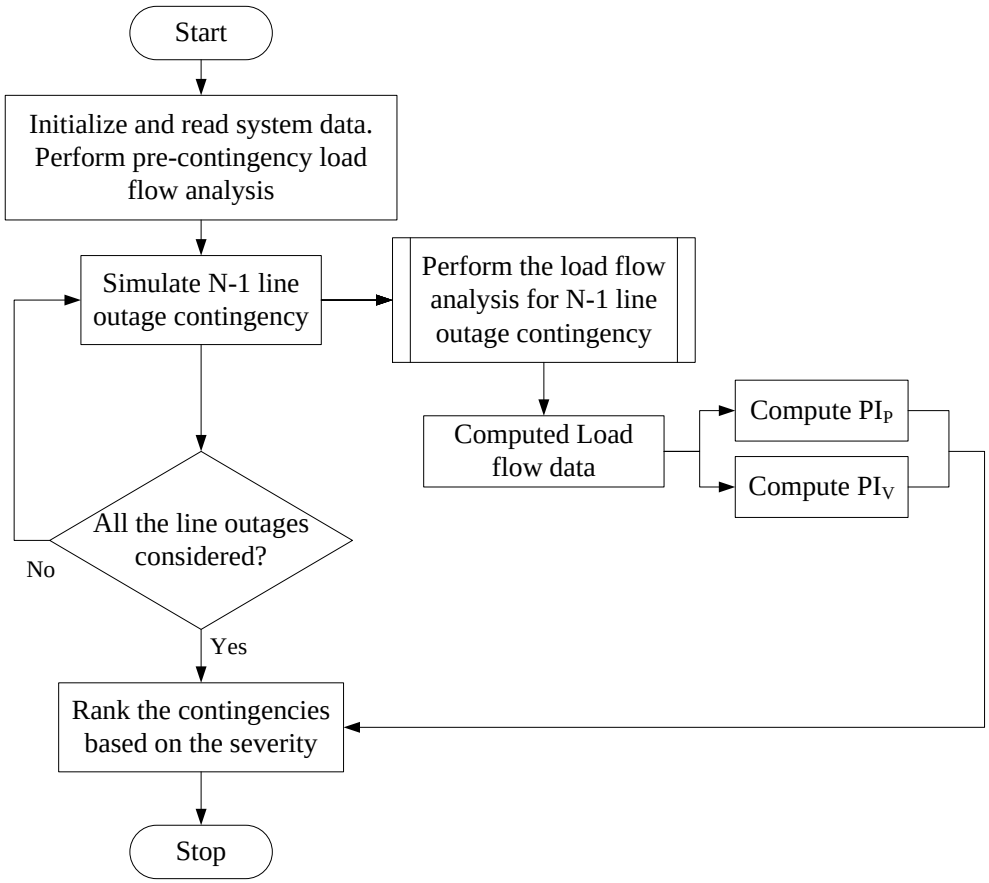

Figure 2.2: Flow chart for the power system contingency ranking using the NRLF method

2.6 Simulation Results and Discussion

In order to investigate the contingency ranking approach, a standard IEEE 30-bus [8] and IEEE-57 bus test system [104] are considered. The simulations are carried in MATLAB 2010a [105] environment, on a windows 7 professional operating system with Intel core I7 processor and 2GB of RAM. The IEEE-30 bus consists of 6 generators and 41 transmission lines. Whereas, IEEE-57 test system consists of 7 generators and 80 transmission lines.

2.6.1 Results for IEEE-30 bus System

In this approach, the IEEE-30 bus test system is simulated for N-1 line outage contingency for the base case data and corresponding line flows and voltages are obtained for each outage. With these values the performance indices are computed for each N-1 line outage case.

According to the algorithm in section 2.5, the N-1 line outage is simulated for all the lines and corresponding performance indices are computed and ranked as shown in Table 2.1.

Table 2.1: Contingency ranking of IEEE-30 bus system (Base load condition)
(Active power PI and Voltage PI)

Line Outage	Active power Performance Index by NRLF	Line Outage	Voltage Performance Index by NRLF
L 1-2	0.7579	L 6-8	2.2073
L 2-5	0.7555	L 6-7	2.1857
L 9-10	0.7387	L 6-9	2.1453
L 4-12	0.7371	L 24-25	2.1187
L 12-15	0.6409	L 23-24	2.0897
L 6-9	0.6374	L 8-28	2.0805
L 6-28	0.6189	L 22-24	2.0742
L 27-30	0.6110	L 21-22	2.0723
L 10-21	0.6091	L 6-28	2.0660
L 15-23	0.6005	L 14-15	2.0649
L 22-24	0.6002	L 18-19	2.0614
L 6-8	0.5988	L 29-30	2.0613
L 25-27	0.5987	L 16-17	2.0576
L 12-16	0.5969	L 3-4	2.0524
L 15-18	0.5961	L 27-29	2.0516
L 27-29	0.5957	L 27-30	2.0466
L 10-20	0.5941	L 5-7	2.0457
L 10-17	0.5874	L 19-20	2.0236
L 12-14	0.5863	L 15-23	2.0230
L 18-19	0.5859	L 10-22	2.0174
L 19-20	0.5858	L 4-6	2.0032
L 24-25	0.5839	L 6-10	1.9858
L 16-17	0.5838	L 10-17	1.9848
L 23-24	0.5834	L 25-27	1.9682
L 10-22	0.5831	L 15-18	1.9658
L 21-22	0.5831	L 2-5	1.9517
L 2-6	0.5820	L 2-4	1.9323
L 4-6	0.5811	L 2-6	1.9247
L 8-28	0.5804	L 10-21	1.9179

L 14-15	0.5797	L 10-20	1.9127
L 29-30	0.5761	L 12-14	1.8940
L 6-7	0.5735	L 12-16	1.8838
L 6-10	0.5696	L 1-3	1.8683
L 1-3	0.5672	L 1-2	1.8128
L 3-4	0.5660	L 4-12	1.6931
L 2-4	0.5643	L 12-15	1.6499
L 5-7	0.5617	L 9-10	1.5084

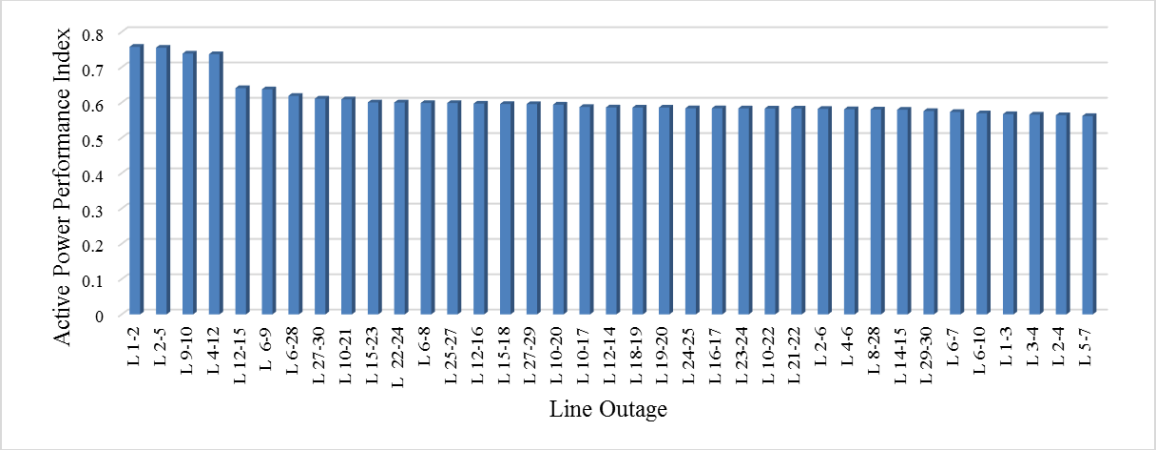

Figure 2.3: Contingency ranking of IEEE-30 bus system (Active Power performance index)

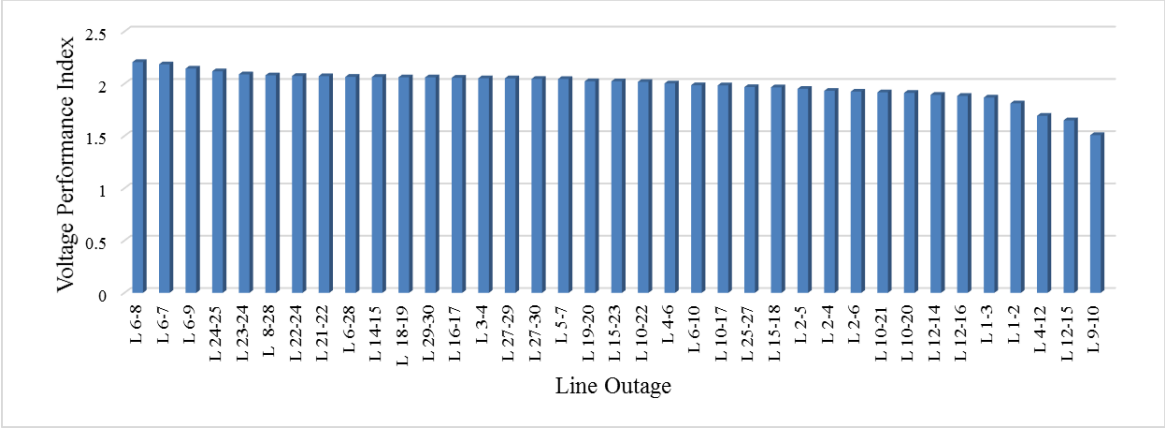

Figure 2.4: Contingency ranking of IEEE-30 bus system (Voltage performance index)

From Table 2.3, it can be observed that the line outage L 1-2 has highest active power performance index of 0.7579 and it is ranked first followed by outage L 2-5. Similarly, the

line outage L 6-8 has highest voltage performance index of 2.2073 followed by outage L 6-7. Based on the importance of security, the top critical contingencies are given highest priority. This analysis helps in identifying the system condition for a contingency. Once it is identified, necessary actions can be implemented. The Figure 2.3 and Figure 2.4 shows the active power PI and voltage PI contingency ranking respectively.

2.6.2 Results for IEEE-57 bus System

The contingency ranking is carried out on base case data of IEEE-30 bus system. Whereas, on IEEE-57 bus test system, the contingency ranking is carried out with a change in 60% of load condition. With this load condition, N-1 line outage contingency is created and the corresponding line flows and voltages are obtained for each outage. With these values the performance indices are computed for each N-1 line outage case. According to the algorithm in section 2.5, the N-1 line outage is simulated for all the lines and corresponding performance indices are computed and ranked as shown in Table 2.2.

Table 2.2: Contingency ranking of IEEE-57 bus system (60% load variation)
(Active power PI and Voltage PI)

Line Outage	Active power Performance Index by NRLF	Line Outage	Voltage Performance Index by NRLF
L 4-6	9.7762	L 7-29	49.1919
L 5-6	8.7931	L 37-38	42.6579
L 8-9	7.4949	L 36-37	23.5421
L 7-29	6.0483	L 28-29	21.9972
L 3-4	5.4184	L 4-6	17.3254
L 37-38	5.3207	L 27-28	13.0076
L 36-37	5.2024	L 22-38	10.0366
L 1-15	5.1414	L 1-15	9.6956
L 1-17	5.0948	L 8-9	8.7644
L 28-29	4.9123	L 5-6	8.7204
L 7-8	4.7285	L 46-47	8.6099
L 27-28	4.7048	L 14-46	8.4288
L 1-16	4.6541	L 22-23	8.238
L 22-38	4.6191	L 26-27	6.1467
L 46-47	4.6117	L 38-48	5.9441
L 14-46	4.6115	L 13-49	5.9226
L 22-23	4.5209	L 7-8	5.8262
L 4-18	4.5015	L 30-31	5.6601
L 14-15	4.4990	L 24-26	5.5838

L 2-3	4.4770	L 1-17	5.4874
L 9-55	4.4755	L 12-13	5.3175
L 41-42	4.4731	L 44-45	5.3062
L 29-52	4.4668	L 15-45	5.2792
L 10-51	4.4652	L 3-4	4.8993
L 11-43	4.4603	L 18-19	4.8097
L 44-45	4.4415	L 47-48	4.7467
L 15-45	4.4414	L 10-51	4.6144
L 38-48	4.3877	L 14-15	4.49
L 41-43	4.3853	L 38-44	4.4821
L 13-49	4.3759	L 24-25	4.4162
L 52-53	4.3745	L 41-42	4.3288
L 18-19	4.368	L 24-25	4.2959
L 47-48	4.3669	L 1-16	4.2533
L 49-50	4.3542	L 21-22	4.1498
L 38-44	4.3530	L 23-24	4.0964
L 21-20	4.3359	L 11-43	4.0611
L 21-22	4.3359	L 36-40	3.9043
L 6-8	4.3344	L 10-12	3.8592
L 9-11	4.3325	L 4-48	3.8375
L 56-41	4.3311	L 21-20	3.8294
L 13-15	4.3291	L 13-15	3.8213
L 9-10	4.3223	L 38-49	3.8026
L 31-32	4.3117	L 12-17	3.7974
L 24-26	4.2965	L 41-43	3.7613
L 26-27	4.2965	L 52-53	3.6403
L 24-25	4.2931	L 50-51	3.6315
L 12-13	4.2921	L 9-10	3.6278
L 6-7	4.2917	L 31-32	3.6037
L 54-55	4.2900	L 29-52	3.5764
L 30-31	4.2889	L 4-18	3.562
L 48-49	4.2874	L 11-4	3.5351
L 11-13	4.2873	L 13-14	3.4715
L 23-24	4.2873	L 2-3	3.4614
L 37-39	4.2869	L 37-39	3.447
L 39-57	4.2869	L 9-11	3.4442
L 56-42	4.2862	L 49-50	3.4428
L 57-56	4.2838	L 56-41	3.3981
L 9-13	4.2817	L 54-55	3.3921
L 12-17	4.2817	L 9-55	3.3781
L 19-20	4.2775	L 6-8	3.3299
L 13-14	4.2770	L 48-49	3.3195
L 12-16	4.2765	L 53-54	3.3096
L 38-49	4.2746	L 57-56	3.2034
L 10-12	4.272	L 3-15	3.1953
L 24-25	4.2714	L 56-42	3.1938
L 9-12	4.2712	L 9-13	3.1808
L 4-18	4.2678	L 11-13	3.1805
L 3-15	4.2645	L 12-16	3.1786

L 11-4	4.2582	L 19-20	3.1725
L 40-56	4.2571	L 9-12	3.1451
L 36-40	4.2522	L 6-7	3.0854
L 53-54	4.2445	L 39-57	3.0349
L 50-51	4.2348	L 40-56	2.8518

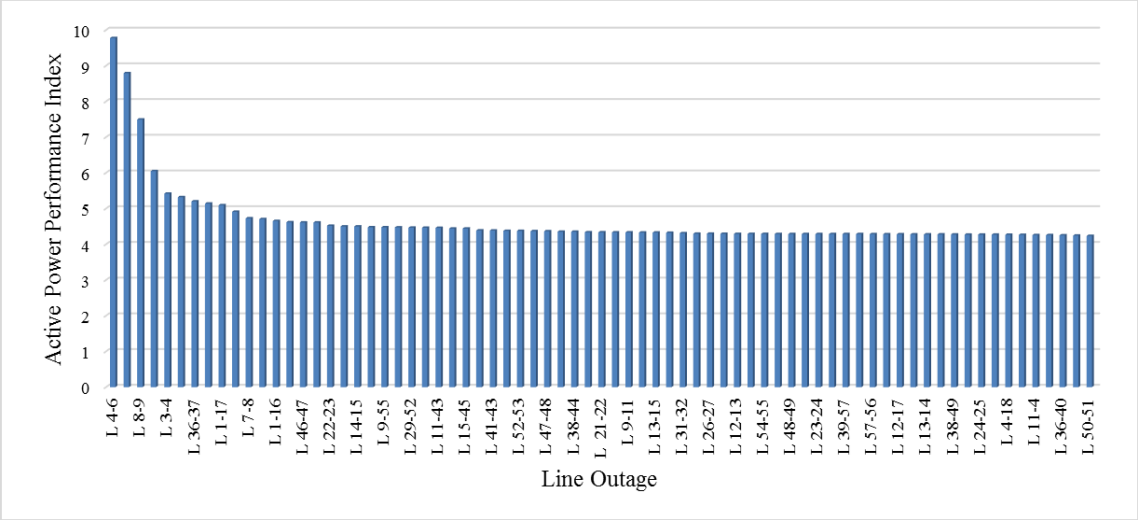

Figure 2.5: Contingency ranking of IEEE-57 bus system (Active power performance index)

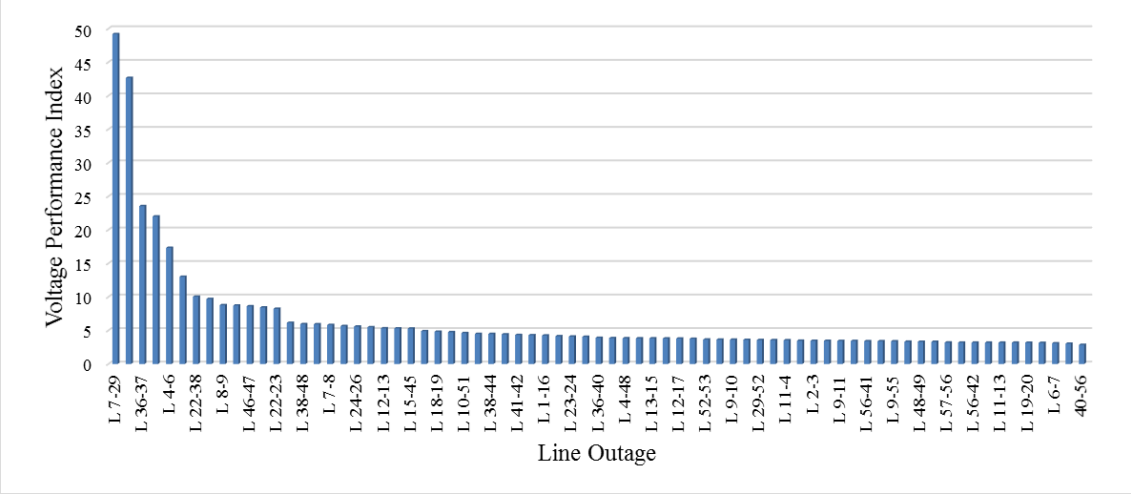

Figure 2.6: Contingency ranking of IEEE-57 bus system (Voltage performance index)

From Table 2.2, it can be observed that the performances indices are high, for the variation in load condition. The line outages L 4-6, L 5-6 and L 8-9 gives the high active power performance index as 9.7762, 8.7931 and 7.4949 respectively. Similarly, the line outages L 7-29, L 37-38 and L 36-37 gives the highest voltage performance index as 49.1919, 42.6579and 23.5421 respectively. These are treated as the critical contingencies which needs much attention for security control. The Figure 2.5 and Figure 2.6 shows the active power PI and voltage PI contingency ranking respectively. With this contingency ranking approach, the severe contingencies can be identified, which aids in taking necessary preventive and control actions to maintain the system security.

2.7 Summary

In this chapter, power system static security assessment is analyzed by contingency ranking approach using the NRLF method. Two performance indices are used, namely the active power performance index and voltage performance index in order to quantify the contingency severity. Two standard IEEE 30-bus and IEEE-57 bus systems are considered to investigate the approach by simulating N-1 line outage contingency. The performances indices are obtained for all the N-1 line outage cases and ranked based on the performance indices. From, these ranking it is easy to analyze the insecure nature of the system for a specific contingency.

However this approach is used to analyze the system security, it suffers from the drawback of solving the load flow equations and this offline method is tedious, making it infeasible for online implementation. Thus, the next chapter focus on modeling the neural networks to predict the performance indices for the assessment of security by contingency ranking approach.

Chapter 3

Prediction of Performance Indices using Multi-Layer Perceptron and Radial Basis Function Network for Security Assessment

3.1 Introduction

In the previous chapter 2, the security of the power system is evaluated by contingency ranking using the conventional NRLF method. However, these methods are highly complex and time consuming for the online implementation. Thus, there is a need to model an efficient online tool for power system security assessment to ensure safe operation of the power system. The deregulation has compelled the utilities to function their systems closer to their security limits, which demands quick and efficient approach for the security assessment. Thus, it is necessary to design a ranking module that can predict the system severity for the security assessment which is feasible for the real time implementation in order to aid the operational engineers.

In this chapter 3, a ranking module is designed using two neural network models. The two neural network models are designed and trained for different operating conditions to predict the performance indices. In the testing phase, the two neural network models are provided with the same input data set (to predict performance indices), which was used to carry out the NRLF based contingency ranking in chapter 2. The results obtained with these networks clearly suggests that both of these networks are efficient in predicting the

performance indices.

This chapter is organized as follows: Section 3.2 presents the brief explanation of the ranking module, Section 3.3 has presented the design of multi-layer feedforward neural network, whereas Section 3.4 gives the procedure to generate data for the training and the testing of the neural network models. Section 3.5 discusses the prediction of the performance indices using MFNN and Section 3.6 presents the simulation results and discussion for the MFNN model. The Section 3.7 presents the design of radial basis function network, whereas, the Section 3.8 discusses the prediction of the performance indices using RBFN. The Section 3.9 presents the simulation results and discussion for the RBFN model. Finally in Section 3.10, the concluding remarks are provided.

3.2 Design of the Ranking Module

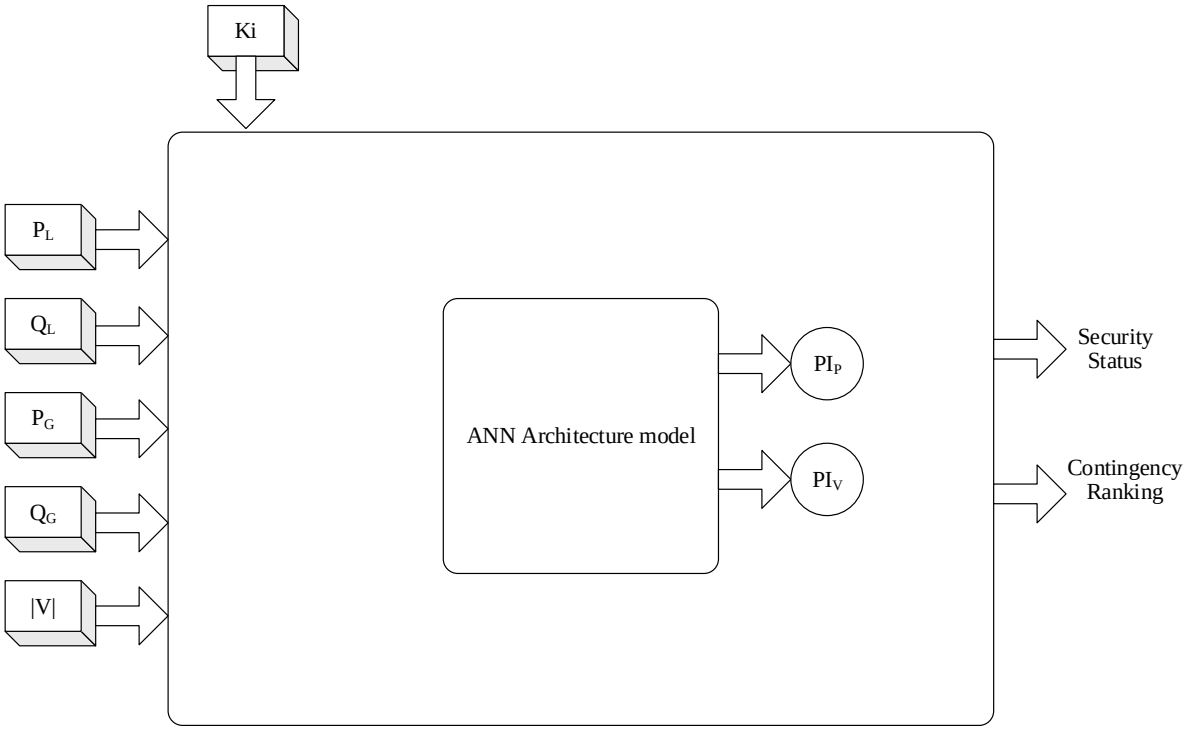

Figure 3.1: Block diagram of the ranking module

The nature of the power system is dynamic, where the system parameters varies continuously. Thus, the classical offline methods are not reliable for continuous monitoring of the system security. However, a trained ANN have the advantage to respond to unknown system conditions, which enhance the security monitoring and assessment, which makes it feasible for online implementation. The key contribution of this work is to establish an online ranking module, which minimizes the offline computational effort and predict the system severity under contingency scenario. The module make use of active power performance index and voltage performance index for quick and efficient security assessment by contingency ranking. The key functions of the module is that: (1) It calculates the system severity for each operating condition. (2) It calculates severity indices under N-1 line outage contingency. (3) The model rank the contingencies based on their order of severity.

The Figure 3.1 shows the block diagram of the ranking module. The input features for the module comprises (covering entire operating scenarios) of active and reactive power at all the load bus (P_L,Q_L) and generator buses (P_G,Q_G), the voltage magnitudes |V| at all the buses along with the N-1 line outage contingency (K_i). The module has the ability to predict the performance indices to assess the security status by contingency ranking for a given operating condition. The module uses two ANN architectures which takes the line outage condition and the loading condition as the inputs along with other operating conditions and performance indices as the output parameter. The neural network models used by the module are, the MFNN and the RBFN. These two networks are trained for various range of operating conditions to predict the performance indices. The details of which are explained in the sections below.

3.3 Multi-Layer Feedforward Network

The application of the artificial neural networks have gained major importance in many engineering fields [77], because of the fact that these models can easily handle complex and non-linear problems. ANNs are massively parallel-interconnected networks of simple elements intended to interact with the real world in the same way as the biological nervous system. They offer an unusual scheme based programming standpoint and exhibit higher computing speeds compared to other conventional methods. The ANNs are characterized based on their topology, such as, the number of interconnections, the node characteristics that

are classified by the type of nonlinear elements used and the kind of learning rules employed. The ANN architecture is designed with well-organized topology of Processing Elements (PEs) called neurons. In Multilayer Feed Forward Neural network (MFNN) the neurons are arranged in layers and only neurons in adjacent layers are connected.

The MFNN architecture consists of three layers, which consists of input layer, hidden layer and an output layer as shown in Figure 3.2.

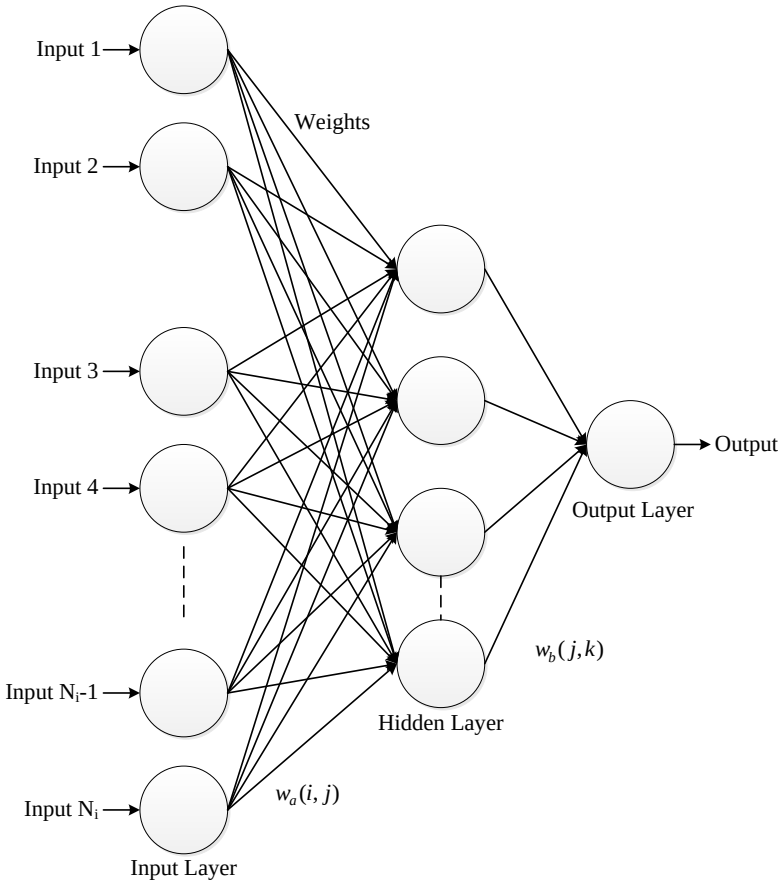

Figure 3.2: Multi-Layer Feedforward Neural Network

Each layer is connected with each neuron of the previous layer with weights attached to it. The MFNN model utilizes the back propagation algorithm (BPA) to train the network. The equation (3.1), shows the sigmoidal activation function for all the neurons except for those neurons in the input layer.

$$S(x) = \frac{1}{(1+e^{-x})} \tag{3.1}$$

3.3.1 Selection of Hidden Neurons

The selection of optimal number of hidden neurons, N_h is the most intriguing and testing perspective in designing of the MFNN. Several authors have proposed various theories to select the proper choice of N_h. Simon Haykin [78] has determined that N_h should lie between 2 and ∞. Hecht- Nielsen [79] uses the ANN interpretation of Kolmogorov's theorem to arrive at the upper bound on the N_h for a single hidden layer network as $2(N_i+1)$, where N_i is the number of input neurons. However, the selection of N_h should be decided very judiciously depending on the requirement of the problem. A large value of N_h may reduce the training error associated with the MFNN, but at the cost of increasing the computational complexity and time. For example, if one gets a tolerably low value of training error with certain value of N_h, there is no point in further increasing the value of N_h to enhance the performance of the MFNN.

3.3.2 Normalization of Input-Output Data

The input and the output data are normalized before being processed in the network. In this scheme of normalization, the maximum values of the input and output vector components are determined as follows:

$$n_{i,\max} = \max(n_i(p)) \quad p = 1,...,N_p, i = 1,...,N_i \tag{3.2}$$

Where, N_p represents the number of patterns in the training set.

$$o_{k,\max} = \max(o_k(p)) \quad p = 1,...N_p, i = 1,...,N_k \tag{3.3}$$

Where, N_k represents the number of neurons in the output layer. Normalized by these maximum values, the input and output variables are obtained as follows:

$$n_{i,nor}(p) = \frac{n_i(p)}{n_{i,\max}} \quad p = 1,...,N_{p,} i = 1,...,N_i \tag{3.4}$$

$$o_{k,nor}(p) = \frac{o_k(p)}{o_{k,\max}} \quad p = 1,...N_p, i = 1,...N_k \tag{3.5}$$

After normalization, the input and output variables lie in the range of 0 to 1.

3.3.3 Selection of ANN Parameters

The learning rate of the BPA is influenced by the momentum factor, α_1 and the learning rate parameter, η_1. The BPA contribute an approximation to the trajectory in the weight space calculated by the method of steepest descent [78]. If the considered value of η_1 is very small, which results in slow rate of learning, while if the value of η_1 is too large in order to speed up the rate of learning, the MFNN may become unstable. A simple method of increasing the rate of learning without making the MFNN unstable is by adding the momentum factor α_1 [80]. Preferably, the values of η_1 and α_1 should lie between 0 and 1.

3.3.4 Weight Update Equations

The weights between the hidden layer and the output layer are updated based on the equation (3.6).

$$w_b(j,k,m+1) = w_b(j,k,m) + \eta_1 * \delta_k(m) * S_b(j) + \alpha_1(w_b(j,k,m) - w_b(j,k,m-1)) \tag{3.6}$$

Where, m is the total number of iterations, where j and k varies from 1 to N_h and 1 to N_k respectively. $\delta_k(m)$ is the error for the k^{th} output at the m^{th} iteration, $S_b(j)$ is the output from the hidden layer.

Similarly, the weights between the hidden layer and the input layer are updated as in equation (3.7).

$$w_a(i,j,m+1) = w_a(i,j,m) + \eta_1 * \delta_j(m) * S_a(i) + \alpha_1(w_a(i,j,m) - w_a(i,j,m-1)) \tag{3.7}$$

Where i varies from 1 to N_i, as there are N_i inputs to the network, $\delta_j(m)$ is the error for the j^{th} output after the m^{th} iteration and $S_a(i)$ is the output from the first layer.

The $\delta_k(m)$ in equation (3.6) and $\delta_j(m)$ in equation (3.7) are related as,

$$\delta_j(m) = \sum_{k=1}^{K} \delta_k(m) * w_b(j,k,m) \tag{3.8}$$

3.3.5 Evaluation Criteria

The Mean Square Error E_{tr} for the training patterns after the m^{th} iteration is defined as,

$$E_{tr}(m) = \left(\frac{1}{N_p}\right) * \left[\sum_{p=1}^{N_p} \left\{X_{1p} - X_{2p}(m)\right\}^2\right] \tag{3.9}$$

Where X_{1p} is the actual value and X_{2p} is the estimated value of the performance indices after the m^{th} iteration. The training is stopped when the least value of E_{tr} is obtained and this value does not change much with the number of iterations. The E_{tr} tells how well the network has adopted to fit the training data only, even if the data is contaminated.

3.4 Data Generation for Training and Testing

In this work, to realize the effectiveness of the ANN models, the data is generated by performing large set of offline computations. This is achieved by considering the IEEE-30 bus and IEEE-57 bus systems, and randomly varying the load condition from 50% to 100% of its base case. For each loading condition, under N-1 line outage contingency, the performances indices, the line flows and the voltages are computed using Newton-Raphson load flow analysis. The generated data is used to train the neural network models.

For IEEE-30 bus system, the total number of line outage cases considered are 37. The load is varied randomly from 50% to 100% of its base case and the corresponding values of active power PI and voltage PI are computed for each loading condition. The total number of input-output data sets generated are 37*6=222. Out of which, 185 sets of input-output patterns are used to train the network and the remaining 37 sets are used to test the network.

For IEEE-57 bus system, the total number of line outage cases considered are 73. The load is varied randomly from 50% to 100% of its base case and the corresponding values of active power PI and voltage PI are computed for each loading condition. The total number of

input-output data sets generated are 73*5 =365. Out of which, 292 sets of input-output patterns are used to train the network and the remaining 73 sets are used to test the network.

Once the neural network models are trained to obtain least mean square error, they are feasible to undergo testing to predict the performance indices. The models are used in the ranking module to predict security status in terms of the performance indices for a particular operating condition for static security assessment by contingency ranking approach.

3.5 Prediction of Performance Indices using MFNN

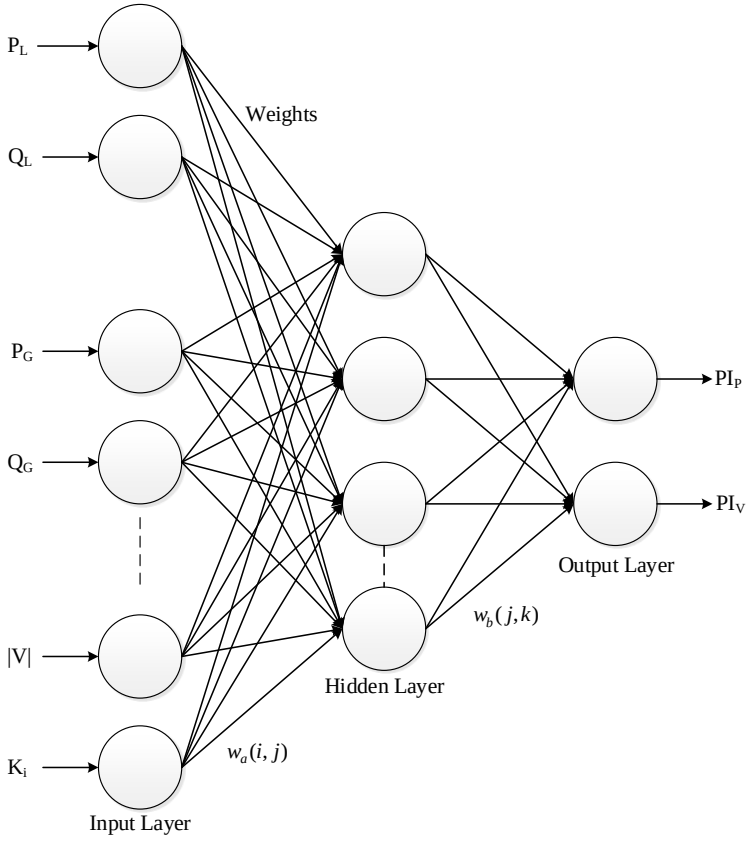

Figure 3.3: MFNN model for the prediction of performance indices

This section explains the prediction of performance indices using MFNN. The model predicts the active power PI and Voltage PI as a function of different power system network

operating conditions. The network is provided with both input data and desired output, and it is trained in a supervised learning fashion using the back propagation algorithm. The back propagation algorithm performs the input to output mapping by making weight connection adjustment following the error between the computed output value and the desired output response. The training phase is completed after a series of iterations. In each iteration, output is compared with the desired response and a match is obtained.

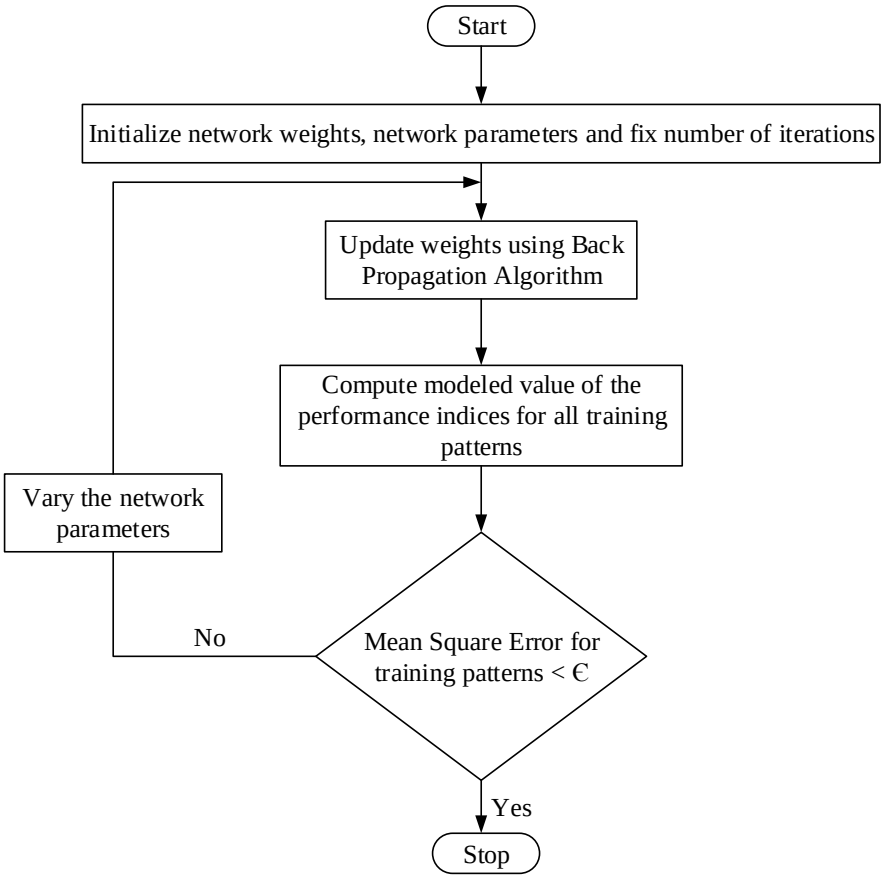

Figure 3.4: Flow chart for MFNN

As shown in Figure 3.3, the number of input parameters to the network is six, that is the active and reactive power at all the load bus (P_L,Q_L) and generator buses (P_G,Q_G), the voltage magnitudes |V| at all the buses along with the N-1 line outage contingency (K_i) and the output parameters are active power performance index and voltage performance index. The Figure 3.4 shows the flowchart for the prediction of performance indices using MFNN.

3.6 Simulation Results and Discussion

The performance of the neural network models depends on the optimal selection of network parameters. In this approach, the optimum network parameters are obtained based on mean square error E_{tr} for the training patterns. The network is trained in a sequential order. In applying the BPA for the prediction of performance indices, the following important parameters are discussed.

1. Network parameters
2. Number of hidden neurons
3. Number of iterations

For BPA, the optimal values of the learning rate η_1, and momentum factor α_1 are obtained by performing simulation with different values of η_1 and α_1. Initially, the values of η_1=0.1 and α_1=0.1 are considered and then they are varied to obtain the optimum value. The range of values of η_1 and α_1 should lie between 0 and 1. The accuracy of the model depends on the optimal selection of the network parameters. To obtain optimal parameters, a series of simulations were carried out to obtain least mean square error (MSE). The simulations are carried to obtain least mean square error, by varying one parameter, with fixed values of other two parameters. The combination with least mean square error E_{tr} are selected as the optimal parameters.

3.6.1 Results for IEEE-30 bus System

The Table 3.1 to Table 3.3 shows the variation of E_{tr} as a function of η_1, α_1 and N_h respectively. The network structure and procedure to predict the performance indices using MFNN is shown in Figure 3.3 and Figure 3.4 respectively. The variation of error E_{tr} of the training data with the number of iterations is shown in Figure 3.5.

From Table 3.1 to Table 3.3, it can be observed that the least mean square error E_{tr} is obtained for η_1 = 0.99, α_1 = 0.7 and N_h=10, which are chosen as optimal network parameters.

In order to test the MFNN model, the network is provided the test data as the inputs. Here the test data is given as the base case load condition data, which is not used in the training

set. The active power performance index and voltage performance index for the test data are predicted by using the updated weights of the network. The predicted performance indices are compared with the indices obtained using NRLF method. Once, the performance indices are predicted, the next task is to rank them based on the severity to evaluate the security of the power system.

Table 3.1: Variation of E_{tr} with η_1 ($N_h = 3$, $\alpha_1 = 0.1$, No. of iterations = 100)

η_1	E_{tr}
0.1	$5.7677*10^{-04}$
0.2	$2.0250*10^{-04}$
0.3	$7.8636*10^{-05}$
0.4	$3.3661*10^{-05}$
0.5	$1.5640*10^{-05}$
0.6	$7.7902*10^{-06}$
0.7	$4.1259*10^{-04}$
0.8	$2.3113*10^{-06}$
0.9	$1.3648*10^{-06}$
0.99	$8.8682*10^{-07}$

Table 3.2: Variation of E_{tr} with α_1 ($N_h = 3$, $\eta_1 = 0.99$, No. of iterations = 100)

α_1	E_{tr}
0.1	$8.8682*10^{-07}$
0.2	$6.2956*10^{-07}$
0.3	$4.2619*10^{-07}$
0.4	$2.6931*10^{-07}$
0.5	$1.5257*10^{-07}$
0.6	$7.1065*10^{-08}$
0.7	$2.1297*10^{-08}$
0.8	$1.1187*10^{-07}$

Table 3.3: Variation of E_{tr} with N_h ($\eta_1 = 0.99$, $\alpha_1 = 0.7$, No. of iterations = 100)

N_h	E_{tr}
3	$2.1297*10^{-08}$
4	$1.0459*10^{-08}$
5	$7.9958*10^{-09}$
6	$4.1083*10^{-09}$
7	$1.6827*10^{-09}$
8	$8.4391*10^{-10}$
9	$6.4844*10^{-10}$
10	$5.4602*10^{-10}$
11	$5.7358*10^{-10}$

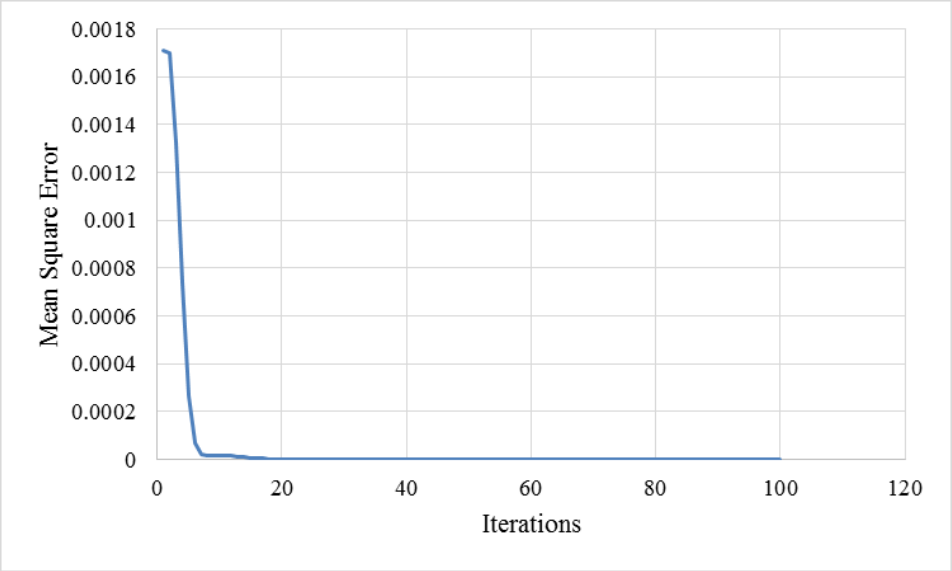

Figure 3.5: E_{tr} vs Iterations for MFNN (for 100 iterations) (IEEE-30 bus system)

Table 3.4: Contingency ranking and Comparison of API and VPI obtained by NRLF method and MFNN (Base load condition for IEEE-30 bus system)

Line Outage	Active power Performance Index by NRLF	Active power Performance Index by MFNN (100 Iterations)	Line Outage	Voltage Performance Index by NRLF	Voltage Performance Index by MFNN (100 Iterations)
(1)	(2)	(3)	(4)	(5)	(6)
L 1-2	0.7579	0.7579	L 6-8	2.2073	2.1987
L 2-5	0.7555	0.7455	L 6-7	2.1857	2.1968
L 9-10	0.7387	0.7373	L 6-9	2.1453	2.1906
L 4-12	0.7371	0.7362	L 24-25	2.1187	2.1819
L 12-15	0.6409	0.6409	L 23-24	2.0897	2.1590
L 6-9	0.6374	0.6374	L 8-28	2.0805	2.1447
L 6-28	0.6189	0.6189	L 22-24	2.0742	2.1315
L 27-30	0.6110	0.6110	L 21-22	2.0723	2.1268
L 10-21	0.6091	0.6091	L 6-28	2.0660	2.1091
L 15-23	0.6005	0.6005	L 14-15	2.0649	2.1057
L 22-24	0.6002	0.6002	L 18-19	2.0614	2.0944
L 6-8	0.5988	0.5988	L 29-30	2.0613	2.0941
L 25-27	0.5987	0.5987	L 16-17	2.0576	2.0817
L 12-16	0.5969	0.5969	L 3-4	2.0524	2.0650
L 15-18	0.5961	0.5961	L 27-29	2.0516	2.0626
L 27-29	0.5957	0.5937	L 27-30	2.0466	2.0496
L 10-20	0.5941	0.5941	L 5-7	2.0457	2.0476
L 10-17	0.5874	0.5874	L 19-20	2.0236	2.0233

L 12-14	0.5863	0.5863	L 15-23	2.0230	2.0228
L 18-19	0.5859	0.5859	L 10-22	2.0174	2.0179
L 19-20	0.5858	0.5858	L 4-6	2.0032	2.0034
L 24-25	0.5839	0.5839	L 6-10	1.9858	1.9856
L 16-17	0.5838	0.5838	L 10-17	1.9848	1.9846
L 23-24	0.5834	0.5835	L 25-27	1.9682	1.9683
L 10-22	0.5831	0.5831	L 15-18	1.9658	1.9659
L 21-22	0.5831	0.5831	L 2-5	1.9517	1.9517
L 2-6	0.5820	0.5820	L 2-4	1.9323	1.9322
L 4-6	0.5811	0.5811	L 2-6	1.9247	1.9247
L 8-28	0.5804	0.5804	L 10-21	1.9179	1.9179
L 14-15	0.5797	0.5797	L 10-20	1.9127	1.9127
L 29-30	0.5761	0.5761	L 12-14	1.8940	1.8940
L 6-7	0.5735	0.5735	L 12-16	1.8838	1.8838
L 6-10	0.5696	0.5696	L 1-3	1.8683	1.8683
L 1-3	0.5672	0.5672	L 1-2	1.8128	1.8128
L 3-4	0.5660	0.5660	L 4-12	1.6931	1.6931
L 2-4	0.5643	0.5643	L 12-15	1.6499	1.6499
L 5-7	0.5617	0.5617	L 9-10	1.5084	1.5084

The Table 3.4 shows the comparison of the predicted active power and voltage performance indices, with the conventional NRLF method and MFNN and its ranking. The Figure 3.6 and Figure 3.7 shows the comparison and contingency ranking based on the performance indices.

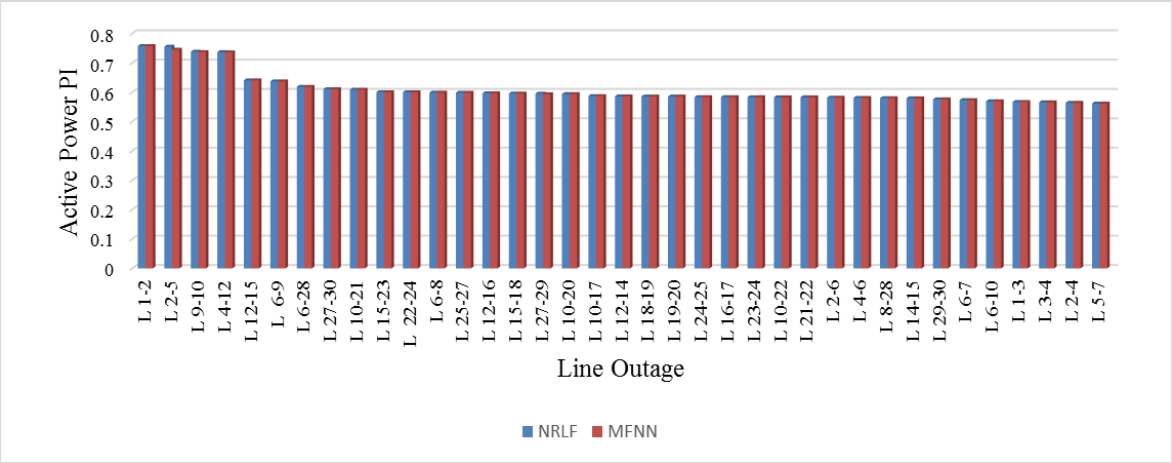

Figure 3.6: Contingency ranking and Comparison of Active power PI between NRLF and MFNN (IEEE-30 bus system)

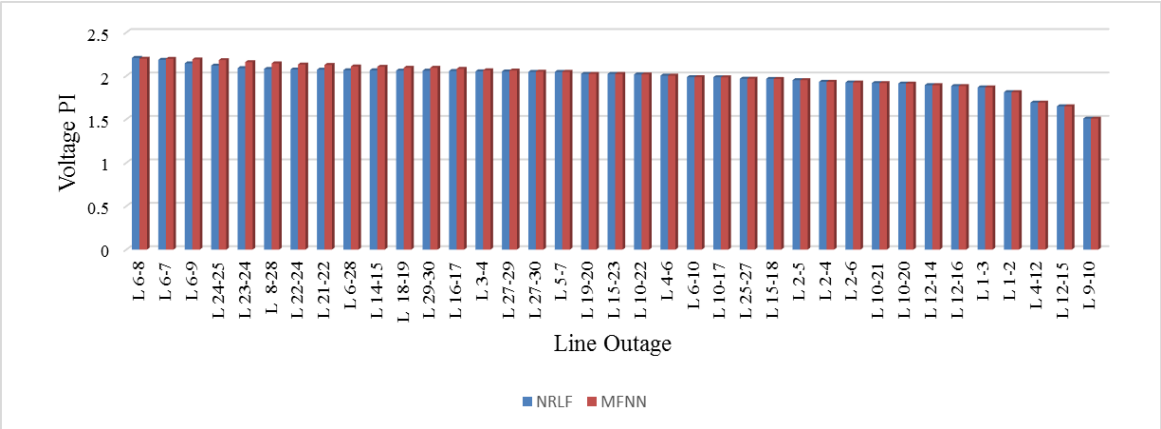

Figure 3.7: Contingency ranking and Comparison of Voltage PI between NRLF and MFNN (IEEE-30 bus system)

3.6.2 Results for IEEE-57 bus System

Similar to the IEEE-30 bus system, the initial step is to obtain the optimal network parameters. The Table 3.5 to Table 3.7 shows the variation of E_{tr} as a function of η_1, α_1 and N_h respectively. The variation of error E_{tr} of the training data with the number of iterations is shown in Figure 3.8.

Table 3.5: Variation of E_{tr} with η_1 (N_h = 3, α_1 = 0.1, No. of iterations = 100)

η_1	E_{tr}
0.1	0.0018
0.2	$6.1969*10^{-04}$
0.3	$2.2482*10^{-04}$
0.4	$8.9717*10^{-05}$
0.5	$3.8866*10^{-05}$
0.6	$1.7968*10^{-05}$
0.7	$8.7413*10^{-05}$
0.8	$4.4283*10^{-06}$
0.9	$2.3183*10^{-06}$
0.99	$1.3259*10^{-06}$

From Table 3.5 to Table 3.7, it can be observed that the least mean square error E_{tr} is obtained for η_1 = 0.99, α_1 = 0.7 and N_h=10, which are chosen as optimal network parameters. In the testing phase, the network is provided with 60% load variation data as the input, which is not used in the training set. The active power performance index and voltage performance

index for the test data are predicted by using the updated weights of the network. The predicted performance indices are compared with the indices obtained using NRLF method.

Table 3.6: Variation of E_{tr} with α_1 ($N_h = 3$, $\eta_1 = 0.99$, No. of iterations = 100)

α_1	E_{tr}
0.1	$1.3259*10^{-06}$
0.2	$8.8897*10^{-07}$
0.3	$5.4767*10^{-07}$
0.4	$2.8907*10^{-07}$
0.5	$1.0898*10^{-07}$
0.6	$2.3442*10^{-08}$
0.7	$4.7198*10^{-09}$
0.8	$2.8226*10^{-08}$

Table 3.7: Variation of E_{tr} with N_h ($\eta_1 = 0.99$, $\alpha_1 = 0.7$, No. of iterations = 100)

N_h	E_{tr}
3	$4.7198*10^{-09}$
4	$1.6935*10^{-09}$
5	$1.5048*10^{-09}$
6	$1.2039*10^{-09}$
7	$5.6150*10^{-10}$
8	$2.7578*10^{-10}$
9	$2.0455*10^{-10}$
10	$1.6673*10^{-10}$
11	$1.8582*10^{-10}$

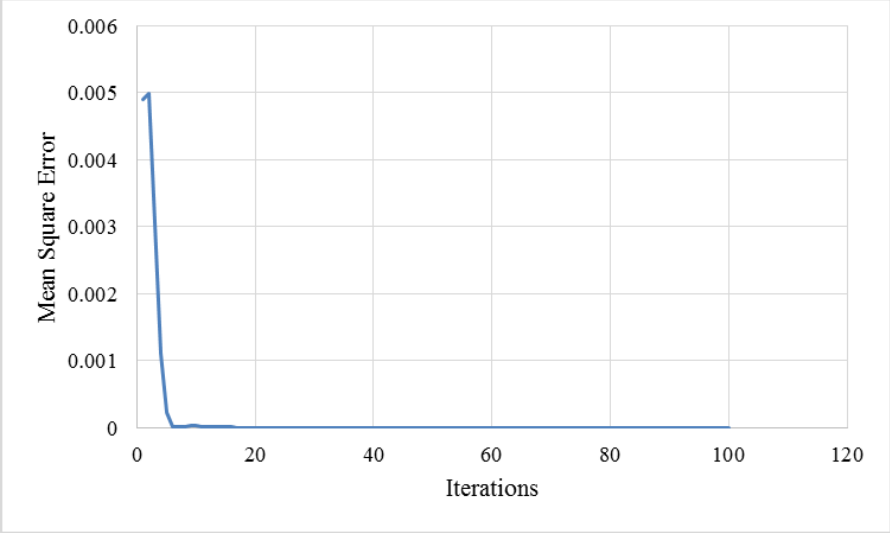

Figure 3.8: E_{tr} vs Iterations for MFNN (for 100 iterations) (IEEE-57 bus system)

Table 3.8: Contingency ranking and Comparison of API and VPI obtained by NRLF method and MFNN (60% load variation for IEEE-57 bus system)

Line Outage	Active power Performance Index by NRLF	Active power Performance Index by MFNN (100 Iterations)	Line Outage	Voltage Performance Index by NRLF	Voltage Performance Index by MFNN (100 Iterations)
(1)	(2)	(3)	(4)	(5)	(6)
L 4-6	9.7762	9.6309	L 7-29	49.1919	48.5541
L 5-6	8.7931	8.7931	L 37-38	42.6579	42.6576
L 8-9	7.4949	7.4949	L 36-37	23.5421	23.5422
L 7-29	6.0483	6.0483	L 28-29	21.9972	21.9972
L 3-4	5.4184	5.4184	L 4-6	17.3254	17.3256
L 37-38	5.3207	5.3207	L 27-28	13.0076	13.0073
L 36-37	5.2024	5.2024	L 22-38	10.0366	10.0362
L 1-15	5.1414	5.1414	L 1-15	9.6956	9.6952
L 1-17	5.0948	5.0948	L 8-9	8.7644	8.7641
L 28-29	4.9123	4.9124	L 5-6	8.7204	8.7201
L 7-8	4.7285	4.7285	L 46-47	8.6099	8.6096
L 27-28	4.7048	4.7048	L 14-46	8.4288	8.4286
L 1-16	4.6541	4.6541	L 22-23	8.238	8.2378
L 22-38	4.6191	4.6191	L 26-27	6.1467	6.1470
L 46-47	4.6117	4.6117	L 38-48	5.9441	5.9443
L 14-46	4.6115	4.6115	L 13-49	5.9226	5.9228
L 22-23	4.5209	4.5209	L 7-8	5.8262	5.8263
L 4-18	4.5015	4.5015	L 30-31	5.6601	5.6600
L 14-15	4.4990	4.4990	L 24-26	5.5838	5.5836
L 2-3	4.4770	4.4770	L 1-17	5.4874	5.4871
L 9-55	4.4755	4.4755	L 12-13	5.3175	5.3170
L 41-42	4.4731	4.4731	L 44-45	5.3062	5.3057
L 29-52	4.4668	4.4668	L 15-45	5.2792	5.2787
L 10-51	4.4652	4.4653	L 3-4	4.8993	4.8987
L 11-43	4.4603	4.4603	L 18-19	4.8097	4.8092
L 44-45	4.4415	4.4415	L 47-48	4.7467	4.7463
L 15-45	4.4414	4.4414	L 10-51	4.6144	4.6142
L 38-48	4.3877	4.3877	L 14-15	4.4900	4.4901
L 41-43	4.3853	4.3853	L 38-44	4.4821	4.4822
L 13-49	4.3759	4.3759	L 24-25	4.4162	4.4165
L 52-53	4.3745	4.3745	L 41-42	4.3288	4.3293
L 18-19	4.3680	4.3680	L 24-25	4.2959	4.2965
L 47-48	4.3669	4.3669	L 1-16	4.2533	4.2540
L 49-50	4.3542	4.3542	L 21-22	4.1498	4.1508
L 38-44	4.3530	4.3530	L 23-24	4.0964	4.0975
L 21-20	4.3359	4.3359	L 11-43	4.0611	4.0622
L 21-22	4.3359	4.3359	L 36-40	3.9043	3.9053
L 6-8	4.3344	4.3344	L 10-12	3.8592	3.8601
L 9-11	4.3325	4.3325	L 4-48	3.8375	3.8383
L 56-41	4.3311	4.3311	L 21-20	3.8294	3.8302

L 13-15	4.3291	4.3291	L 13-15	3.8213	3.8220
L 9-10	4.3223	4.3223	L 38-49	3.8026	3.8032
L 31-32	4.3117	4.3117	L 12-17	3.7974	3.7980
L 24-26	4.2965	4.2965	L 41-43	3.7613	3.7617
L 26-27	4.2965	4.2965	L 52-53	3.6403	3.6396
L 24-25	4.2931	4.2931	L 50-51	3.6315	3.6307
L 12-13	4.2921	4.2921	L 9-10	3.6278	3.6270
L 6-7	4.2917	4.2917	L 31-32	3.6037	3.6025
L 54-55	4.2900	4.2900	L 29-52	3.5764	3.5749
L 30-31	4.2889	4.2889	L 4-18	3.562	3.5602
L 48-49	4.2874	4.2874	L 11-4	3.5351	3.5329
L 11-13	4.2873	4.2873	L 13-14	3.4715	3.4681
L 23-24	4.2873	4.2873	L 2-3	3.4614	3.4578
L 37-39	4.2869	4.2869	L 37-39	3.447	3.4430
L 39-57	4.2869	4.2869	L 9-11	3.4442	3.4402
L 56-42	4.2862	4.2862	L 49-50	3.4428	3.4388
L 57-56	4.2838	4.2838	L 56-41	3.3981	3.3930
L 9-13	4.2817	4.2817	L 54-55	3.3921	3.3868
L 12-17	4.2817	4.2817	L 9-55	3.3781	3.3724
L 19-20	4.2775	4.2775	L 6-8	3.3299	3.3229
L 13-14	4.2770	4.2770	L 48-49	3.3195	3.3122
L 12-16	4.2765	4.2765	L 53-54	3.3096	3.3019
L 38-49	4.2746	4.2746	L 57-56	3.2034	3.1920
L 10-12	4.2720	4.2720	L 3-15	3.1953	3.1836
L 24-25	4.2714	4.2714	L 56-42	3.1938	3.1820
L 9-12	4.2712	4.2712	L 9-13	3.1808	3.1685
L 4-18	4.2678	4.2678	L 11-13	3.1805	3.1682
L 3-15	4.2645	4.2645	L 12-16	3.1786	3.1662
L 11-4	4.2582	4.2592	L 19-20	3.1725	3.1599
L 40-56	4.2571	4.2571	L 9-12	3.1451	3.1313
L 36-40	4.2522	4.2522	L 6-7	3.0854	3.0690
L 53-54	4.2445	4.2445	L 39-57	3.0349	3.0161
L 50-51	4.2348	4.2348	40-56	2.8518	2.8231

The Table 3.8 shows the comparison of the predicted active power and voltage performance indices, with the conventional NRLF method and its ranking The Figure 3.10 and Figure 3.11 shows the comparison of contingency ranking and performance indices.

The MFNN based ranking module operate to obtain the complete security assessment by predicting the system severity for a given operating condition and rank them in the order system severity based on the performance indices.

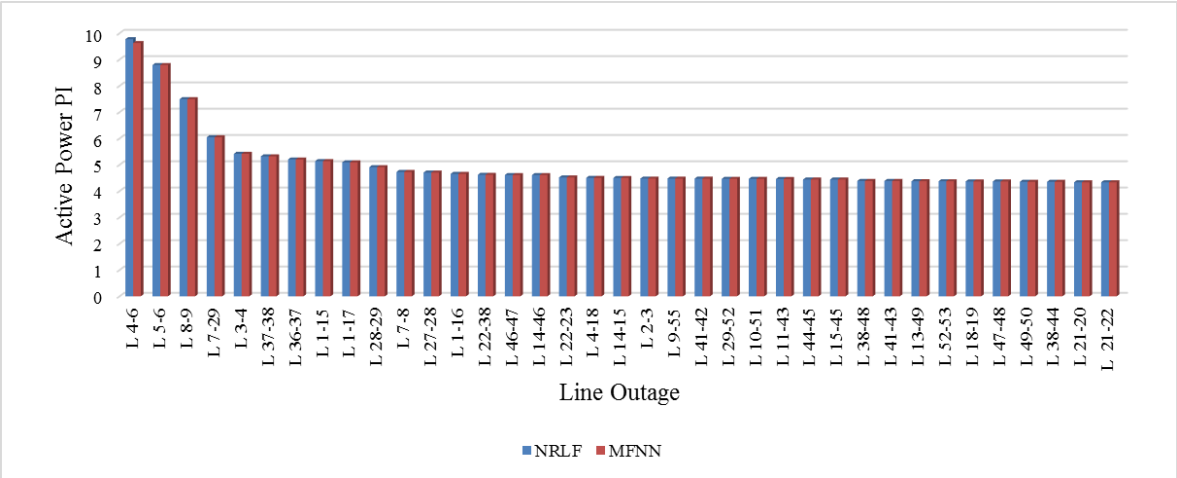

Figure 3.9: Contingency ranking and Comparison of Active Power PI between NRLF and MFNN (IEEE-57 bus system)

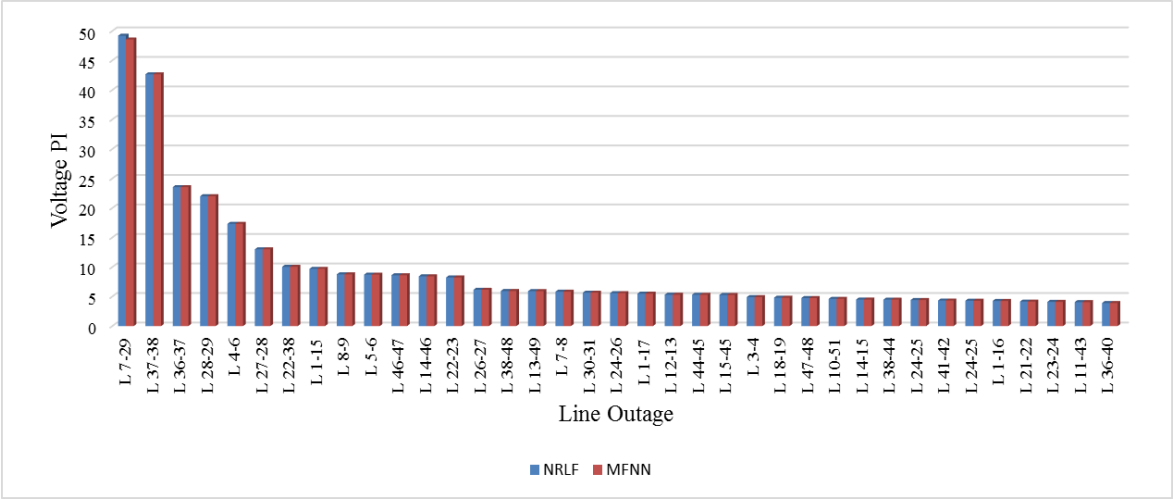

Figure 3.10: Contingency ranking and Comparison of Voltage PI between NRLF and MFNN (IEEE-57 bus system)

The Table 3.4 shows the performance indices and contingency ranking for the base case load condition and the Table 3.8 shows the performance indices and contingency ranking for 60% variation in load condition. The 1st and 4th columns of respective tables shows the various line outages and ranked based on severity using active power performance index and voltage performance index computed using NRLF analysis, as shown in 2nd and 5th columns

of respective tables. The 3rd and 5th columns of Table 3.4 and Table 3.8 shows the active power and voltage performance indices values obtained using the MFNN model. It can be observed that for all the critical contingencies, the predicted values and ranking are almost equal by the module using MFNN model in comparison with columns 2 and 5 respectively. Here, the top critical contingencies need to be given higher priority during security evaluation. Once the critical contingencies are identified, the operational engineers should take necessary control action.

Further, the time taken by the model is found to be 0.62 sec (IEEE-30 bus system) for 100 iterations and 1.29 sec (IEEE-57 bus system) for 100 iterations. From this, it is clear that the ranking module for security assessment by contingency ranking is very quick and accurate for unseen system conditions. From the simulation results and above discussion, for various system operating conditions, the ranking module using MFNN is found to be quick and efficient approach to predict the performance indices and rank the contingencies. Thus, this MFNN ranking module is found feasible for online implementation for security assessment by contingency ranking.

3.7 Radial Basis Function Network

The MFNN may be viewed as the application of a recursive technique known in statistics as stochastic approximation. The RBFN follows a different approach with respect to MFNN. The RBFN attempts to design a neural network as a curve fitting approximation problem in a high dimension space. The learning is equivalent to finding a surface in a multidimensional space that provides a best fit to the training data. Corresponding, generalization is equivalent to the use of this multidimensional surface to interpolate the test data.

The RBFN structure is shown in Figure 3.11. As shown, there are N_i input nodes of this network in the input layer corresponding to the N_i inputs that is quiet similar to MFNN shown in Figure 3.2. The second layer is the hidden layer composed of nonlinear units [81]. In the context of a neural network, the hidden units provide a set of functions that constitute an arbitrary basis for the input patterns when they are expanded into hidden space. The number of nonlinear units is m_1. The output layer comprises of a summer. The nonlinear units in the hidden layer and the output layer are connected by linear weights. The linear weights tend to evolve on a different time scale compared to the nonlinear activation

functions of the hidden layer. The hidden layer's activation functions also known as Radial Basis Functions (RBF) evolve slowly in accordance with some nonlinear optimization strategy. The linear weights adjust themselves rapidly through a linear optimization strategy, such as, the LMS algorithm and the RLS algorithm. There are different learning strategies that may be followed in the design of the RBFN, depending on how the centers of the RBF of the network are specified. In the present work the Fixed Centers Selected at Random (FCSR) strategy are adopted to specify the centers.

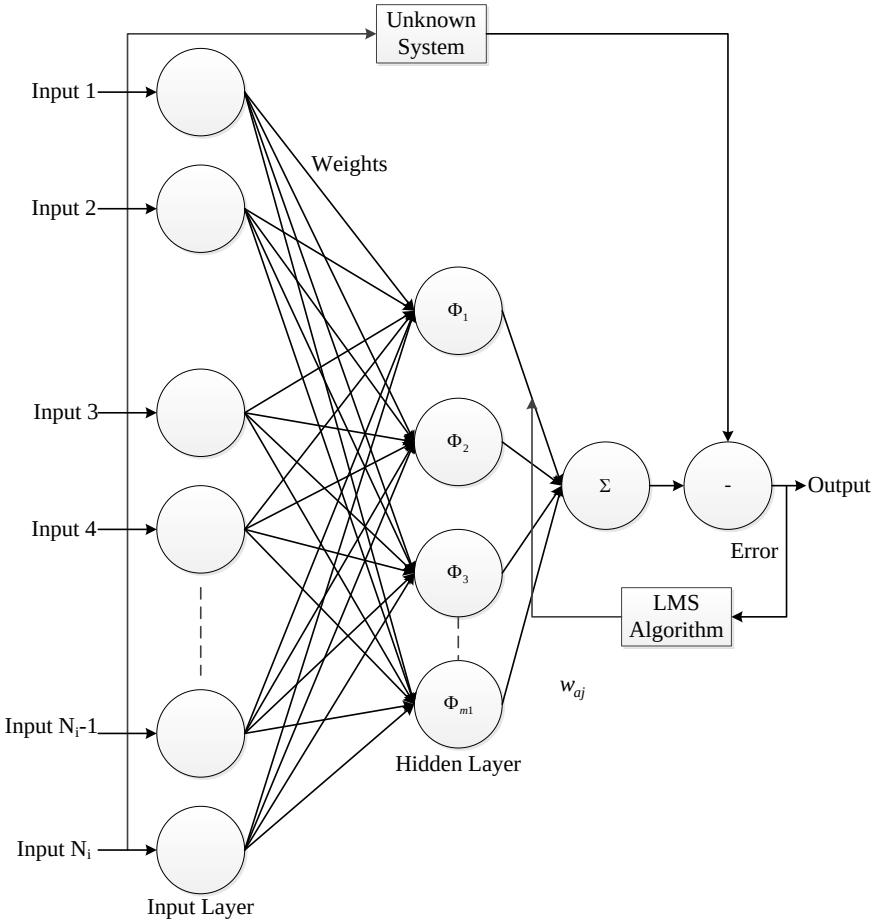

Figure 3.11: Radial basis function network

3.7.1 Fixed Centers Selected at Random

According to this approach the location of the centers are chosen randomly from the input training patterns. The RBF is assumed isotropic Gaussian function whose standard deviation is fixed according to the spread of the centers.

The radial basis function network consists of input layer, hidden layer (radial basis function called radial centres) and output layer. The Fixed RBFN are defined as in equation (3.10).

$$G\left(\left\|X_1 - X_2\right\|^2\right) = \exp\left(-\left(m_1 / d_{\max}^2\right) * \left\|X_1 - X_2\right\|^2\right) \tag{3.10}$$

Where x_1 is the input pattern, x_2 is the coordinates of the center, m_1 is the number of chosen centers or number of nonlinear radial basis functions, d_{max} is the maximum distance between the chosen centers. $||x_1-x_2||$ is the Euclidean distance between x_1 and x_2.

The RBF are multiplied by the respective weights and are summed. The modeled value of performance indices at the m^{th} iteration is given as,

$$PI_{2P}(m) = \sum_{j=1}^{m_1} G\left(\left\|X_1 - X_2\right\|^2\right) * w_{aj}(m) \tag{3.11}$$

Where W_{aj} are the weights connected between the hidden layer and the output layer. The error at the m^{th} iteration is given by,

$$e_{1p}(m) = PI_{1P} - PI_{2P}(m) \tag{3.12}$$

3.7.2 Weight Update Equation

The weights W_{aj} are updated through a linear optimization strategy. The linear optimization strategy employed in this work is the least mean square (LMS) algorithm. The weight update equation as per the LMS algorithm is given by,

$$w_{aj}(m+1) = w_{ai}(m) + \eta_2 * G\left(\left\| X_1 - X_2 \right\|^2\right) * e_{1p}(m) \tag{3.13}$$

The stopping criteria adopted is this model is same as the MFNN model. The training errors, E_{tr} for the RBFN is calculated using equation (3.9). The training phase is completed once the training error seems to reach a desired minimum.

3.8 Prediction of Performance Indices using RBFN

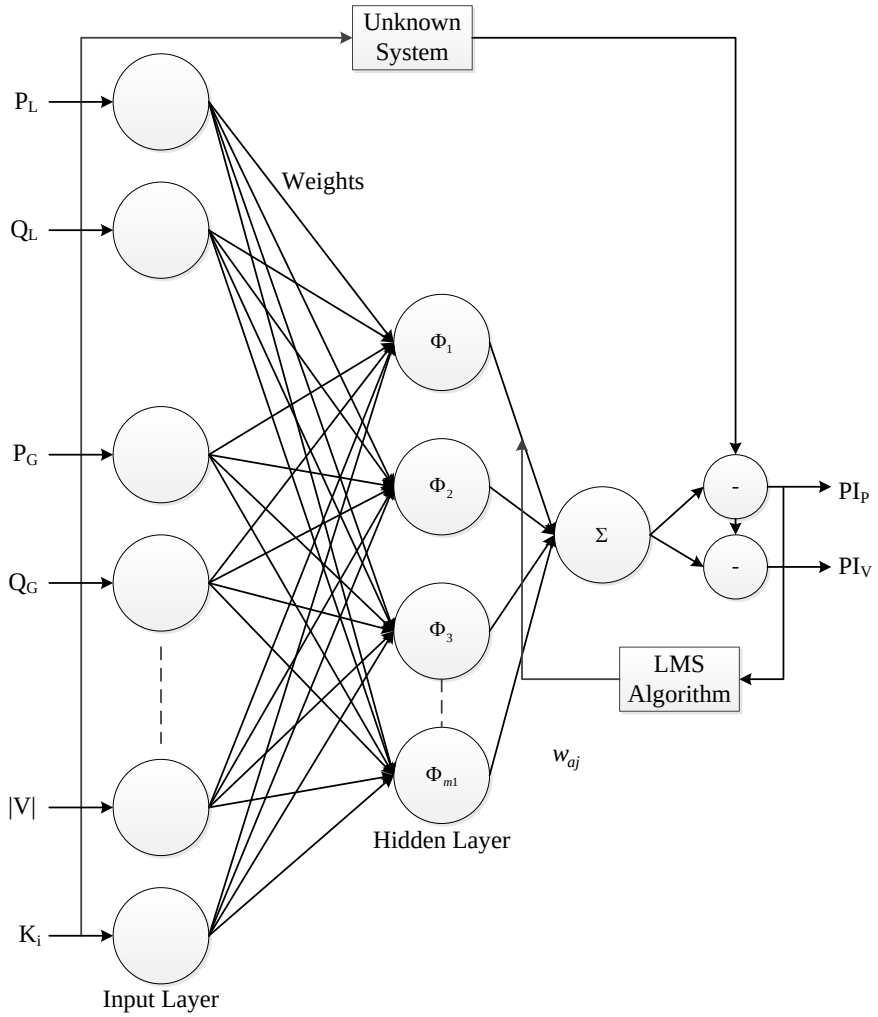

Figure 3.12: RBFN model for the prediction of performance indices

The network is provided with both input data and desired output, and it is trained in a supervised learning fashion, similar to that of MFNN. The weights are updated using the LMS algorithm. The training phase is completed after a series of iterations. Output is compared with the desired response in each iteration, and a match is obtained. The Figure 3.12 shows the RBFN model designed to predict the performance indices. This model has used the same number of input-output parameters as in the MFNN model. The number of input parameters to the network is six, that is, active and reactive power at all the load bus (P_L,Q_L) and generator buses (P_G,Q_G), the voltage magnitudes |V| at all the buses along with the N-1 line outage contingency (K_i) and the output parameters are active power performance index and voltage performance index. The Figure 3.13 shows the flowchart for the RBFN.

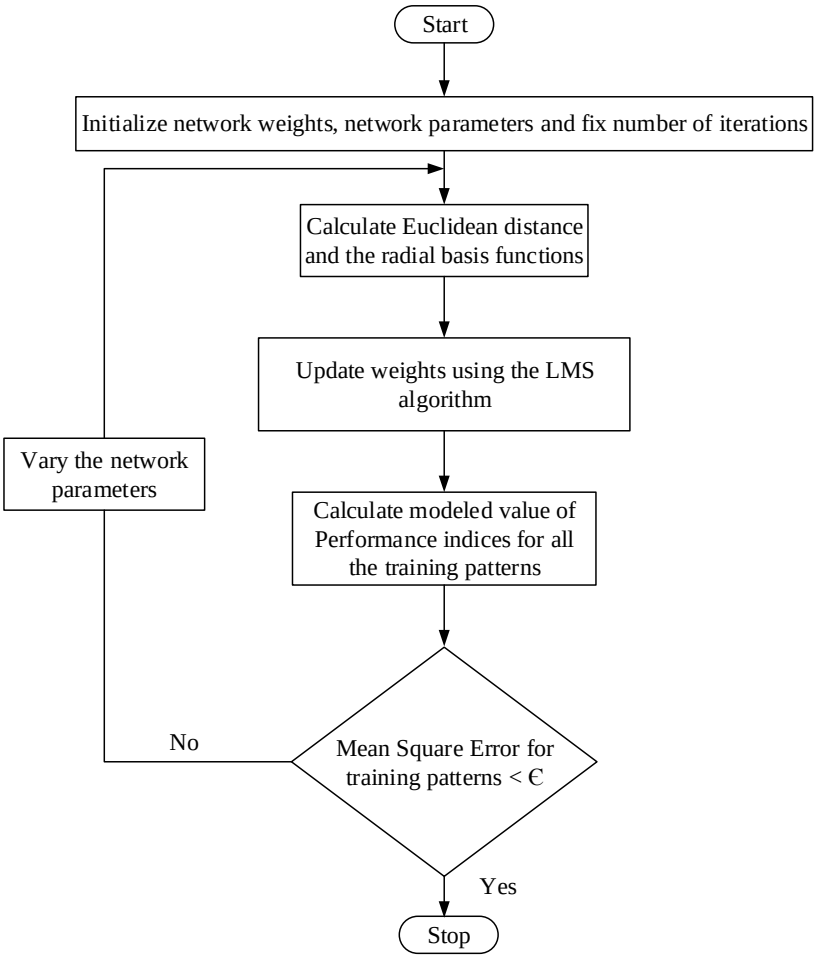

Figure 3.13: Flow chart for RBFN

3.9 Simulation Results and Discussion

3.9.1 Results for IEEE-30 bus System

In this approach, the optimum network parameters are obtained based on mean square error E_{tr} for the training patterns. The network is trained in a sequential order. In applying the RBF and LMS algorithm for the prediction of performance indices, the following important parameters are discussed.

1. Number of chosen centers m_1
2. Learning rate of the LMS algorithm η_2
3. Number of iterations

The data set generated for MFNN is used to train the RBFN architecture. To select the optimal values, the parameters η_2 and m_1 are varied to get the least mean square error for the training data by performing simulation with different values of η_2 and m_1. The combination with least mean square error E_{tr} are selected as the optimal parameters.

Table 3.9: Variation of E_{tr} with no. of centers m_1 (η_2 = 0.1, No. of iterations = 100)

m_1	E_{tr}	m_1	E_{tr}
4	0.3263	22	0.1677
5	0.3237	23	0.1520
6	0.3211	24	0.1322
7	0.3197	25	0.1184
8	0.3176	26	0.1040
9	0.3160	27	0.0924
10	0.3147	28	0.0847
11	0.3120	29	0.0765
12	0.3100	30	0.0677
13	0.3055	31	0.0613
14	0.3001	32	0.0391
15	0.2813	33	0.0334
16	0.2705	34	0.0255
17	0.2537	35	0.0243
18	0.2373	36	0.0230
19	0.2240	37	0.0224
20	0.2028	38	0.0170
21	0.1906	39	0.0219

Table 3.10: Variation of E_{tr} with η_2 (m_1= 38, No. of iterations = 100)

η_2	E_{tr}	η_2	E_{tr}
0.1	0.0170	1.1	$4.6262*10^{-4}$
0.2	0.0113	1.2	$4.0435*10^{-4}$
0.3	0.0033	1.3	$3.3283*10^{-4}$
0.4	0.0031	1.4	$2.7148*10^{-4}$
0.5	0.0030	1.5	$2.2878*10^{-4}$
0.6	0.0021	1.6	$2.0181*10^{-4}$
0.7	0.0013	1.7	$1.8391*10^{-4}$
0.8	$7.5149*10^{-4}$	1.8	$1.6958*10^{-4}$
0.9	$5.3229*10^{-4}$	1.9	242.5707
1.0	$4.8947*10^{-4}$		

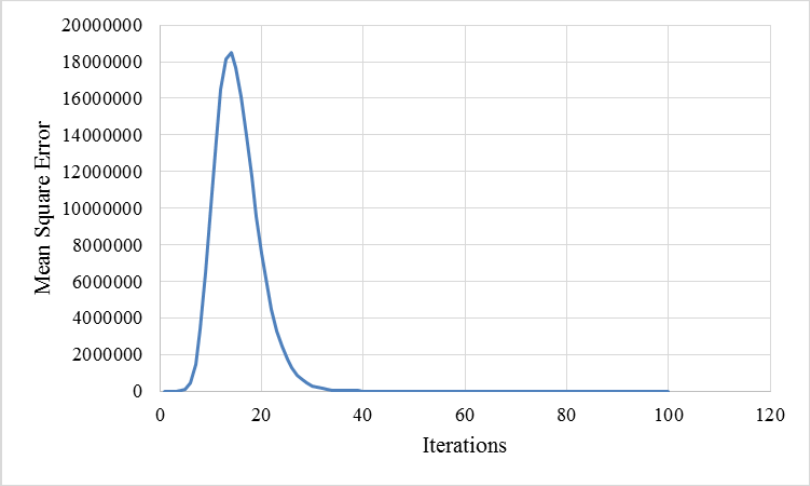

Figure 3.14: E_{tr} vs Iterations for RBFN (for 100 iterations) (IEEE-30 bus system)

The Table 3.9 and Table 3.10 shows the variation of E_{tr} as a function of η_2 and m_1 respectively. It can be observed that the least mean square error E_{tr} is obtained for η_2 = 1.8, m_1 = 38, which are chosen as optimal network parameters. The network structure to predict the performance indices is shown in Figure 3.12, whereas the Figure 3.13 shows the flowchart representation of the prediction approach. The variation of error E_{tr} of the training data with the number of iterations is shown in Figure 3.14.

To test the RBFN model, the base case load condition data is given as input to predict the performance indices which are compared with the indices obtained using NRLF analysis. This approach is similar to the procedure followed for MFNN. The Table 3.11 shows the

comparison of the predicted active power and voltage performance indices, with the conventional NRLF method and its ranking.

Table 3.11: Contingency ranking and Comparison of API and VPI obtained by NRLF method and RBFN (Base load condition for IEEE-30 bus system)

Line Outage	API (NRLF)	API (MFNN) (100 Iterations)	API(RBFN) (100 Iterations)	Line Outage	VPI(NRLF)	VPI (MFNN) (100 Iterations)	VPI (RBFN) (100 Iterations)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
L 1-2	0.7579	0.7579	0.7463	L 6-8	2.2073	2.1987	2.2071
L 2-5	0.7555	0.7455	0.7559	L 6-7	2.1857	2.1968	2.1820
L 9-10	0.7387	0.7373	0.7469	L 6-9	2.1453	2.1906	2.1203
L 4-12	0.7371	0.7362	0.7355	L 24-25	2.1187	2.1819	2.1094
L 12-15	0.6409	0.6409	0.6412	L 23-24	2.0897	2.1590	2.0897
L 6-9	0.6374	0.6374	0.6353	L 8-28	2.0805	2.1447	2.0805
L 6-28	0.6189	0.6189	0.6189	L 22-24	2.0742	2.1315	2.0993
L 27-30	0.6110	0.6110	0.6109	L 21-22	2.0723	2.1268	2.1115
L 10-21	0.6091	0.6091	0.6043	L 6-28	2.0660	2.1091	2.0660
L 15-23	0.6005	0.6005	0.5850	L 14-15	2.0649	2.1057	2.0650
L 22-24	0.6002	0.6002	0.6054	L 18-19	2.0614	2.0944	2.0601
L 6-8	0.5988	0.5988	0.5785	L 29-30	2.0613	2.0941	2.0612
L 25-27	0.5987	0.5987	0.5990	L 16-17	2.0576	2.0817	2.0576
L 12-16	0.5969	0.5969	0.5966	L 3-4	2.0524	2.0650	2.0526
L 15-18	0.5961	0.5961	0.5961	L 27-29	2.0516	2.0626	2.0517
L 27-29	0.5957	0.5937	0.5938	L 27-30	2.0466	2.0496	2.0468
L 10-20	0.5941	0.5941	0.5939	L 5-7	2.0457	2.0476	2.0464
L 10-17	0.5874	0.5874	0.5875	L 19-20	2.0236	2.0233	2.0223
L 12-14	0.5863	0.5863	0.5861	L 15-23	2.0230	2.0228	1.9774
L 18-19	0.5859	0.5859	0.5852	L 10-22	2.0174	2.0179	2.0246
L 19-20	0.5858	0.5858	0.5863	L 4-6	2.0032	2.0034	2.0035
L 24-25	0.5839	0.5839	0.5862	L 6-10	1.9858	1.9856	2.0000
L 16-17	0.5838	0.5838	0.5838	L 10-17	1.9848	1.9846	1.9846
L 23-24	0.5834	0.5835	0.5870	L 25-27	1.9682	1.9683	1.9680
L 10-22	0.5831	0.5831	0.5922	L 15-18	1.9658	1.9659	1.9660
L 21-22	0.5831	0.5831	0.5843	L 2-5	1.9517	1.9517	1.9523
L 2-6	0.5820	0.5820	0.5819	L 2-4	1.9323	1.9322	1.9321
L 4-6	0.5811	0.5811	0.5811	L 2-6	1.9247	1.9247	1.9251
L 8-28	0.5804	0.5804	0.5804	L 10-21	1.9179	1.9179	1.9247
L 14-15	0.5797	0.5797	0.5796	L 10-20	1.9127	1.9127	1.9133
L 29-30	0.5761	0.5761	0.5761	L 12-14	1.8940	1.8940	1.8951
L 6-7	0.5735	0.5735	0.5779	L 12-16	1.8838	1.8838	1.8842
L 6-10	0.5696	0.5696	0.5790	L 1-3	1.8683	1.8683	1.8623
L 1-3	0.5672	0.5672	0.5672	L 1-2	1.8128	1.8128	1.8128
L 3-4	0.5660	0.5660	0.5661	L 4-12	1.6931	1.6931	1.6818
L 2-4	0.5643	0.5643	0.5642	L 12-15	1.6499	1.6499	1.6494
L 5-7	0.5617	0.5617	0.5624	L 9-10	1.5084	1.5084	1.5051

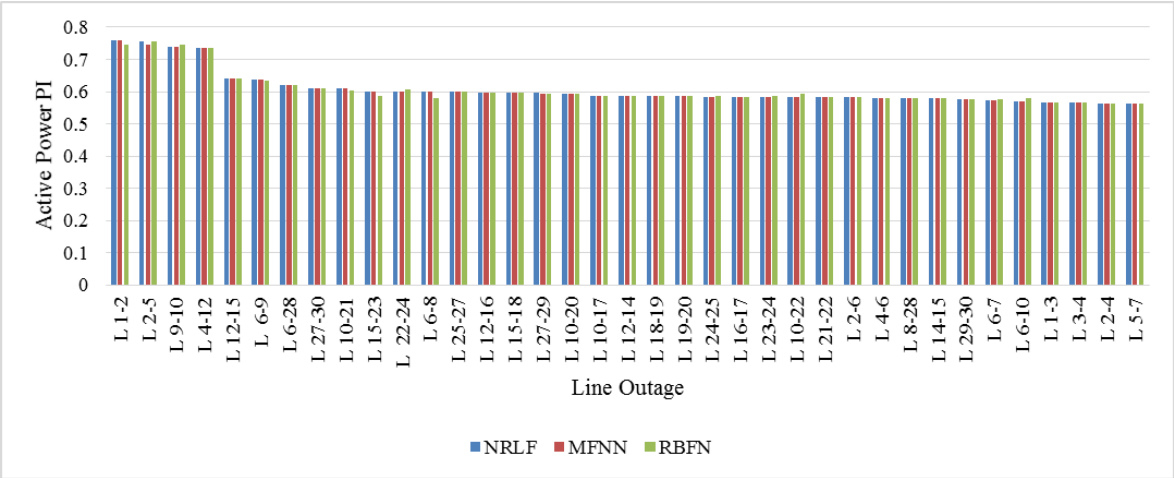

Figure 3.15: Contingency ranking and Comparison of Active Power PI between NRLF and RBFN (IEEE-30 bus system)

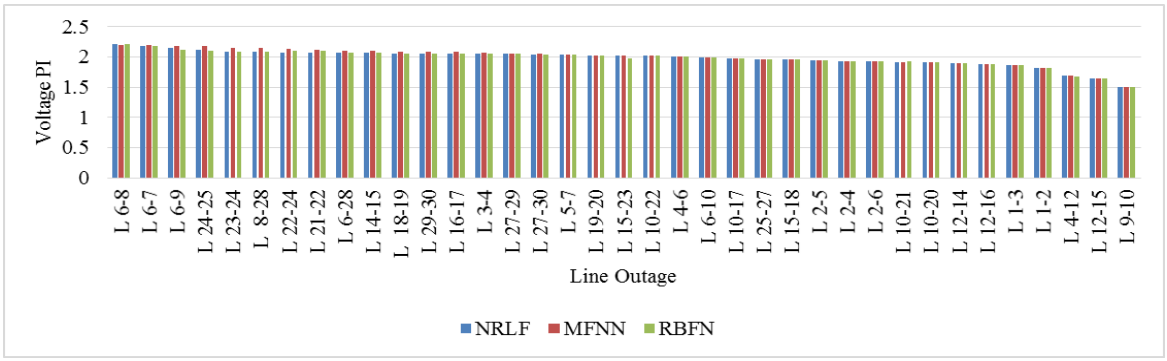

Figure 3.16: Contingency ranking and Comparison of Voltage PI between NRLF and RBFN (IEEE-30 bus system)

The Figure 3.15 and Figure 3.16 shows the comparison and contingency ranking based on the performance indices.

3.9.2 Results for IEEE-57 bus System

Similar to the IEEE-30 bus system, the initial step is to obtain the optimal network parameters. The Table 3.12 and Table 3.13 shows the variation of E_{tr} as a function of η_2 and

m_1 respectively. It can be observed that the least mean square error E_{tr} is obtained for η_2 = 1.7, m_1 = 63, which are chosen as optimal network parameters.

Table 3.12: Variation of E_{tr} with no. of centers m_1 (η_2 = 0.1, No. of iterations = 100)

m_1	E_{tr}	m_1	E_{tr}
41	0.0250	53	0.0107
42	0.0207	54	0.0108
43	0.0189	55	0.0095
44	0.0186	56	0.0080
45	0.0167	57	0.0079
46	0.0163	58	0.0066
47	0.0152	59	0.0062
48	0.0143	60	0.0055
49	0.0142	61	0.0047
50	0.0136	62	0.0050
51	0.0134	63	0.0044
52	0.0121	64	0.0055

Table 3.13: Variation of E_{tr} with η_2 (m_1= 63, No. of iterations = 100)

η_2	E_{tr}	η_2	E_{tr}
0.1	0.0044	1.0	1.5544*10-4
0.2	0.0015	1.1	1.3870*10-4
0.3	8.3605*10-4	1.2	1.2471*10-4
0.4	5.6172*10-4	1.3	1.1283*10-4
0.5	4.0005*10-4	1.4	1.0267*10-4
0.6	3.0255*10-4	1.5	9.3964*10-5
0.7	2.4256*10-4	1.6	8.6490*10-5
0.8	2.0355*10-4	1.7	8.0044*10-5
0.9	1.7619*10-4	1.8	0.0043

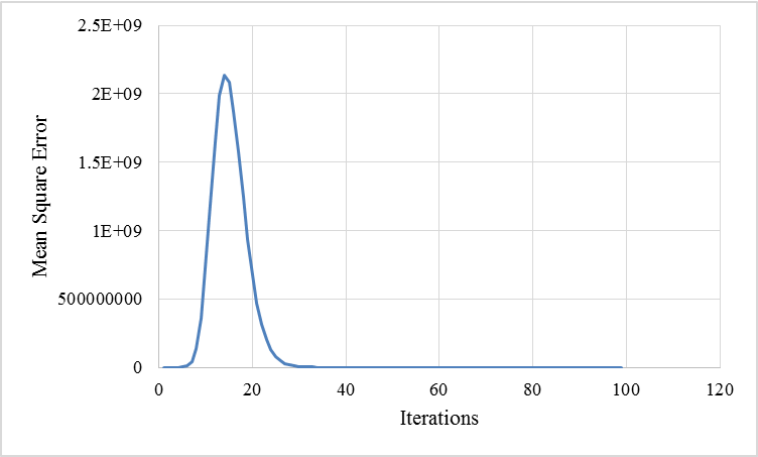

Figure 3.17: E_{tr} vs Iterations for RBFN (for 100 iterations)

The variation of error E_{tr} of the training data with the number of iterations is shown in Figure 3.17.

To test the RBFN model, the 60% load variation data is given as input to predict the performance indices which are compared with the indices obtained using NRLF analysis.

Table 3.14: Contingency ranking and Comparison of API and VPI obtained by NRLF method and RBFN (60% load condition for IEEE-57 bus system)

Line Outage	API (NRLF)	API (MFNN) (100 Iterations)	API (RBFN) (100 Iterations)	Line Outage	VPI(NRLF)	VPI (MFNN) (100 Iterations)	VPI (RBFN) (100 Iterations)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
L 4-6	9.7762	9.6309	9.7768	L 7-29	49.1919	48.5541	49.2038
L 5-6	8.7931	8.7931	8.7732	L 37-38	42.6579	42.6576	42.6337
L 8-9	7.4949	7.4949	7.4821	L 36-37	23.5421	23.5422	23.8821
L 7-29	6.0483	6.0483	6.0507	L 28-29	21.9972	21.9972	21.9808
L 3-4	5.4184	5.4184	5.7134	L 4-6	17.3254	17.3256	17.3286
L 37-38	5.3207	5.3207	5.4687	L 27-28	13.0076	13.0073	12.9631
L 36-37	5.2024	5.2024	5.4197	L 22-38	10.0366	10.0362	11.0959
L 1-15	5.1414	5.1414	5.4154	L 1-15	9.6956	9.6952	9.5169
L 1-17	5.0948	5.0948	5.2309	L 8-9	8.7644	8.7641	8.8093
L 28-29	4.9123	4.9124	4.9914	L 5-6	8.7204	8.7201	8.7000
L 7-8	4.7285	4.7285	4.9090	L 46-47	8.6099	8.6096	8.6330
L 27-28	4.7048	4.7048	4.7196	L 14-46	8.4288	8.4286	8.6205
L 1-16	4.6541	4.6541	4.6959	L 22-23	8.238	8.2378	8.5766
L 22-38	4.6191	4.6191	4.6918	L 26-27	6.1467	6.1470	6.1724
L 46-47	4.6117	4.6117	4.6409	L 38-48	5.9441	5.9443	5.9941
L 14-46	4.6115	4.6115	4.6344	L 13-49	5.9226	5.9228	5.9225
L 22-23	4.5209	4.5209	4.6163	L 7-8	5.8262	5.8263	5.7812
L 4-18	4.5015	4.5015	4.5663	L 30-31	5.6601	5.6600	5.6570
L 14-15	4.4990	4.4990	4.5158	L 24-26	5.5838	5.5836	5.5064
L 2-3	4.4770	4.4770	4.5016	L 1-17	5.4874	5.4871	5.3979
L 9-55	4.4755	4.4755	4.4799	L 12-13	5.3175	5.3170	5.3063
L 41-42	4.4731	4.4731	4.4792	L 44-45	5.3062	5.3057	5.2654
L 29-52	4.4668	4.4668	4.4668	L 15-45	5.2792	5.2787	5.2166
L 10-51	4.4652	4.4653	4.4652	L 3-4	4.8993	4.8987	4.0654
L 11-43	4.4603	4.4603	4.4603	L 18-19	4.8097	4.8092	4.8841
L 44-45	4.4415	4.4415	4.4435	L 47-48	4.7467	4.7463	4.8249
L 15-45	4.4414	4.4414	4.4415	L 10-51	4.6144	4.6142	4.7977
L 38-48	4.3877	4.3877	4.4391	L 14-15	4.4900	4.4901	4.7506
L 41-43	4.3853	4.3853	4.4387	L 38-44	4.4821	4.4822	4.6567
L 13-49	4.3759	4.3759	4.3877	L 24-25	4.4162	4.4165	4.6145
L 52-53	4.3745	4.3745	4.3759	L 41-42	4.3288	4.3293	4.5033
L 18-19	4.3680	4.3680	4.3745	L 24-25	4.2959	4.2965	4.4430
L 47-48	4.3669	4.3669	4.3710	L 1-16	4.2533	4.2540	4.4214

L 49-50	4.3542	4.3542	4.3677	L 21-22	4.1498	4.1508	4.2350
L 38-44	4.3530	4.3530	4.3550	L 23-24	4.0964	4.0975	4.2018
L 21-20	4.3359	4.3359	4.3540	L 11-43	4.0611	4.0622	4.1206
L 21-22	4.3359	4.3359	4.3512	L 36-40	3.9043	3.9053	4.0883
L 6-8	4.3344	4.3344	4.3358	L 10-12	3.8592	3.8601	4.0611
L 9-11	4.3325	4.3325	4.3318	L 4-48	3.8375	3.8383	3.8768
L 56-41	4.3311	4.3311	4.3274	L 21-20	3.8294	3.8302	3.8610
L 13-15	4.3291	4.3291	4.3247	L 13-15	3.8213	3.8220	3.8239
L 9-10	4.3223	4.3223	4.3199	L 38-49	3.8026	3.8032	3.6403
L 31-32	4.3117	4.3117	4.3136	L 12-17	3.7974	3.7980	3.6314
L 24-26	4.2965	4.2965	4.3122	L 41-43	3.7613	3.7617	3.6157
L 26-27	4.2965	4.2965	4.3081	L 52-53	3.6403	3.6396	3.6061
L 24-25	4.2931	4.2931	4.3005	L 50-51	3.6315	3.6307	3.5764
L 12-13	4.2921	4.2921	4.2975	L 9-10	3.6278	3.6270	3.5656
L 6-7	4.2917	4.2917	4.2957	L 31-32	3.6037	3.6025	3.5434
L 54-55	4.2900	4.2900	4.2900	L 29-52	3.5764	3.5749	3.5236
L 30-31	4.2889	4.2889	4.2888	L 4-18	3.562	3.5602	3.4723
L 48-49	4.2874	4.2874	4.2883	L 11-4	3.5351	3.5329	3.4420
L 11-13	4.2873	4.2873	4.2873	L 13-14	3.4715	3.4681	3.4321
L 23-24	4.2873	4.2873	4.2855	L 2-3	3.4614	3.4578	3.4048
L 37-39	4.2869	4.2869	4.2836	L 37-39	3.447	3.4430	3.3991
L 39-57	4.2869	4.2869	4.2811	L 9-11	3.4442	3.4402	3.3921
L 56-42	4.2862	4.2862	4.2686	L 49-50	3.4428	3.4388	3.3192
L 57-56	4.2838	4.2838	4.2662	L 56-41	3.3981	3.3930	3.3096
L 9-13	4.2817	4.2817	4.2659	L 54-55	3.3921	3.3868	3.2995
L 12-17	4.2817	4.2817	4.2650	L 9-55	3.3781	3.3724	3.2945
L 19-20	4.2775	4.2775	4.2621	L 6-8	3.3299	3.3229	3.2748
L 13-14	4.2770	4.2770	4.2570	L 48-49	3.3195	3.3122	3.2494
L 12-16	4.2765	4.2765	4.2445	L 53-54	3.3096	3.3019	3.1749
L 38-49	4.2746	4.2746	4.2420	L 57-56	3.2034	3.1920	3.1714
L 10-12	4.2720	4.2720	4.2366	L 3-15	3.1953	3.1836	3.1183
L 24-25	4.2714	4.2714	4.2348	L 56-42	3.1938	3.1820	3.1151
L 9-12	4.2712	4.2712	4.2279	L 9-13	3.1808	3.1685	3.1060
L 4-18	4.2678	4.2678	4.2252	L 11-13	3.1805	3.1682	3.0934
L 3-15	4.2645	4.2645	4.1881	L 12-16	3.1786	3.1662	3.0707
L 11-4	4.2582	4.2592	4.1298	L 19-20	3.1725	3.1599	2.8840
L 40-56	4.2571	4.2571	4.1259	L 9-12	3.1451	3.1313	2.8515
L 36-40	4.2522	4.2522	4.0828	L 6-7	3.0854	3.0690	2.8110
L 53-54	4.2445	4.2445	4.0727	L 39-57	3.0349	3.0161	2.5313
L 50-51	4.2348	4.2348	4.0588	40-56	2.8518	2.8231	2.4349

The Table 3.14 shows the comparison of the predicted active power and voltage performance indices, with the conventional NRLF method and its ranking The Figure 3.18 and Figure 3.19 shows the comparison of contingency ranking and performance indices.

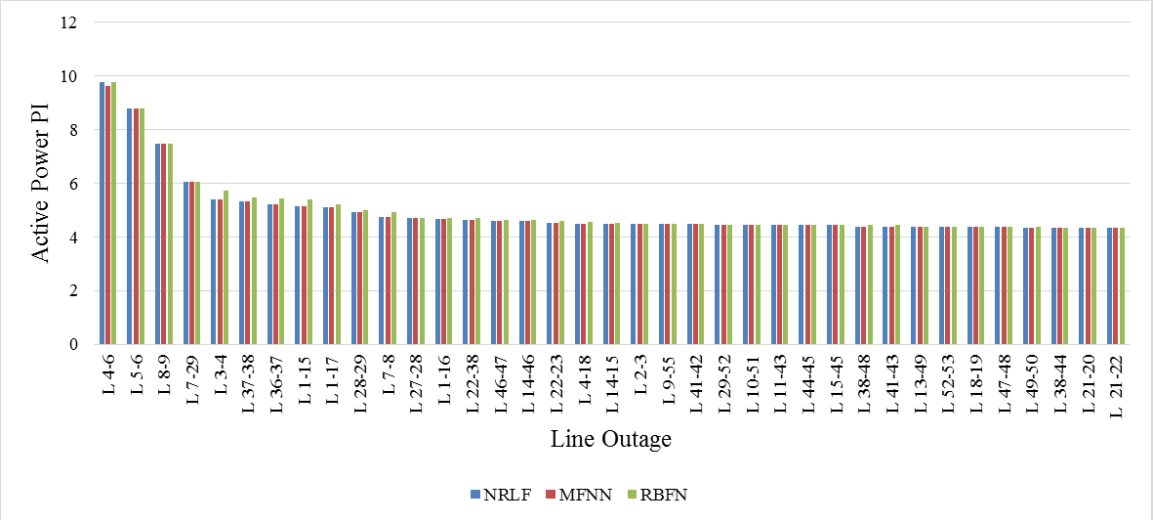

Figure 3.18: Contingency ranking and Comparison of Active Power PI between NRLF and RBFN (IEEE-57 bus system)

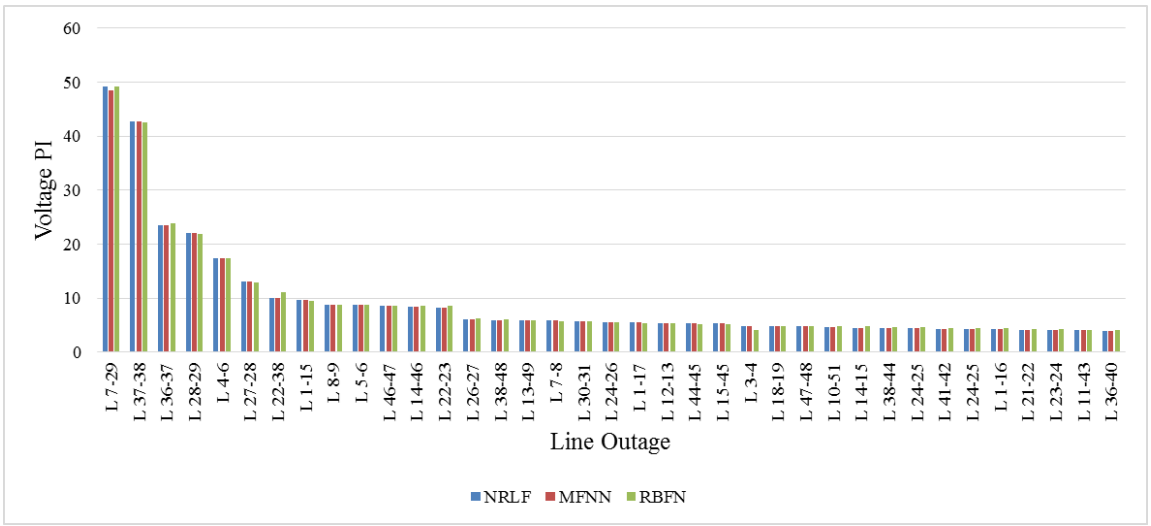

Figure 3.19: Contingency ranking and Comparison of Voltage PI between NRLF and RBFN (IEEE-57 bus system)

The Table 3.11 shows the performance indices and contingency ranking for the base case load condition and the Table 3.14 shows the performance indices and contingency ranking for 60% variation in load condition. The 1st and 5th columns of respective tables shows the

various line outages ranked based on severity using active power performance index and voltage performance index computed using NRLF analysis, as shown in 2nd and 6th columns of respective tables. The 4th and 8th columns of Table 3.11 and Table 3.14 shows the active power and voltage performance indices values obtained using the RBFN model. It can be observed that for all the critical contingencies, the predicted values and ranking are almost equal by the module using RBFN model in comparison with columns 2 and 6 respectively. Here, the top critical contingencies need to be given higher priority during security evaluation. Once the critical contingencies are identified, the operational engineers should take necessary preventive and control actions.

Further, the time taken by the model is found to be 0.82 sec (IEEE-30 bus system) for 100 iterations and 2.49 sec (IEEE-57 bus system) for 100 iterations. From this, it is clear that the ranking module for security assessment by contingency ranking is very quick and accurate for unseen system conditions. From the simulation results and above discussion, for various system operating conditions, the ranking module using MFNN and RBFN is found to be quick and efficient approach to predict the performance indices and rank the contingencies. Thus, the MFNN and RBFN based ranking model is found feasible for online implementation for security assessment by contingency ranking.

3.10 Summary

In this chapter, the prediction of active power performance index and voltage performance index using MFNN and RBFN models are presented. The simulation results clearly shows that both the MFNN and RBFN are quiet effective in predicting the performance indices within reasonable number of iterations in quick time. Thus, the ranking module with MFNN and RBFN models is efficient to predict the system severity for security assessment by contingency ranking, which makes it feasible for real time implementation.

Chapter 4

Classification and Assessment of Power System Security using Decision Tree Classifier

4.1 Introduction

In chapter 3, two neural network models namely, the MFNN and the RBFN are used to predict the performance indices in order to assess the system security by contingency ranking approach. The results are compared with the conventional method using NRLF analysis. The numerical results revealed that the MFNN and the RBFN are efficient in predicting the performance indices for unseen network conditions within reasonable number of iterations. However, apart from the contingency ranking approach for the security assessment, there exists another method to evaluate the security of the power system, known as the classification approach. In this approach, the security status is classified into secure and insecure classes for security assessment. In this chapter, the security assessment by classification approach is presented.

This chapter presents the classification of the power system static security status using the decision tree pattern classifier model. To evaluate the stress on the system under contingency, an index known as static severity index is used, which is computed using NRLF method under N-1 line outage contingency. The SSI is obtained for variable load and generating conditions. The data generated is used to design the multiclass security problem,

where the DT is trained and tested to classify the security status. Finally, the classification accuracy is computed in order to study the efficiency and robustness of the classifier.

This chapter is organized as follows: Section 4.2 presents the brief introduction to pattern recognition, Section 4.3 presents the brief introduction of the security classifier model. The Section 4.4 discuss the static security assessment, Section 4.5 presents the data generation and design of the multiclass security problem. The Section 4.6 discuss the design of the decision tree based security classifier model, followed by the details of the decision tree classifier model for security classification in Section 4.7. The simulation results and discussions are presented in Section 4.8. Finally in Section 4.9, the concluding remarks are provided.

4.2 Pattern Recognition

The Pattern recognition is a branch of machine learning discovering the spotlights on the identification of patterns and consistency in data set. A statistical pattern recognition can be characterized as a strategy, which for each given input data, it assigns an output derived from a previously assessed model. The pattern recognition system is named based on the output type of the system. If the output is numerical value, then it is termed as regression, whereas, if the output is the label of the one of the classes defined before, then it is named as *classification*. The classification approach is one of the example of pattern recognition, which endeavors to assign a typical data or input to one of the designed classes. The estimation of the model utilized by the system by the use of data samples is called as *learning*. If the learning process utilize the output values of the data samples, then it is termed as *supervised learning*. If the learning process does not utilize the output values of the data samples, then it is termed as *unsupervised learning*.

The application of the pattern recognition is found in many areas such as, engineering, science, finance and management etc. The pattern recognition approach has gained importance in the field of electrical engineering, where its application is found in power system security assessment. This approach is used to study the security patterns to decide or predict the security nature of the system. One of the pattern recognition approach is classification, which is implemented in chapter-4, to classify the security status by recognizing the security patterns.

4.3 Security Classifier Model

This research work proposes a pattern classifier model for security assessment by classification. The Figure 4.1 shows the approach for security assessment by pattern recognition approach. In the off-line stage, an efficient pattern classifier system is designed for security assessment. This stage includes data generation and classification scheme. The data patterns is generated to design the classifier system. In the classification scheme, based on the training data, a classifier model is developed by utilizing a suitable learning algorithm in the classifier design block. The trained model is tested for its performance with the testing samples.

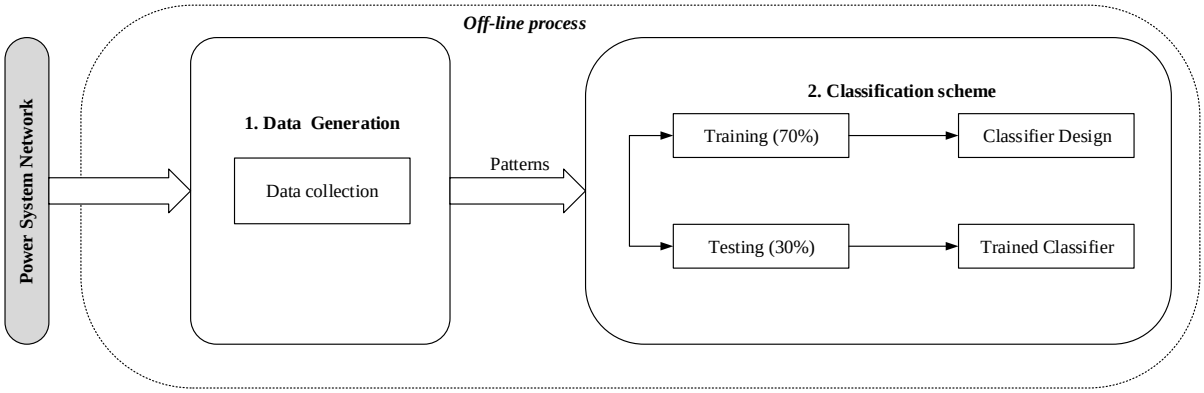

Figure 4.1: Block diagram of security classifier scheme

4.4 Static Security Assessment

As discussed in previous section 4.2, the stress of a contingency need to be computed for variable system operating conditions. Thus, this section presents the formulation to obtain the system severity under contingency scenario. The capability of the power system to regain stable state inside the stated security limit after a contingency is stated as the 'static security'. The primary considerations in this analysis are the bus voltages and transmission line flow violations. If the two parameters are within the limits, then the system is said to be secure. Thus, in order to assess the security of the system for an N-1 contingency, an index called static security index (SSI) is used, which takes into consideration, the bus voltage and the line flow violations.

$$LOI_{pq} = \begin{cases} \dfrac{S_{pq} - S_{pq}^{\max}}{S_{pq}} \times 100 & if\ S_{pq} > S_{pq}^{\max} \\ 0 & if\ S_{pq} \le S_{pq}^{\max} \end{cases} \tag{4.1}$$

The SSI is computed using the line overload index parameter (LOI), which computes the line flow violations and the voltage deviation index (VDI) parameter, which computes the voltage deviation. These two parameters are given in equations (4.1) and (4.2).

$$VDI_p = \begin{cases} \dfrac{\left|V_p^{\min}\right| - \left|V_p\right|}{\left|V_p^{\min}\right|} \times 100 & if\ \left|V_p\right| < \left|V_p^{\min}\right| \\ \dfrac{\left|V_p\right| - \left|V_p^{\max}\right|}{\left|V_p^{\max}\right|} \times 100 & if\ \left|V_p\right| > \left|V_p^{\min}\right| \\ 0 & otherwise \end{cases} \tag{4.2}$$

With these two parameters, the comprehensive term, SSI is given in equation (4.3), which gives the severity of the specific N-1 contingency.

$$SSI = \frac{W_1 \sum_{i=1}^{N_l} LOI_i + W_2 \sum_{i=1}^{N_b} VDI_i}{N_l + N_b} \tag{4.3}$$

The weighting factors assumed for the line overload index as $W_1 = 3$ and for VDI as $W_2 = 2$. The weighting factors selected are based on the importance of the system security. The SSI is computed for the variable load and generating conditions in order to obtain the security patterns, which are used to design the security problem, as discussed in section 4.3.

4.5 Data Generation and Design of the Multiclass Problem

The classification of the online security condition of the power system is the initial step in the security monitoring mechanism. This can be achieved through pattern recognition [82], which minimizes the real-time computing. This task is accomplished by large amount of

tasks done in an off-line mode.

The pattern classifier system based security problem is divided into two stages. In the first stage, the patterns [83] are generated in an offline mode under N-1 contingency scenario, and its security level SSI is computed. In the second stage, the generated patterns are used to train and test the classifier for the security classification.

The efficiency of any pattern classifier depends on the range of patterns generated through offline simulations, which cover the total operating states of the power system [84]. In the present work, an IEEE-30 bus and IEEE-57 bus systems are considered, and the data is generated by simulating N-1 line outage contingency (using NRLF method). The load and the generator operating conditions are varied from 50% to 150% (for IEEE-30 bus system) and 10% to 90% (for IEEE-57 bus system) of its base case. However, the change in the generation is limited to its maximum limits. The pattern vector is selected from the variables obtained through the load flow solution. The attributes used in the pattern vector for the security assessment is given below.

$$P_{SSA} = \left[V_p \; \theta_p \; S_{Gp} \; S_{Lp} \; S_{pq} \; SSI \; Class \right]$$

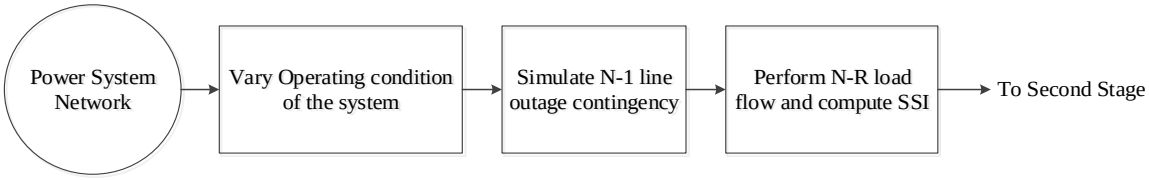

Figure 4.2: Offline procedure to compute static security index (stage 1)

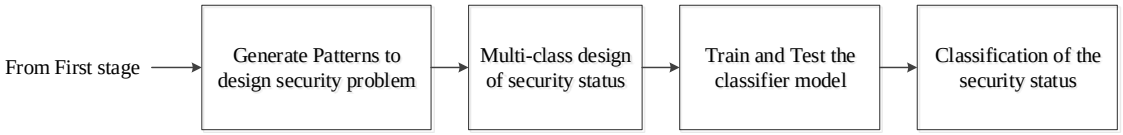

Figure 4.3: Classifier system for the security evaluation (stage 2)

The Figure 4.2 shows the offline procedure followed to compute the SSI in order to apply the pattern classification approach for the security assessment problem. The Figure 4.3 shows

the second stage, where the generated security patterns are used to design multiclass security problem.

Here, the SSI is assigned to one of the four classes namely, static secure, static critically secure, static insecure and static highly insecure, for the security evaluation as shown in Table 4.1. The SSI computed for security assessment is a percentage measure ranging from 0 to 100. Higher value of SSI signifies the more severe nature of the security level. With this idea, the range of SSI for each class label have been fixed. If SSI = 0 & SSI $\leq$ 1 then it is labelled as static secure with class A category. Similarly, if SSI > 1 & SSI $\leq$ 5 then it is labelled as static critically secure with class B category. If SSI > 5 & SSI $\leq$ 15 then it is labelled as static insecure with class C category and if SSI > 15 then it is labelled as static highly insecure with class D category.

Table 4.1: Multiclass design for power system static security assessment

Static Security Index (SSI)	**Label / Class Category**
SSI = 0 & SSI $\leq$ 1	Static secure / Class A
SSI > 1 & SSI $\leq$ 5	Static critically Secure / Class B
SSI > 5 & SSI $\leq$ 15	Static Insecure / Class C
SSI > 15	Static Highly Insecure / Class D

In real time, the problem definition depends on the security requirement and limits. In this study, a four class security problem is considered for the classification and assessment. The objective of the classifier model is to classify the unseen security patterns to one among the four security classes, respectively, without any false alarm. Once the security patterns and the multiclass problem is designed, then the next task is to train and test the classifier model.

4.6 Design of Decision Tree Security Classifier Model

The Figure 4.4 shows the block diagram model of the decision tree based security classifier. This structure shows the entire procedure to implement the decision tree classifier for power system security assessment by classification approach.

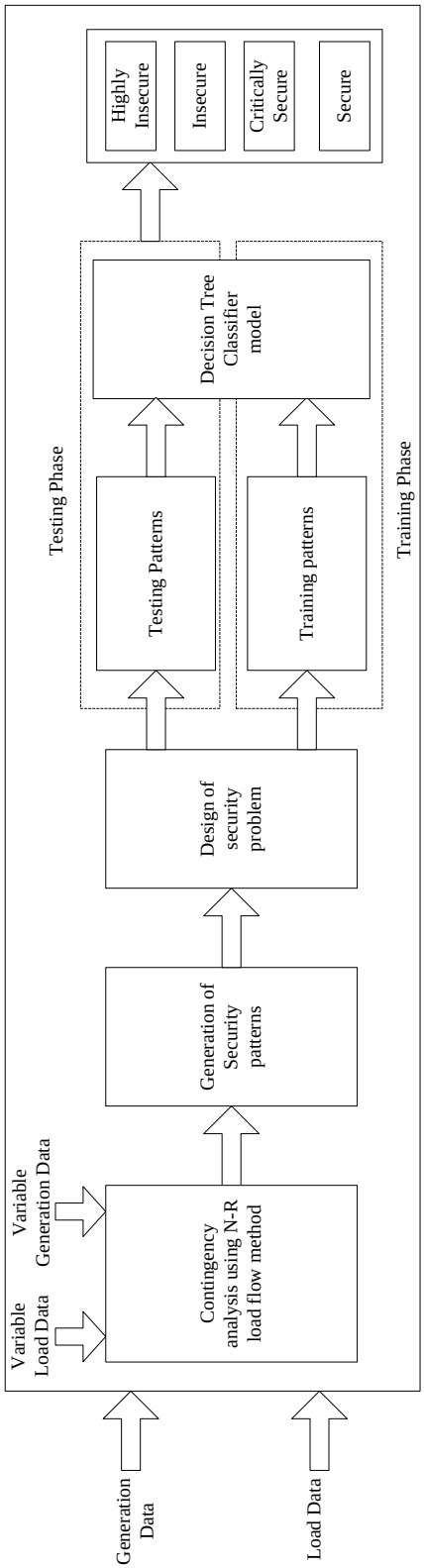

Figure 4.4: Block diagram of Decision Tree based Security Classifier model

1) Initially, the load and the generator data are given as the inputs.
2) With the provided data, the contingency analysis is carried out by creating N-1 line outage contingency under variable load and generator conditions. The NRLF method is used to obtain the severity of the contingency.
3) The contingencies are created for several load and generating conditions in order to obtain the large range of the security patterns covering the entire range of operating states.
4) Then, the important stage is designing the multi-class security problem, for which the generated security patterns need to be classified. The design of the security problem depends on the requirements of the specific security condition. Once, the security problem is designed, some sample of security patterns are given as inputs to train the decision tree classifier model. Once the decision tree classifier is trained, then the remaining set of patterns are given as inputs to test the DT classifier model for its accuracy in classifying the security status.
5) Finally, classification accuracy is computed for the DT classifier model.

4.7 Decision Tree Classifier Model

A classifier is a methodical approach in order to design the classification model from the input data samples. The key function of a learning algorithm is to frame the model with good generalization capability.

In this chapter, a decision tree classifier model is implemented in order to classify the security status for security assessment. A decision tree is defined as, repeatedly separating the input region, and designating a local model for each resulted region of input. The basic decision tree model is shown in Figure 4.5. The root node holds the data set samples and splitting is processed based on a question asked at each node. The split of the main node results in right and left node, which gives further split based on further question. Once, the data set is sufficiently divided based on the features of the data set, then the class that the specific features belongs will be assigned. This class identification should have higher accuracy, which assesses the efficiency of the classifier model.

Several algorithms has been developed for the decision tree model. The classification and regression tree (CART) algorithm based DT was developed by Breiman [85]. Later, C 4.5

(Extension of ID 3 algorithm by Quinlan in 1979), algorithm based DT was developed by Quinlan [86]. The application of the DT is found in many fields of science, technology [87-93] and management. The DT performance is better than the linear models. Moreover it is easy to design and evaluate, making it inexpensive for computation. Once the tree is designed it can be used for any number of data samples.

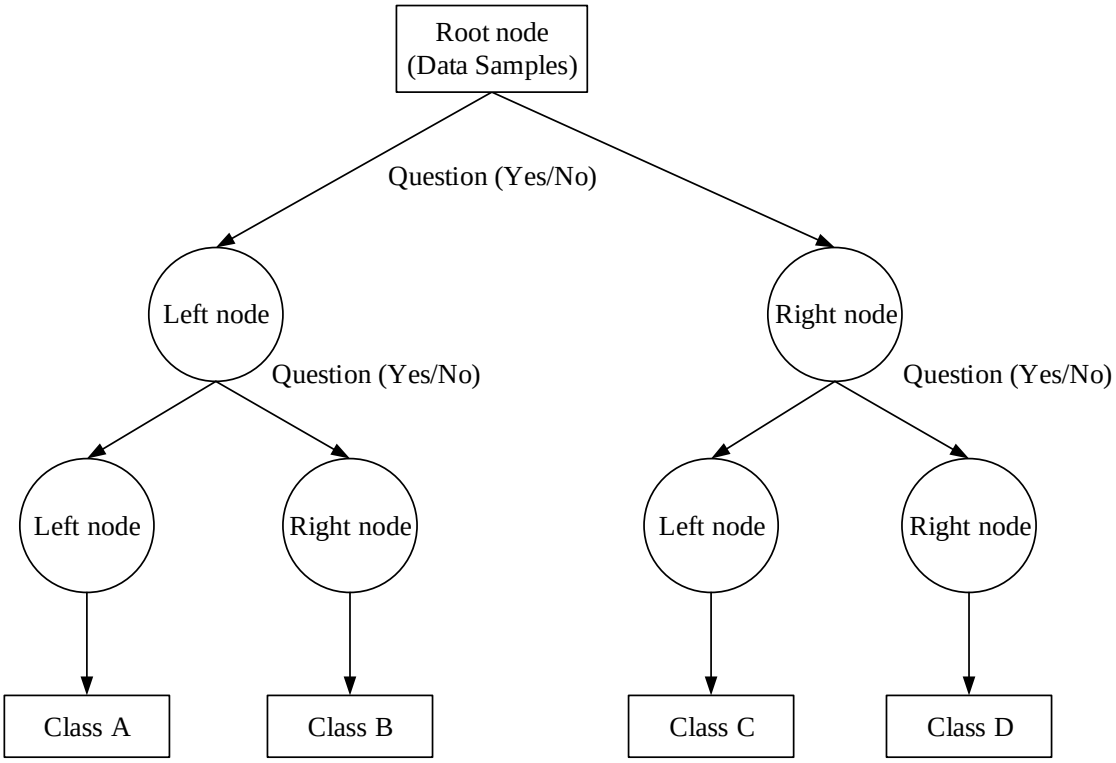

Figure 4.5: Basic decision tree model

The decision tree can be designed from top to down, bottom to up and other special approaches. The most commonly used approach is top to down approach.

1) The approach starts with the entire data samples at a node called the “root node”.
2) The next step is to divide the records or data samples, which have different feature based on the attribute test conditions. This is assigned to a node called the “internal node”.
3) The next step is assigning a class label to a node called the “leaf node”.
4) Once the classifier is designed, the testing of a data sample using the classifier is a simple approach.

A decision tree is used to classify a case, i.e. to assign a class value to a case depending on the values of the attributes of the case. In fact, a path from the root to a leaf of the decision tree can be followed based on the attribute values of the case. The class specified at the leaf is the class predicted by the decision tree.

4.7.1 The Tree Construction Algorithm

The algorithm constructs the decision tree with a divide and conquer strategy. Also, cases are assigned weights to take into account unknown attribute values. At the beginning, only the root is present, with associated the whole training set *TS* and with all case weights equal to 1.0. At each node the following divide and conquer algorithm is executed, trying to exploit the locally best choice, with no backtracking allowed.

The algorithmic steps involved in the Pseudo Code of decision tree model:

```
Form Tree (T)
    (1)  Compute Class Frequency (T);
    (2)  if One Class or Few Cases
             return a leaf;
         Form a decision node N;
    (3)  For each Attribute A
             Compute Gain (A);
    (4)  N.test = Attribute With Best Gain;
    (5)  if N.test is continuous
             find Threshold;
    (6)  For Each T' in the splitting of T
    (7)   if T' is Empty
            Child of N is a leaf
         else
    (8)   Child of N= Form Tree (T');
    (9)  Compute Errors of N;
         return N
```

Step-1: Let T be the set of cases associated at the node. The weighted frequency $freq(C_i, T)$ is computed of cases in T whose class is C_i, for $i \in [1, NClass]$.

Step-2: If all cases in T belong to a same class C_j (or the number of cases in T is less than a certain value) then the node is a leaf, with associated class C_j (respectively the most

frequent class). The classification error of the leaf is the weighted sum of the cases in T whose class is not C_j (respectively the most frequent class).

Step-3: If T contains cases belonging to two or more classes, then the *information gain* of each attribute is calculated. For discrete attributes, the information gain is relative to the splitting of cases in T into sets with distinct attribute values. For continuous attributes, the information gain is relative to the splitting of T into two subsets, namely cases with attribute value *not greater than* and cases with attribute value *greater than* a certain local *threshold*, which is determined during information gain calculation.

Step-4: The attribute with the highest information gain is selected for the test at the node.

Step-5: Moreover, in case a continuous attribute is selected, the *threshold* is computed as the greatest value of the *whole* training set that is below the local threshold.

Step-6: A decision node has "s" children if $T_1,....,T_s$ are the sets of the splitting produced by the test on the selected attribute.

Step-7: For i = [1, s], if T_i is empty, the child node is directly set to be a leaf, with associated class the most frequent class at the parent node.

Step-8: If T_i is not empty, the divide and conquer approach consists of recursively applying the same operations on the set consisting of T_i plus those cases in T with unknown value of the selected attribute.

Step-9: Finally, the classification error of the node is calculated as the sum of the errors of the child nodes. If the result is greater than the error of classifying all cases in T as belonging to the most frequent class in T, then the node is set to be a leaf, and all sub-trees are removed.

4.7.1.1 Information Gain

The information gain of an attribute "a" for a set of cases T is calculated as follows. If "a" is discrete, and $T_1,....,T_s$ are the subsets of T consisting of cases with distinct known value for attribute "a", then:

$$gain = info(T) - \sum_{i=1}^{s} \frac{|T_i|}{|T|} \times info(T_i) \tag{4.4}$$

Where,

$$info(T) = -\sum_{j=1}^{NClass} \frac{freq(C_j, T)}{|T|} \times log_2 \left(\frac{freq(C_j, T)}{|T|} \right) \tag{4.5}$$

is the entropy function. The information gain ratio of the splitting T_1,....,T_s, which is the ratio of information gain to its split information.

$$Split(T) = -\sum_{i=1}^{s} \frac{|T_i|}{|T|} \times log_2 \left(\frac{|T_i|}{|T|} \right) \tag{4.6}$$

When all the nodes reach their adequate level of purity, the algorithm is terminated. This process is implemented in both the training and testing phase in order to obtain the confusion matrix to assess the performance of the classifier model for security assessment.

4.8 Simulation Results and Discussion

The key objective of the DT classifier is to classify the large number of the security patterns to their respective security classes without false alarm. The experiments to test the DT classifier model for the power system static security classification and assessment is employed on IEEE-30 bus and IEEE-57 bus systems on an Intel Core I7 3.40 GHz processor with Windows 7 professional operating system**.**

4.8.1 Results for IEEE-30 bus system

In order to implement the approach, it is necessary to generate the security patterns. The security patterns are obtained through offline simulations performed in MATLAB 2010a environment. The total number of operating scenarios considered are 414. Among the available data, 70% data is used for the training purpose and 30% data is used for testing the classifier model.

Table 4.2: Data generation for SSA (IEEE-30 bus system)

Operating scenarios	**Class**	**414(288+126)**
Static Secure	A	33(23+10)
Static critically secure	B	68(47+21)
Static Insecure	C	104(72+32)
Static Highly Insecure	D	209(146+63)

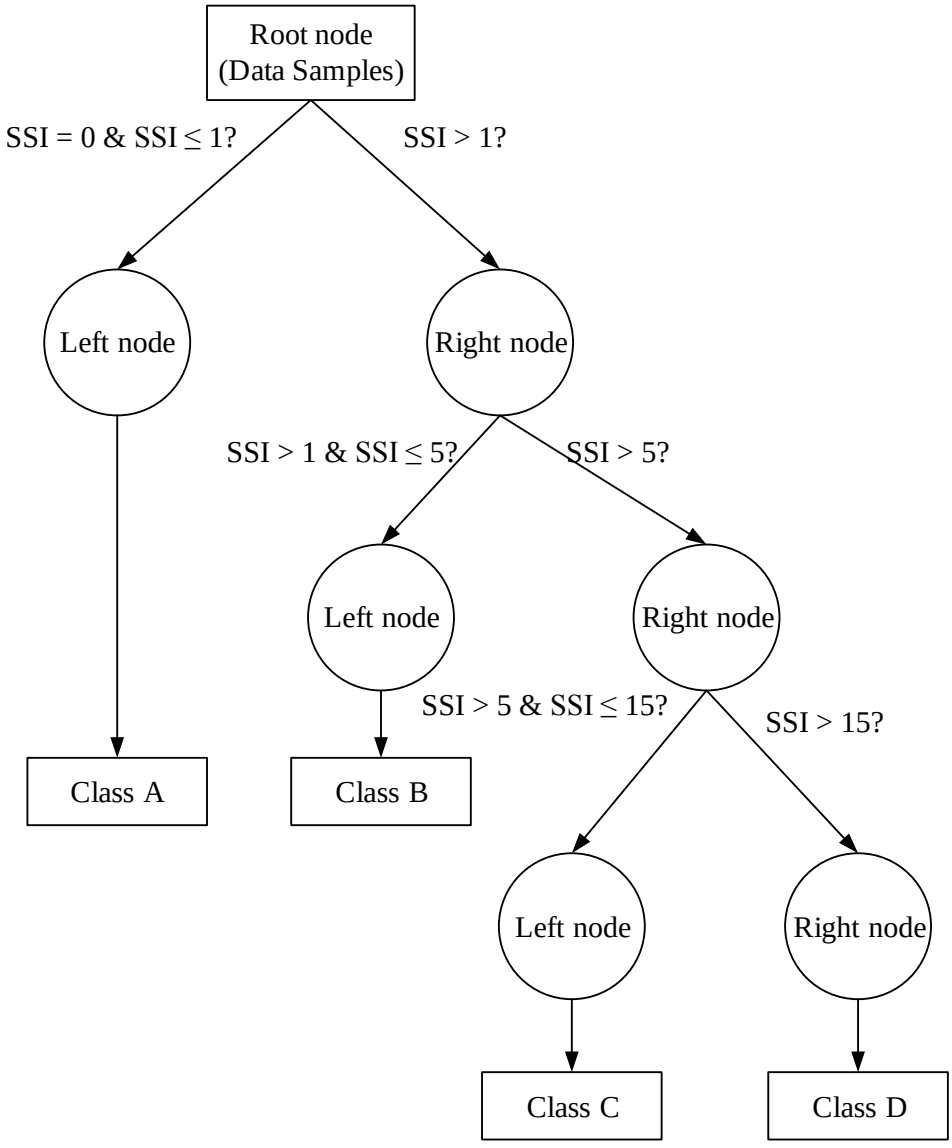

Figure 4.6: Decision tree classifier model for security assessment

The Table 4.2 shows how the data is divided for the training and the testing phase of the classifier model. From Table 4.2, it can be observed that out of 414 data samples, 288 are selected for training and 126 are selected to test the trained classifier. Out of the selected data samples, 33 data samples (23 training +10 testing) belongs to class A, 68 data samples (47 training +21 testing) belongs to class B, 104 data samples (72 training +32 testing) belongs to class C, 209 data samples (146 training +63 testing) belongs to class D. In testing phase, all the data samples that corresponds to their classes stated above must be classified correctly.

The selected data for the training phase as stated above, is used to train the decision tree classifier. The trained classifier should be capable of classifying the unseen security patterns in the testing data to their respective security classes. Any false alarm of the classifier will lead to faulty assessment of the security by the operational engineers, which may lead to system interruption or even blackout. Thus, it is highly necessary to have a classifier module with maximum accuracy and least misclassification rate.

The Figure 4.6 shows the decision tree classifier model for the security assessment. In the root node, all the prepared security data patterns are given as the input features. The decision tree uses the pattern recognition in order to recognize the security patterns based on the input features. At the first node, a question is asked if SSI = 0 & SSI $\leq$ 1. If this condition is satisfied, it is assigned to the left node and that node is saturated and assigned to class A. If SSI > 1 the right node is assigned. At this node, again a question is asked if SSI > 1 & SSI $\leq$ 5. If this condition is satisfied, it is assigned to left node and that node is saturated and class B is assigned. Similarly, the right node is questioned if SSI > 5. Further, if SSI > 5 & SSI $\leq$ 15 it is assigned with class C at the left node and right node is assigned with class D if SSI > 15. Once all the patterns are assigned to the four classes, the model yields the confusion matrix in order to evaluate the performance of the DT classifier model.

4.8.1.1 Confusion matrix

In the field of machine learning, the confusion matrix is a table layout, which contains the information about the actual and the predicted classifications done by a classification model. The performance of such models are evaluated using the data in the matrix. Each column in the matrix represents the instances in a predicted class, while each row represents the instances in an actual class. The confusion matrix is also called as the contingency table or an

error matrix.

Table 4.3: Confusion matrices for the classifier models (IEEE-30 bus system)

Classifier Type	Training	Testing
Decision Tree	Predicted Actual $\begin{pmatrix} 23 & 0 & 0 & 0 \\ 0 & 47 & 0 & 0 \\ 0 & 0 & 72 & 0 \\ 0 & 0 & 0 & 146 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 10 & 0 & 0 & 0 \\ 0 & 18 & 3 & 0 \\ 0 & 0 & 29 & 3 \\ 0 & 0 & 0 & 63 \end{pmatrix}$
Multilayer perceptron	Predicted Actual $\begin{pmatrix} 23 & 0 & 0 & 0 \\ 4 & 43 & 0 & 0 \\ 0 & 1 & 71 & 0 \\ 0 & 0 & 0 & 146 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 10 & 0 & 0 & 0 \\ 0 & 19 & 2 & 0 \\ 0 & 0 & 27 & 5 \\ 0 & 0 & 0 & 63 \end{pmatrix}$
Radial basis function	Predicted Actual $\begin{pmatrix} 23 & 0 & 0 & 0 \\ 4 & 45 & 2 & 0 \\ 0 & 3 & 67 & 0 \\ 0 & 0 & 0 & 146 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 10 & 0 & 0 & 0 \\ 4 & 13 & 8 & 0 \\ 0 & 0 & 26 & 6 \\ 0 & 0 & 0 & 63 \end{pmatrix}$
Support vector machine	Predicted Actual $\begin{pmatrix} 23 & 0 & 0 & 0 \\ 0 & 47 & 0 & 0 \\ 0 & 0 & 72 & 0 \\ 0 & 0 & 0 & 146 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 2 & 0 & 0 & 8 \\ 0 & 2 & 2 & 17 \\ 0 & 0 & 0 & 32 \\ 0 & 0 & 0 & 63 \end{pmatrix}$

By definition, a confusion matrix C is such that $C_{i,j}$ is equal to the number of observations known to be in group *i*, but predicted to be in group *j*. In this study, along with the DT classifier model, the MLP, the RBF and the SVM classifiers are evaluated on the same data set used for the DT classifier model. Initially, the DT classifier is provided with the training samples to build the DT security classifier model. Once it is trained, it will generate the confusion matrix for the security patterns. Once the model is designed, then it is tested with the test samples to classify the security patterns. This will result in confusion matrices showing the classification of the security patterns. The Table 4.3 shows the confusion matrices for the DT, the MLP, the RBF and the SVM classifier models in the

training and the testing phase. These confusion matrices, are used to compute the classification accuracy and misclassification rate of the classifier models.

The confusion matrix in Table 4.3 for the decision tree is analyzed as follows: In the training phase, the total number of security patterns that belongs to class A, class B, class C and class D are 23, 47, 72 and 146 respectively. This means that all the security patterns corresponds to class A, class B, class C and class D, are classified correctly to their respective designed security states or classes. Whereas in the testing phase, the total number of security patterns that belongs to class A, class B, class C and class D are 10, 21, 32 and 63 respectively. The 10 security patterns that belongs to class A are classified correctly. Whereas, out of 21 patterns in class B, 18 security patterns are classified or predicted to class B correctly, but 3 patterns that belong to class B are predicted as class C. similarly, out of 32 patterns in class C, 29 security patterns are classified or predicted to class C correctly, but 3 patterns that belong to class C are predicted as class D. Finally, out of 63 patterns of class D, all the security patterns are classified correctly to its respective class.

To assess the performance of the classifiers, two performance measures are computed in the train and test phases. They are,

Classification Accuracy (CA):

$$\mathrm{CA}(\%) = \frac{\text{No.of data samples classified correctly}}{\text{Total no.of data samples in data set}} \times 100 \tag{4.7}$$

Misclassification rate (MR):

$$\mathrm{MR}(\%) = \frac{\text{No.of misclassification in class Q}}{\text{Total no.of data samples in class Q}} \times 100 \tag{4.8}$$

The equation (4.7) gives how accurately the security status is classified to their respective security classes. Higher accuracy gives the adaptability and the robustness of the classifier model for the security classification. Whereas, equation (4.8) gives the percentage of false alarm or misclassification in a particular class. For example, the security state of a pattern may belong to class A, but the classifier may misclassify to class B, C or D. Thus, for a classifier model, it is necessary to have high classification accuracy and least misclassification. The Figure 4.7 shows the flowchart to implement the classification

approach using the decision tree classifier model.

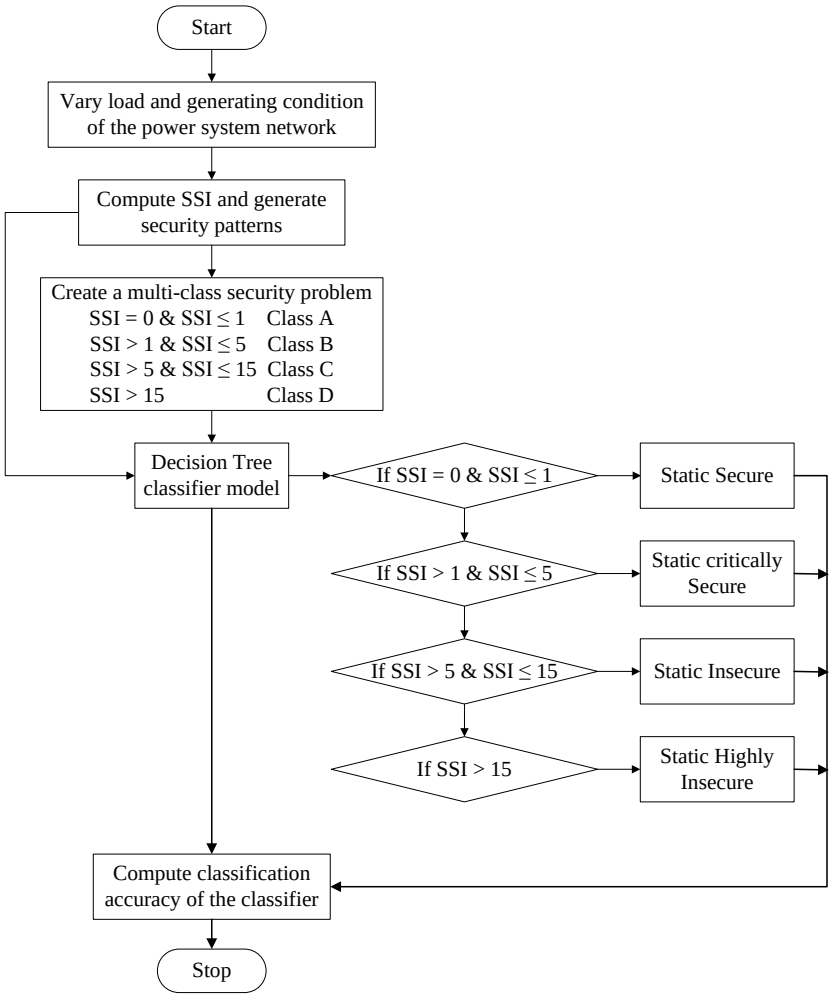

Figure 4.7: Flowchart showing the implementation of decision tree classifier

Table 4.4: Performance Evaluation of the Classifiers (IEEE-30 bus system)

	Classifier Type	CA (%)	Time (Sec)	Misclassification Rate (%)			
				A	B	C	D
Training Phase	DT	100.00	0.03	0	0	0	0
	MLP	98.263	0.38	0	8.51	1.38	0
	RBF	97.569	0.22	0	4.25	4.16	0
	SVM	100.00	0.22	0	0	0	0
Testing Phase	DT	95.238	0.02	0	14.28	9.37	0
	MLP	94.444	0.33	0	9.52	15.62	0
	RBF	88.888	0.23	0	38.09	18.75	0
	SVM	53.174	0.09	80	90.47	100	0

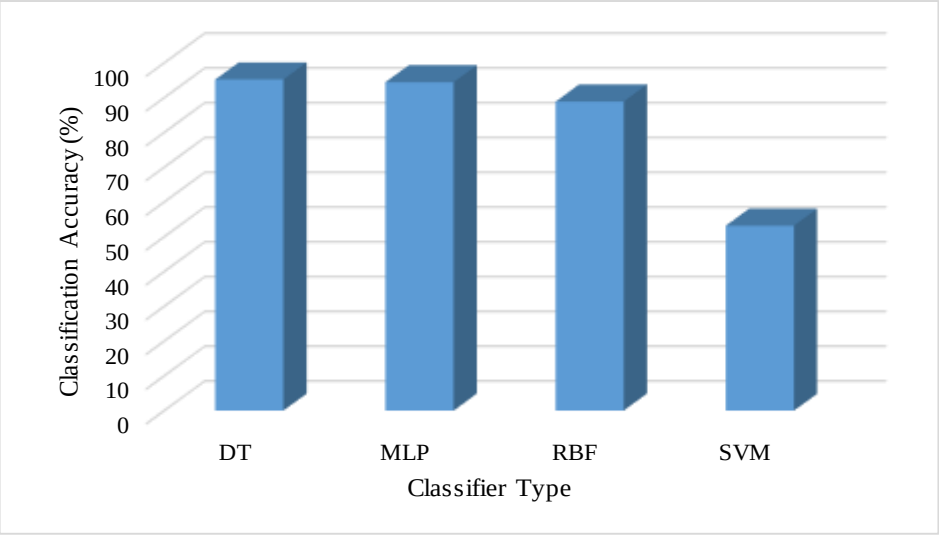

Figure 4.8: Performance comparison of the classifier models (IEEE-30 bus system)

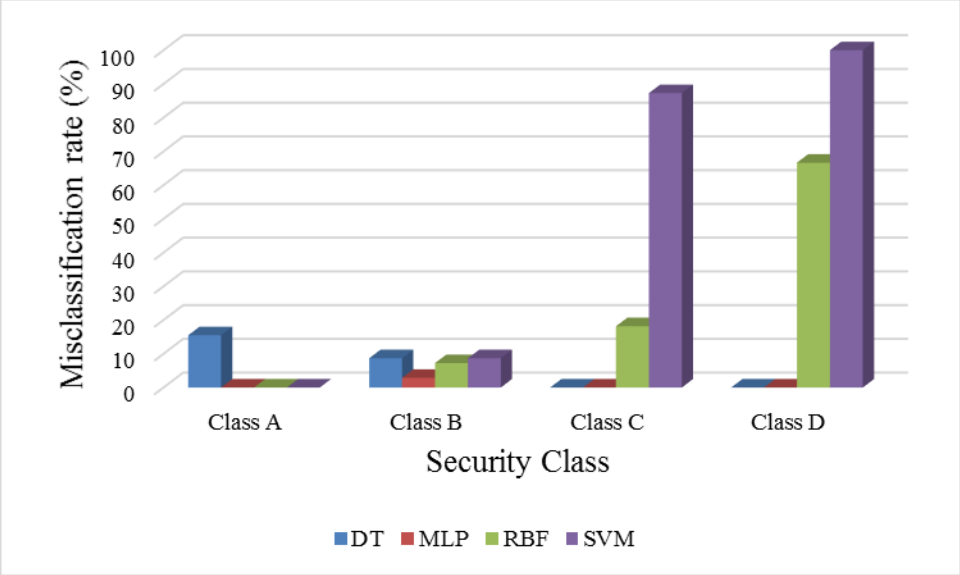

Figure 4.9: Misclassification rate comparison for each security class (IEEE-30 bus system)

The Table 4.4 shows the performance evaluation of various classifiers. From Table 4.4, it can be observed that, in the training phase, the classification accuracy for the DT, MLP, RBF and SVM are 100%, 98.26%, 97.56% and 100% respectively. However, in the testing phase

the classification accuracies are found to be DT (95.23%), MLP (94.44%), RBF (88.88%) and SVM (53.17%). It can be observed from the results that a single decision tree is performing better in classifying the security patterns.

Further, it can be observed that the DT classifier model took very less time of the order of milliseconds for evaluating a set of samples. But, in real time only one data sample needs to be accessed for security status at a particular instant. This further reduces the classification time for DT, which proves the adaptability and robustness of the DT classifier model in classifying the security patterns. The Figure 4.8 and Figure 4.9 shows the comparison of the classification accuracy and misclassification rate of the classifiers respectively.

4.8.2 Results for IEEE-57 bus system

Similar to the IEEE-30 bus system, the security patterns are obtained through offline simulations performed in MATLAB 2010a environment. The total number of operating scenarios considered are 631. Among the available data, 70% data is used for the training purpose and 30% data is used for testing the classifier model.

Table 4.5: Data generation for SSA (IEEE-57 bus system)

Operating scenarios	**Class**	**631(440+191)**
Static Secure	A	191(133+58)
Static critically secure	B	228(159+69)
Static Insecure	C	182(127+55)
Static Highly Insecure	D	30(21+9)

The Table 4.5 shows how the data is divided for the training and the testing phase of the classifier model. From Table 4.5, it can be observed that out of 631 data samples, 440 are selected for training and 191 are selected to test the trained classifier. Out of the selected data samples, 191 data samples (133 training +58 testing) belongs to class A, 228 data samples (159 training +69 testing) belongs to class B, 182 data samples (127 training +55 testing) belongs to class C, 30 data samples (21 training +9 testing) belongs to class D. In testing phase, all the data samples that corresponds to their classes stated above must be classified correctly. The Table 4.6 shows the confusion matrices for the DT, the MLP, the RBF and the SVM classifier models in the training and the testing phase.

Table 4.6: Confusion matrices for the classifier models (IEEE-57 bus system)

Classifier Type	Training	Testing
Decision Tree	Predicted Actual $\begin{pmatrix} 133 & 0 & 0 & 0 \\ 0 & 159 & 0 & 0 \\ 0 & 0 & 127 & 0 \\ 0 & 0 & 0 & 21 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 49 & 9 & 0 & 0 \\ 0 & 63 & 6 & 0 \\ 0 & 0 & 55 & 0 \\ 0 & 0 & 0 & 9 \end{pmatrix}$
Multilayer perceptron	Predicted Actual $\begin{pmatrix} 125 & 8 & 0 & 0 \\ 0 & 159 & 0 & 0 \\ 0 & 1 & 126 & 0 \\ 0 & 0 & 21 & 0 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 15 & 43 & 0 & 0 \\ 0 & 67 & 2 & 0 \\ 0 & 4 & 51 & 0 \\ 0 & 0 & 9 & 0 \end{pmatrix}$
Radial basis function	Predicted Actual $\begin{pmatrix} 130 & 3 & 0 & 0 \\ 22 & 132 & 5 & 0 \\ 0 & 1 & 123 & 3 \\ 0 & 0 & 2 & 19 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 51 & 7 & 0 & 0 \\ 0 & 64 & 5 & 0 \\ 0 & 10 & 45 & 0 \\ 0 & 0 & 6 & 3 \end{pmatrix}$
Support vector machine	Predicted Actual $\begin{pmatrix} 133 & 0 & 0 & 0 \\ 0 & 159 & 0 & 0 \\ 0 & 0 & 127 & 0 \\ 0 & 0 & 0 & 21 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 16 & 42 & 0 & 0 \\ 1 & 63 & 5 & 0 \\ 0 & 48 & 7 & 0 \\ 0 & 9 & 0 & 0 \end{pmatrix}$

Table 4.7: Performance Evaluation of the Classifiers (IEEE-57 bus system)

	Classifier Type	**CA (%)**	**Time (Sec)**	**Misclassification Rate (%)**			
				A	**B**	**C**	**D**
Training Phase	DT	100	0.03	0	0	0	0
	MLP	93.18	0.5	6.01	0	0.78	100
	RBF	91.81	0.11	2.25	16.98	3.14	9.52
	SVM	100	0.16	0	0	0	0
Testing Phase	DT	92.14	0.02	15.51	8.69	0	0
	MLP	69.63	0.5	74.13	2.89	0	0
	RBF	85.34	0.13	12.06	7.24	18.18	66.66
	SVM	45.02	0.12	72.41	8.69	87.27	100

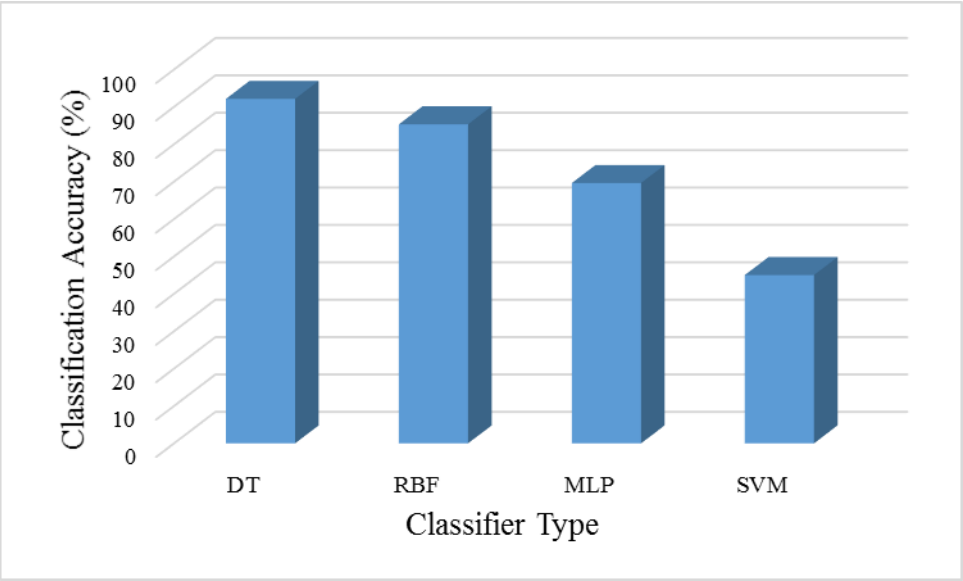

Figure 4.10: Performance comparison of the classifier models (IEEE-57 bus system)

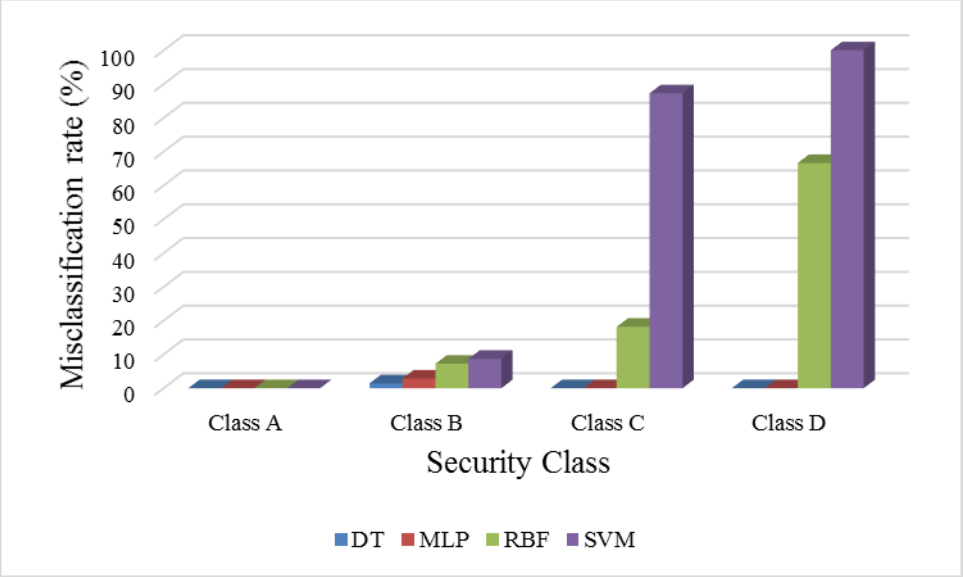

Figure 4.11: Misclassification rate comparison for each security class (IEEE-57 bus system)

The Table 4.7 shows the performance evaluation of various classifiers. From Table 4.7, it can be observed that, in the training phase, the classification accuracy for the DT, MLP, RBF

and SVM are 100%, 93.18%, 91.81% and 100% respectively. However, in the testing phase the performance of MLP (69.63%), RBF (85.34%) and SVM (45.02%) is dominated by DT classifier with 92.14% in 0.02 sec, which proves the adaptability and robustness of the DT classifier model in classifying the security patterns. The Figure 4.10 and Figure 4.11 shows the comparison of the classification accuracy and misclassification rate of the classifiers respectively.

Thus, the DT based security classifier model, capable of accessing the security level in less time with high accuracy, is found to be suitable for on-line implementation. This allows the operator to monitor the system security status from time to time, and take appropriate control actions, whenever needed.

4.9 Summary

In this chapter, a decision tree classifier model is implemented in order to classify the security status of the power system. The data is generated in an offline mode, which is used to train and test the classifier. The simulation results demonstrate that the decision tree classifier is efficient in classifying the security patterns in quick time, when compared to MLP, RBF and SVM classifier models. The adaptability and robustness of the decision tree classifier model makes it feasible for online implementation.

Chapter-5

Classification and Assessment of Power System Security using Random Forest Classifier

5.1 Introduction

In chapter 4, a decision tree classifier model is implemented for the classification and the assessment of the power system static security. It has been observed that the classification accuracy of the DT model is 95.23% (for IEEE-30 bus) and 92.14% (for IEEE-57 bus). However, the classification accuracy can be further improved using multiple decision trees or ensemble trees known as random forest, which is presented in this chapter.

In this chapter, a random forest model is implemented for the classification and the assessment of the power system security patterns. The RF model uses multiple decision trees, where each tree cast a vote to the specific class. The security patterns generated for the training and the testing purposes are same as used in chapter 4. The RF model is trained and tested with the data sets and finally, the classification accuracy is computed to study the efficiency and robustness of the classifier.

This chapter is organized as follows: Section 5.2 presents the design of the random forest based security classifier model, section 5.3 explains the random forest classifier model for security classification. The section 5.4 presents the simulation results and discussions. Finally

in section 5.5, the concluding remarks are provided.

5.2 Design of Random Forest Security Classifier Model

As discussed in previous chapter-4, the initial stage is to design overall architecture in order to implement the classification and the assessment of power system static security. The Figure 5.1 shows the block diagram model of the random forest based security classifier. This structure shows the entire procedure to implement the classifier.

1) Initially, the power system parameters, namely the load and the generator data are given as the inputs.

2) With the provided data, contingency analysis is carried out by creating N-1 line outage contingency under variable load and generator conditions using NRLF method in order to obtain the severity of the contingency.

3) The contingencies are created for the several load and the generating conditions in order to obtain the large range of security patterns covering the entire range of operating states.

4) Then, the important stage is designing the multi-class security problem, for which the generated security patterns needs to be classified. The design of the security problem depends on the requirements of the specific security condition. Once, the security problem is designed, some sample of the security patterns are given as inputs to train the random forest classifier model. After the classifier is trained, then the remaining set of patterns are given as inputs to test the classifier model for its accuracy in classifying the security status.

5) Finally, the classification accuracy is computed for the classifier model.

The formulation of the static security assessment has been discussed in section 4.4 and the design of the multiclass problem for security assessment has been discussed in section 4.5. These are used to implement the random forest classifier for the security assessment. Hence, the section 5.3, deals with the explanation of the random forest classifier model.

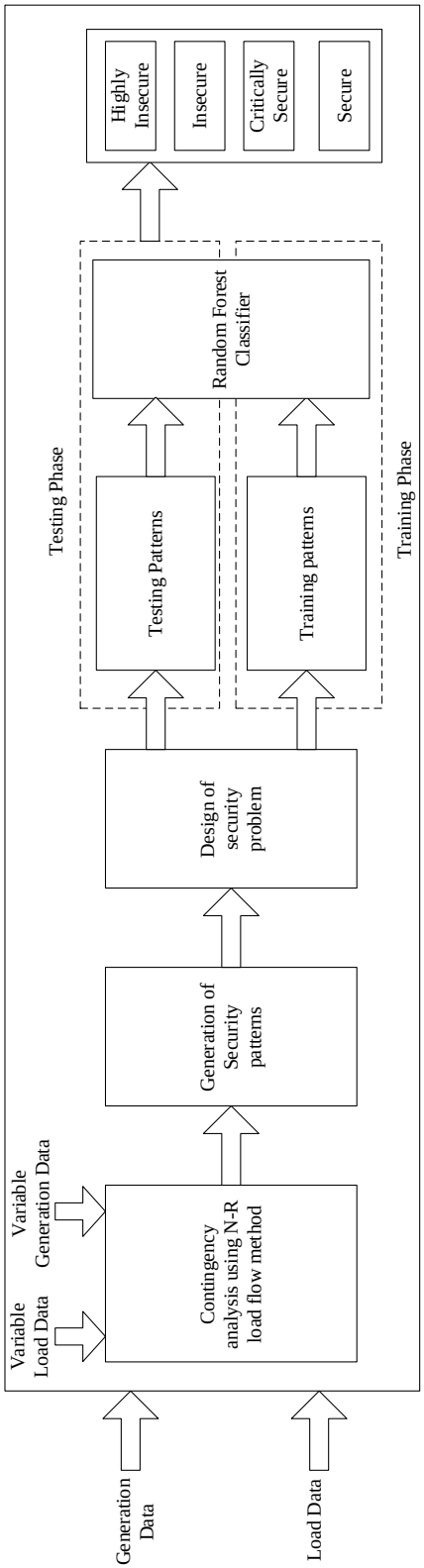

Figure 5.1: Block diagram of Random Forest based Security Classifier model

5.3 Random Forest Classifier Model

The decision tree models are used for the classification of the security patterns, however the performance of the classifier can be improved using ensemble of trees known as the random forest. The random forest is an ensemble model, which uses many decision tree models. This approach may be treated as the divide and conquer approach, where a group of weak individual learners forms as a strong learners. The results of many decision tree models are grouped in order to obtain the final output, which is known as the random forest. The Figure 5.2 shows the typical random forest classifier model, where the entire data set is divided into random subsets in order to form many decision trees. The combination of decision trees results in random forest in order to get the final output based on the individual results of each decision tree.

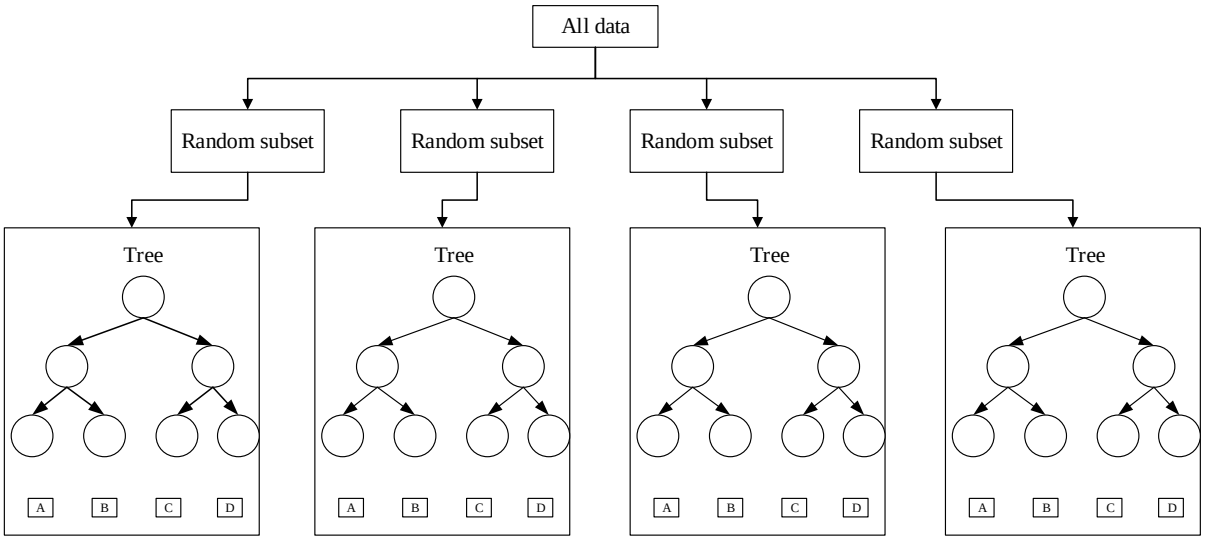

Figure 5.2: Random Forest classifier model

The random forests are a combination of tree predictors such that each tree depends on the values of a random vector sampled independently and with the same distribution for all the trees in the forest [91]. In comparison to the individual tree, there is an improvement of the accuracy of the RF model, where the generalization error converges to a limit as the tree grows deeply, making it ideal for many applications. The RF has got many advantages such as it's easy to use, high accuracy, no over fitting problem, robust with respect to noise, internal estimates monitor the error, strength, correlation and also used to measure variable

importance.

The definition of the RF by Leo Breiman [91] is stated as: A random forest is a classifier consisting of a collection of tree structured classifier, $R_k(y,\Phi_k), k=1,\ldots n_t$. where $\{\Phi_k\}$ is independent identically distributed random vectors are and each tree casts a unit vote for the most popular class at input y.

The fundamental procedure for growing of the ensemble tree is that, for the k^{th} tree ($k \le n_t$, the no.of trees in the ensemble), a random vector Φ_k is generated, which is independent of the previous random vectors $\Phi_1,\ldots,\Phi_{k-1}$, but with the identical distribution, and an individual tree is grown using the training set T_r with the attributes in Φ_k, resulting in a classifier $R_k(y,\Phi_k)$, where *y* is the input vector corresponding to equation (4.4). In random split selection, Φ consists of a number of independent random integers where $n_{try} \le n_a$, the number of attributes in *y*. When the trees are grown sufficiently in depth, they cast a vote for the best class. This approach is named as the random forest.

The algorithm for RF growing procedure for security classification is presented below:

1. For $k=1,\ldots,n_t$
    a) Select the data sample T_r^* of size N from the training set T_r (Which contains M > N samples)
    b) Start growing the RF tree $R_k(y,\Phi_k)$ using the data sample by repeating the procedure below, at each node of the generated tree, until an unpruned tree is encountered(i.e., no further splitting possible)
        i. Select the n_{try} variables from the n_a security features
        ii. Choose the best split point/variable among n_{try}
        iii. Split the chosen node into two daughter nodes
2. Obtain the random forest (ensemble of trees) $\{R_k(y,\Phi_k), k=1,\ldots n_t\}$.

5.3.1 Prediction from Ensemble Trees

The prediction by a random forest model is the consolidation of all the single tree predictions. For the security assessment multi class problem, the classification is made on the

class that majority trees vote for, is returned as the prediction of the ensemble.

$$C_{RF}^{n_t}(y) = majority\,vote\{C_k(y), k = 1,...,n_t\} \tag{5.1}$$

For predicting probabilities, i.e., relative class frequencies, the results obtained from the individual trees are aggregated.

$$P_{RF}^{n_t}(\mathrm{C}_{RF}^{n_t} \in \{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D} \mid \mathrm{y}\}) = \frac{1}{n_t}\sum_{1}^{n_t} P_{T_k(\Phi_k,\mathrm{S})}(\mathrm{C}_k \in \{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D} \mid \mathrm{y}\}) \tag{5.2}$$

Where, $P_{T_k(\Phi_k,\mathrm{S})}(\mathrm{C}_k \in \{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D} \mid \mathrm{y}\})$ is the probability of mapping the data *y* to class A, B, C or D by the RF R_k .

A conventional decision tree basically represents a specific decision boundary, and the data S is classified into class Q, if falls in the zone of decision area (basically a leaf of the DT) analogous to Q. The class probability p (Q|S) is usually predicted by the portion of data of class Q in the leaf into which S falls. This prediction is very important, when the DT is pruned. The reason is that the data falling in the same leaf has the same class probability. Thus, unpruned trees are required to obtain the efficient probability prediction, which are very crucial for the random forests.

The concept described above is the basic prediction, however, RF has out-of-bag (oob) prediction. Basically, the single tree is built from the sample data set T_r^*, which is used as the learning set for the specific tree. In fact, the sample data set T_r^* consists of only some portion of the entire data set. The remaining data set are used as the test sample to calculate the prediction accuracy of the specific tree. The benefit of oob error is that, a greater sensible prediction error rate can be obtained. If the random forest is provided with 70% (for training) of the entire data set and 30% for testing, it can be observed that out of the 70% of the data, each tree is trained with only $(2/3)^{rd}$ of the data. In the training stage, only 50% of the data will be observed by each tree in the RF model. If such a RF model, results in high prediction accuracy, it can be said that RF model is a robust and a general model.

The pseudo code for RF growing procedure is given below:

To create R classifiers:

(1) ***for*** *k = 1 to* n_t
do
(2) Randomly sample the training data T_r *with substitute to produce* T_{ri}
(3) Create a root or base node, Qi consisting T_{ri}
(4) Call Build Tree (C_i*)*
end for
(5) Build Tree (C):
(6) ***if*** *C consists cases of only single class then*
return
else
(7) Randomly select y% of the potential splitting features in C
(8) Select the feature F with the highest information gain to split on
(9) Create f child nodes of C , C_1 *,..,* C_f *, where F has f possible values (* F_1 *, … ,* F_f *)*
(10) ***for*** *k = 1 to f*
do
(11) Set the contents of C_i *to* T_{ri} *, where* T_{ri} *is all instances in C that match* F_i
(12) Call BuildTree (C_i*)*
end for
end if

5.4 Simulation Results and Discussion

The key objective of the RF classifier is to classify the large number of the security patterns to their respective security classes without false alarm. The experiments to test the RF classifier model for the security classification and assessment is employed on IEEE-30 bus and IEEE-57 bus test system on an Intel Core I7 3.40 GHz processor with Windows 7 professional operating system.

5.4.1 Results for IEEE-30 bus system

In order to implement the approach, the total number of operating scenarios considered are 414. Among the available data, 70% data is used for the training purpose and 30% data is used for testing the classifier model. The Table 4.2 shows how the data is divided for the training and the testing phase of the classifier model.

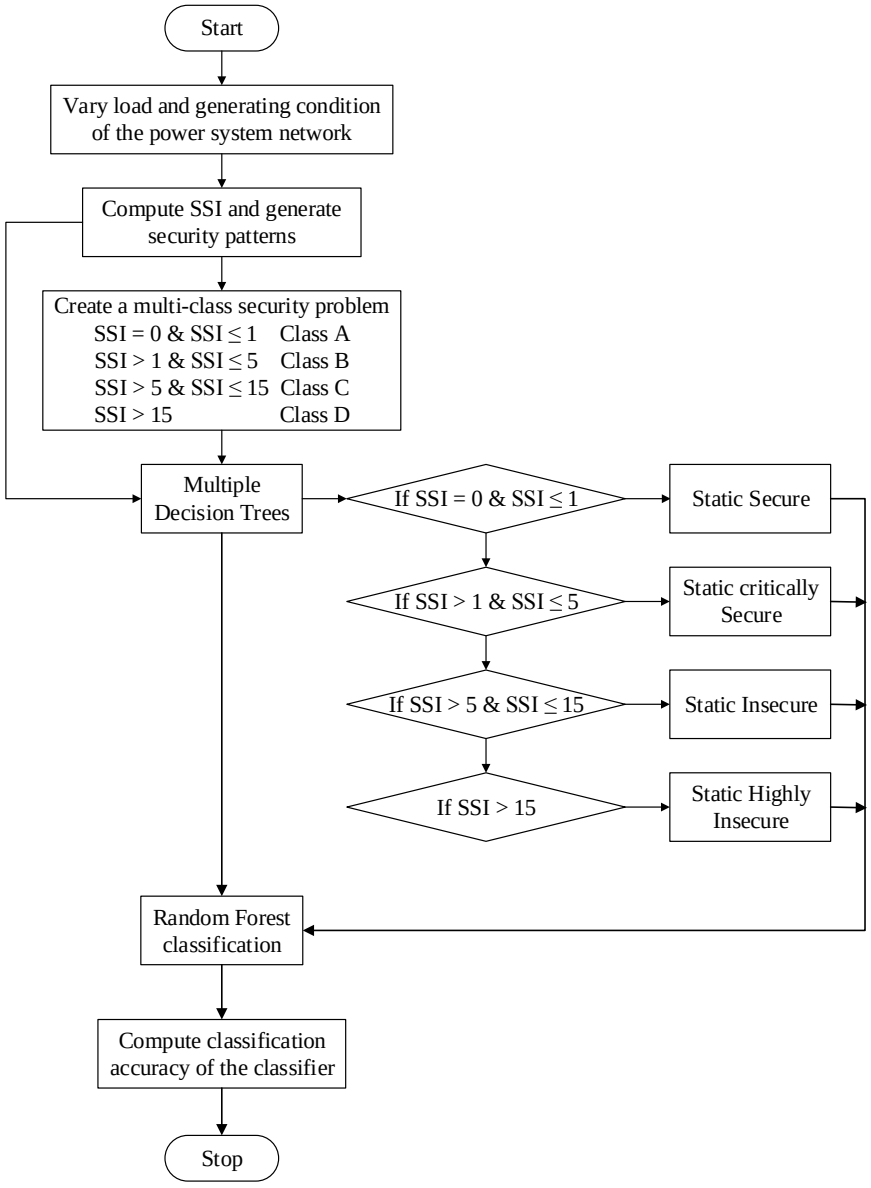

Figure 5.3: Flowchart showing the implementation of Random forest classifier

From Table 4.2, it can be observed that out of 414 data samples, 288 are selected for the training and 126 are selected to test the trained classifier. Out of the selected data samples, 33 data samples (23 training +10 testing) belongs to class A, 68 data samples (47 training +21 testing) belongs to class B, 104 data samples (72 training +32 testing) belongs to class C, 209 data samples (146 training +63 testing) belongs to class D. In the testing phase, all the data samples that corresponds to their classes stated above must be classified correctly. The overall concept of the RF approach for security classification is represented in the flow chart shown in Figure 5.3.

Initially, the RF classifier is provided with the training samples to build the RF security classifier model. Once it is trained, it will generate the confusion matrix for the security patterns. Once the model is designed, then it is tested with the test samples to classify the security patterns. This will result in confusion matrices showing the classification of the security patterns, which is used to compute the classification accuracy of the model. The Table 5.1 shows the confusion matrices in both the training and the testing phase, which are used to evaluate the performance of the classifier for the security classification.

Table 5.1: Confusion matrices for RF classifier model (IEEE-30 bus system)

Classifier Type	Training	Testing
Random Forest	Predicted Actual $\begin{pmatrix} 23 & 0 & 0 & 0 \\ 0 & 47 & 0 & 0 \\ 0 & 0 & 72 & 0 \\ 0 & 0 & 0 & 146 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 10 & 0 & 0 & 0 \\ 0 & 20 & 1 & 0 \\ 0 & 0 & 32 & 0 \\ 0 & 0 & 0 & 63 \end{pmatrix}$

The confusion matrix for the random forest is analyzed as follows: In the training phase, the total number of security patterns that belongs to class A, class B, class C and class D are 23, 47, 72 and 146 respectively. This means that all the security patterns corresponds to class A, class B, class C and class D, are classified correctly to their respective designed security states or classes. Whereas in the testing phase, the total number of security patterns that belongs to class A, class B, class C and class D are 10, 21, 32 and 63 respectively. The 10 security patterns that belongs to class A are classified correctly. Whereas, out of 21 patterns in class B, 20 security patterns are classified or predicted to class B correctly, but 1 pattern that belong to class B is predicted as class C. But 32 patterns in class C and 63 patterns in

class D are predicted or classified to their respective classes accurately.

Table 5.2: Performance Evaluation of the Classifiers (IEEE-30 bus system)

	Classifier Type	CA (%)	Time (Sec)	Misclassification Rate (%)			
				A	B	C	D
Training Phase	RF	100	0.02	0	0	0	0
	DT	100.00	0.03	0	0	0	0
	MLP	98.263	0.38	0	8.51	1.38	0
	RBF	97.569	0.22	0	4.25	4.16	0
	SVM	100.00	0.22	0	0	0	0
Testing Phase	RF	99.20	0.02	0	4.76	0	0
	DT	95.238	0.02	0	14.28	9.37	0
	MLP	94.444	0.33	0	9.52	15.62	0
	RBF	88.888	0.23	0	38.09	18.75	0
	SVM	53.174	0.09	80	90.47	100	0

In order to evaluate the performance of the classifier, the performance measures are computed based on equation (4.11) and equation (4.12). The Table 5.2 shows the classification accuracy and misclassification rate of the random forest classifier along with DT, MLP, RBF and SVM classifiers. The Figure 5.4 shows the comparison of the classification accuracy and the Figure 5.5 shows the comparison of misclassification rate of RF with DT, MLP, RBF and SVM classifier models respectively.

From Table 5.2, it can be observed that, in the training phase, the classification accuracy for RF, DT, MLP, RBF and SVM are 100%, 100%, 98.26%, 97.56 and 100% respectively. However, in the testing phase the classification accuracies are found to be of RF (99.20%), DT (95.23%), MLP (94.44%), RBF (88.88%) and SVM (53.17%). It can be observed from the results that the accuracy is improved (99.20%) by using ensemble of trees (random forest model) in classifying the security patterns.

Further, it can be observed that the RF classifier model took very less time of the order of milliseconds for evaluating a set of samples, which proves the capability and robustness of the RF classifier model in classifying the security level of the power system.

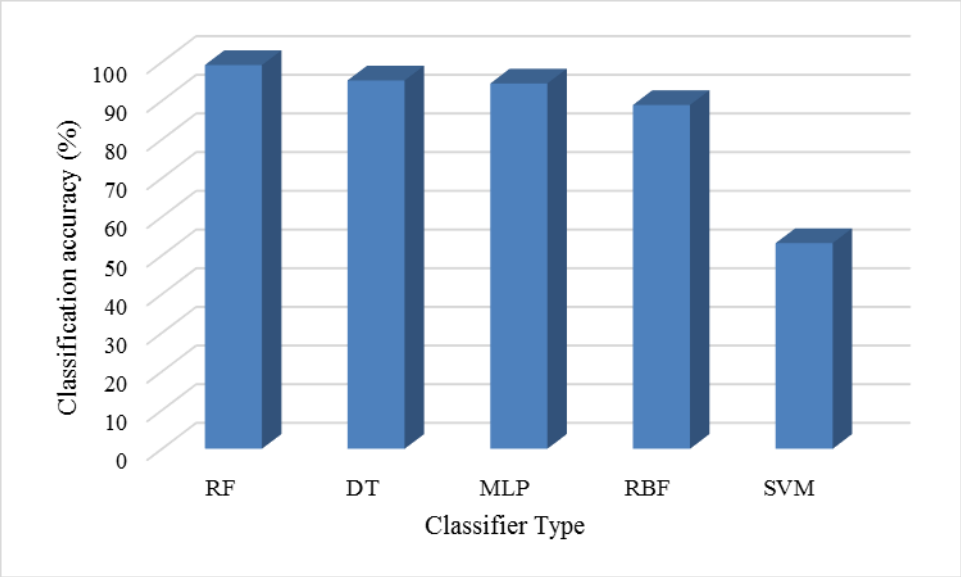

Figure 5.4: Performance comparison of the classifier models (IEEE-30 bus system)

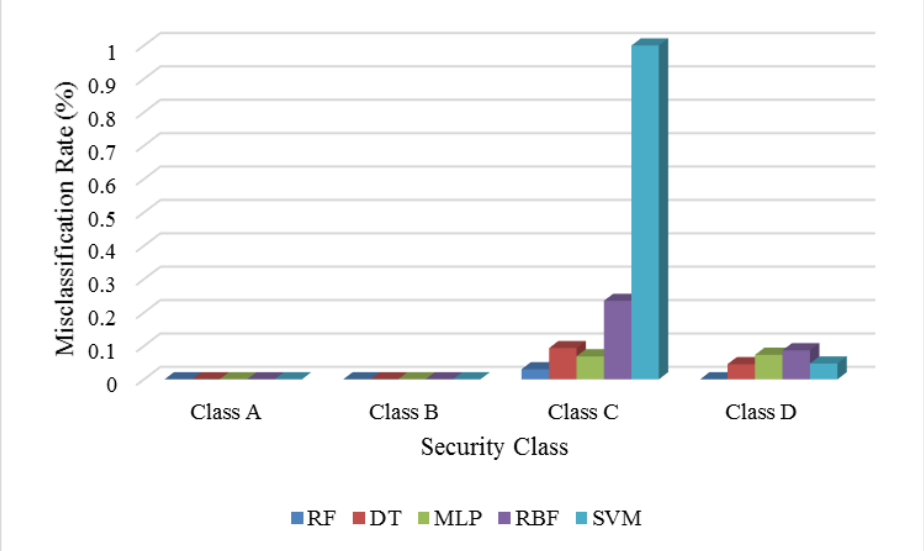

Figure 5.5: Misclassification rate comparison for each security class (IEEE-30 bus system)

5.4.2 Results for IEEE-57 bus system

Similar to the IEEE-30 bus system, the security patterns are obtained through offline simulations performed in MATLAB 2010a environment. The total number of operating scenarios considered are 631. Among the available data, 70% data is used for the training purpose and 30% data is used for testing the classifier model. The Table 4.5 shows how the data is divided for the training and the testing phase of the RF classifier model.

The Table 5.3 shows the confusion matrices in both the training and the testing phase, which are used to evaluate the performance of the classifier for the security classification. The Table 5.4 shows the classification accuracy and misclassification rate of the random forest classifier along with DT, MLP, RBF and SVM classifiers.

Table 5.3: Confusion matrices for RF classifier model (IEEE-57 bus system)

Classifier Type	Training	Testing
Random Forest	Predicted Actual $\begin{pmatrix} 133 & 0 & 0 & 0 \\ 0 & 159 & 0 & 0 \\ 0 & 0 & 127 & 0 \\ 0 & 0 & 0 & 21 \end{pmatrix}$	Predicted Actual $\begin{pmatrix} 48 & 10 & 0 & 0 \\ 4 & 68 & 1 & 0 \\ 0 & 0 & 55 & 0 \\ 0 & 0 & 0 & 9 \end{pmatrix}$

Table 5.4: Performance Evaluation of the Classifiers (IEEE-57 bus system)

	Classifier Type	**CA (%)**	**Time (Sec)**	**Misclassification Rate (%)**			
				A	**B**	**C**	**D**
Training Phase	RF	100	0.03	0	0	0	0
	DT	100	0.03	0	0	0	0
	MLP	93.18	0.5	6.01	0	0.78	100
	RBF	91.81	0.11	2.25	16.98	3.14	9.52
	SVM	100	0.16	0	0	0	0
Testing Phase	RF	94.24	0.02	17.24	1.44	0	0
	DT	92.14	0.02	15.51	8.69	0	0
	MLP	69.63	0.5	74.13	2.89	0	0
	RBF	85.34	0.13	12.06	7.24	18.18	66.66
	SVM	45.02	0.12	72.41	8.69	87.27	100

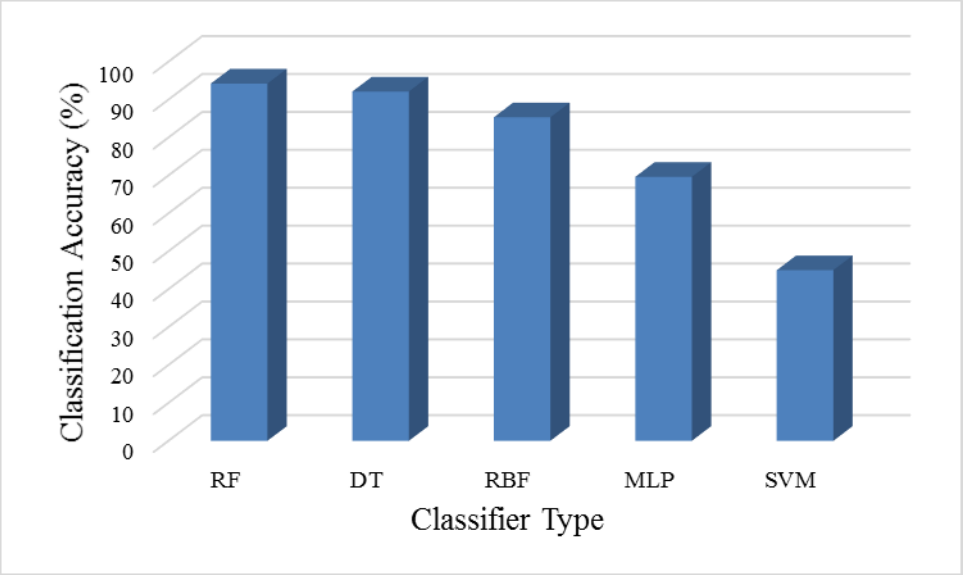

Figure 5.6: Performance comparison of the classifier models (IEEE-57 bus system)

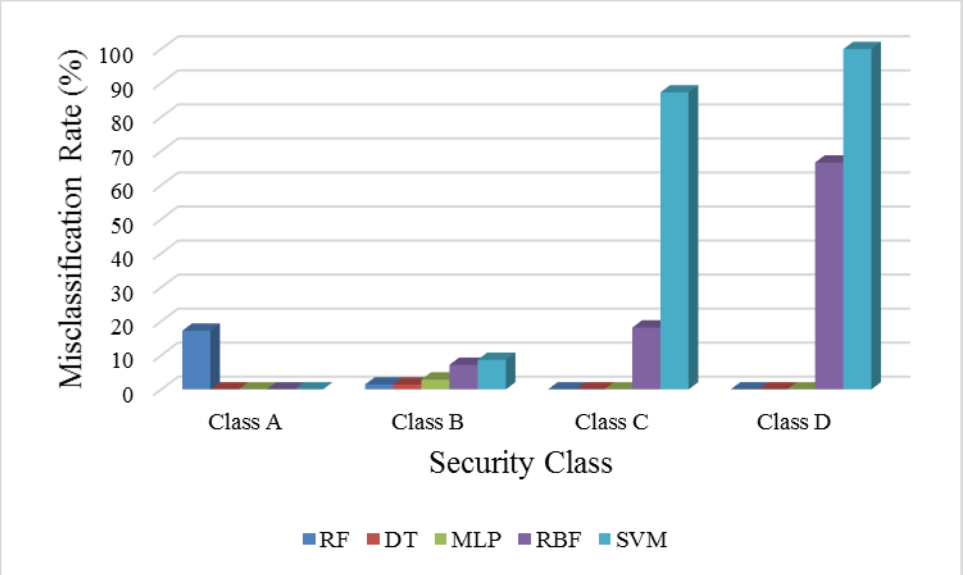

Figure 5.7: Misclassification rate comparison for each security class (IEEE-57 bus system)

From Table 5.4, it can be observed that, in the training phase, the classification accuracy for RF, DT, MLP, RBF and SVM are 100%, 100%, 93.18%, 91.81% and 100% respectively. However, in the testing phase the performance of DT (92.14%), MLP (69.63%), RBF

(85.34%) and SVM (45.02%) is dominated by RF classifier with 94.24%. From the results it can be observed that using ensemble of trees (random forest model) the classification accuracy is improved to 94.24% in 0.02 sec. The Figure 5.6 shows the comparison of the classification accuracy and the Figure 5.7 shows the comparison of misclassification rate of RF with DT, MLP, RBF and SVM classifier models respectively.

Thus, the RF based security classifier model, capable of accessing the security level in less time with high accuracy, is found to be suitable for on-line implementation. This allows the operator to monitor the system security status from time to time, and take appropriate control actions, whenever needed.

5.5 Summary

In this chapter, a random forest classifier model is presented to classify the security patterns of the power system. The data is generated in an offline mode, which is used to train and test the classifier. The classification accuracy is found to be higher for the random forest when compared to the single decision tree. Also, the RF classification accuracy is higher when compared to the MLP, the RBF and the SVM classifier models. The adaptability and robustness of the random forest classifier model makes it feasible for the online implementation.

Chapter 6

An Enhanced Cuckoo Search Algorithm for Contingency Constrained Economic Load Dispatch for Security Enhancement

6.1 Introduction

The chapter 2 to chapter 5 have discussed two important aspects of the security assessment namely the contingency ranking and the classification approach. These assessment process helps in giving the secure and insecure nature of the power system. As discussed in chapter 1, the security assessment is the initial stage in order to evaluate the system security. However, the security control is another important aspect of security under contingency scenario. Thus, in this chapter 6, the security enhancement under contingency case is presented.

During the N-1 line outage contingency scenario, the transmission lines are overloaded which effects the system security. One of the control aspects of security known as the security enhancement which is achieved by generator rescheduling with minimum fuel cost. The enhancement process relieves the overloaded lines from stress, which results in minimum severity index.

In order to achieve this objective, a meta-heuristic algorithm namely, an enhanced cuckoo search algorithm is designed to reschedule the generators with minimum fuel cost, such that

severity is minimized. In order to prove the accuracy of the ECS algorithm, the results obtained on an IEEE-30 bus test system, are compared with other state-of-the-art algorithms namely PSO, BA and CS.

This chapter is organized as follows: The Section 6.2 presents the design of CCELD approach, Section 6.3 presents the formulation of severity index, whereas Section 6.4 presents the problem formulation for CCELD approach. The Section 6.5 presents the over view of cuckoo search algorithm and Section 6.6 discuss the development of enhanced cuckoo search algorithm. The Section 6.7 discuss the simulation results. Finally, in Section 6.8 the concluding remarks are provided.

6.2 Design of CCELD Approach

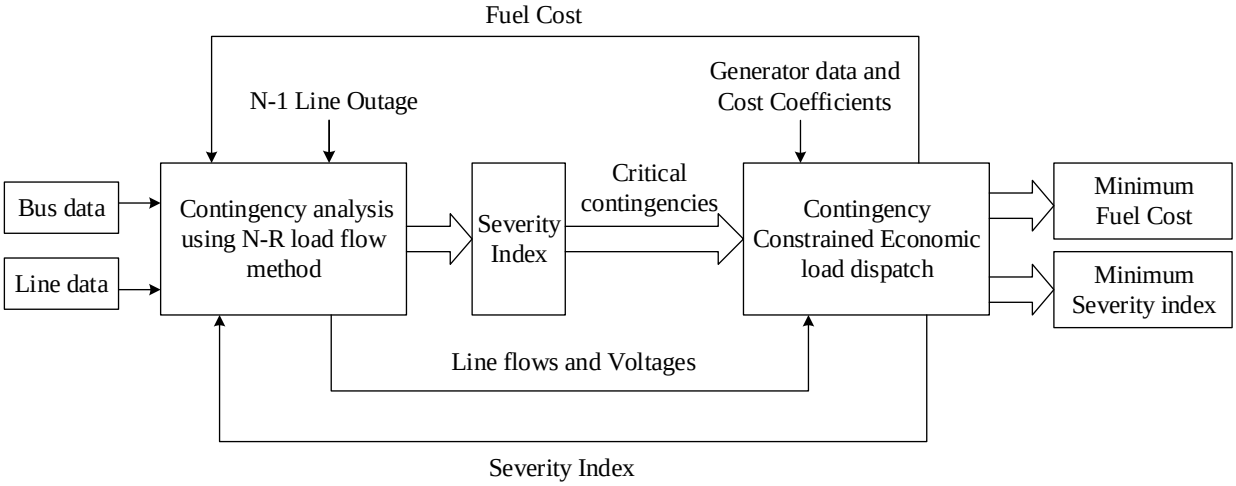

Figure 6.1: Block diagram of CCELD approach

In the area of power system security, the important aspect is the security assessment to avoid the system blackout. However in real time scenario, there is a need for necessary control action to enhance the security under critical contingencies. These N-1 line outage critical contingencies overload the transmission lines, threatening the system security. One of the control action can be achieved by generation rescheduling with minimum fuel cost, in such a way that the overload lines are relieved from stress under contingency scenario. The complete approach is explained based on Figure 6.1, which shows the design approach for

contingency constrained economic load dispatch.

To implement the approach, initially the power system bus data and the load data is used to run the contingency analysis by N-R load flow method under N-1 line outage contingency. From the contingency analysis, the severity index is computed and the critical contingencies are identified and forwarded to the CCELD phase. In this phase, the system reads the generator data and the fuel cost coefficients, along with the line flows and voltages from the contingency analysis phase. In the CCELD phase, the generators are rescheduled and computes the fuel cost and the severity index. The rescheduled generators active power are fed back (limited to number of iterations) to the contingency analysis phase in order to achieve minimum fuel cost and minimum severity index. The designed CCELD problem is implemented on a standard IEEE 30-bus test system with the application of enhanced cuckoo search algorithm.

6.3 Severity Index

As discussed in the previous section, from the contingency analysis it is necessary to compute the severity index in order to identify the critical contingencies. The contingencies in the power system over load the transmission lines. The severity of such overloaded lines is measured by an index called the severity index, which states the post-contingency condition of the power system, as given by equation (6.1)

$$\text{Severity Index } I_{sl} = \sum_{l=L_0}^{n} \left[\frac{S_l}{S_l^{\max}} \right]^{2m} \tag{6.1}$$

The equation (6.1), uses the line flows to compute the severity index which are obtained using Newton-Raphson load-flow analysis and *m* is an integer exponent, which is fixed as 1. Higher value of severity index, indicates more insecure nature of the contingency. In this study of security assessment using the severity index, over loaded lines alone are taken into consideration to prevent the masking effects.

6.4 Problem Formulation

In the CCELD phase it is necessary to design the problem formulation. The classical optimal power flow problem is to schedule the generators with minimum fuel cost, which is the objective function as given in equation (6.2)

$$Min \sum_{i \in N_g} F_T(P_{gi}) \tag{6.2}$$

$$F_T(P_{gi}) = a_i P_{gi}^2 + b_i P_{gi} + c_i \tag{6.3}$$

The minimization problem is subjected to the following constraints:

1) Power balance constraint:

$$\sum_{i=1}^{N_g} P_{gi} = P_D + P_L \tag{6.4}$$

2) Power flow equation of the power network:

$$g\left(|v|, \delta\right) = 0 \tag{6.5}$$

$$g\left(|v|, \delta\right) = \begin{vmatrix} P_i\left(|v|, \delta\right) - P_i^{net} \\ Q_i\left(|v|, \delta\right) - Q_i^{net} \end{vmatrix} \qquad i = 1, ...N_b \tag{6.6}$$

3) Inequality constraints on active power generation P_{gi} of each unit i:

$$P_{gi}^{\min} \le P_{gi} \le P_{gi}^{\max} \qquad i = 1, ..., N_g \tag{6.7}$$

4) Inequality voltage constraint on each bus:

$$V_i^{\min} \le V_i \le V_i^{\max} \qquad i = 1, ..., N_b \tag{6.8}$$

5) Power limit on transmission line:

$$S_l \le S_l^{\max} \tag{6.9}$$

6.5 History and Overview of Cuckoo Search Algorithm

The concept of meta-heuristic algorithm known as the cuckoo search algorithm [94] was developed by Yang and Deb. In recent years, the cuckoo search (CS) algorithm gained great importance and applicability [95] in many fields like engineering [96-103], Object oriented software (software testing), pattern recognition, networking, data fusion in wireless sensor networks and job scheduling. It was inspired by the obligate brood parasitism, where the algorithm is based on the unique behavior of some cuckoo species laying their eggs in the communal nests or the nests of the other species birds. In order to simplify the concept of CS, three simple rules are framed.

1) Each cuckoo lays a single egg at a time, and a random nest is selected to dump the egg.

2) The best nests with good quality of eggs will persist to the next generations.

3) In the entire search process, the quantity of available nests is fixed, and the host bird goes in search of discovering an alien egg with a probability $p_a \in [0, 1]$. If the host bird discovers an alien egg, it may either throw the egg or abandon the nest or it may build a new nest.

These rules are transformed to optimization technique. Each egg in a nest resembles a solution and a cuckoo egg resembles the best solution. The key objective is to obtain the best solution. Based on the above rules, the standard cuckoo search algorithm is developed as follows:

In the cuckoo search method, each egg in a nest can be treated as a solution. The algorithm starts with the randomly generated solution and population. The population uses D-dimension parameter vector restricted by the maximum and minimum limits as given by equation (6.10) and equation (6.11).

1) $$\vec{X}_{\min} = \left\{ x_{1\min}, x_{2\min}, ..., x_{D\min} \right\} \tag{6.10}$$

$$\vec{X}_{\max} = \left\{ x_{1\max}, x_{2\max}, ..., x_{D\max} \right\} \tag{6.11}$$

Thus, j_{th} component is generated from the i_{th} vector, is given by (6.12).

2) $x_{j,i}^{t} = x_{j\min} + rand_{i,j}[0,1] \cdot (x_{j\max} - x_{j\min})$ (6.12)

Where $i = 1, \ldots, NP$, $j = 1, \ldots, D$ and $rand_{i,j}[0,1]$ function generate uniformly distributed random elements in range of 0 to 1.

During the generation of the new solution, a Lêvy flight is performed as given by (6.13).

4) $x_i^{t+1} = x_i^t + \alpha \oplus L\hat{e}vy(\lambda)$ (6.13)

The term x_i^{t+1} represents a new solution, x_i^t represents the current location and $L\hat{e}vy(\lambda)$ is the transition probability. The notation $\oplus$ represents entry-wise multiplications. Where $\alpha > 0$ is the step size, related to the scales of problem of interest. In most cases the value of α is taken as 1.

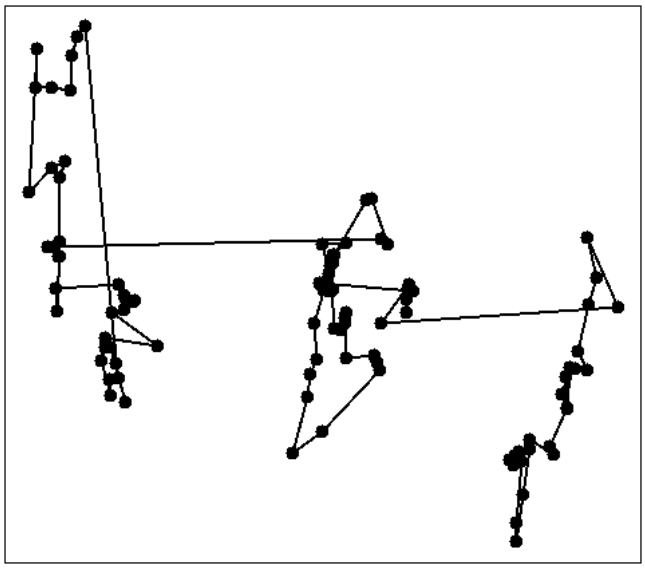

Figure 6.2: A typical Lêvy flight

A Lêvy flight is a random walk where the step lengths are distributed according to a heavy-tailed probability distribution as given by (6.14).

5) $L\hat{e}vy \sim u = t^{-\lambda}$ $(1 < \lambda < 3)$ (6.14)

This is a stochastic equation for the random walk in the course of obtaining new solutions, which has an infinite variance with an infinite mean. The next location of the Markov chain

random walk depends on the parameters given by equation (6.13). The successive jumps of a cuckoo essentially form a random walk process which obeys a power-law step-length distribution with a heavy tail.

In the growth stage, x_i^t starts with the donor vector $\upsilon = x_i^t$. The next step is to obtain the step size, which is given by (6.15).

6) $$stepsize = 0.01\left(\frac{u_j}{v_j}\right)^{1/\lambda}.\left(\upsilon - X_{best}\right) \quad (6.15)$$

Where, $u = t^{-\lambda} \times randn[\mathrm{D}]$ and $v = randn[\mathrm{D}]$. The function *randn [D]* generates normally the distributed random numbers in range of 0 to 1.

Now, a new solution vector is computed by using (6.16).

7) $$\upsilon_i = \upsilon_i + stepsize_j \times randn[\mathrm{D}] \quad (6.16)$$

The new solution vector υ_i is computed and compared with x_i. If $\upsilon_i < x_i$, then υ_i is treated as a new primary solution, else x_i is obtained.

The next task in the CS is to establish some nests by building a new solution, which is given as in (6.17)

8) $$\upsilon = \begin{cases} X_i + rand \cdot (X_{r1} - X_{r2}) & rand < p_a \\ X_i & otherwise \end{cases} \quad (6.17)$$

The final step is a greedy algorithm. Again, the new solution vector v_i is computed and compared with x_i. If $v_i < x_i$, then v_i is treated as a new primary solution, else x_i is obtained.

To understand the concept of CS algorithm, the pseudo code is given below:

Start
(1) Objective function *f (x)*
(2) Generation initialization *t* =1
(3) Initialize population (*n*), parameters and random values
(4) While (generation < max generation)

(5) Randomly select a cuckoo by Lêvy flights
(6) Compute the fitness of the selected cuckoo F_i
(7) Randomly select a nest (nest j, among n)
(8) If $F_i > F_j$, then
(9) Replace j by the new solution
(10) End
(11) A fraction of worse nests (p_a) are abandoned
(12) Build new nests
(13) Retain the best solution
(14) Obtain the current best solution among the ranked solutions
(15) Update Generation $t = t+1$
(16) End while
Stop

6.6 Development of the Enhanced Cuckoo Search Algorithm

The standard CS algorithm uses the parameters like p_a, α and λ in order to obtain the local and global enhanced solutions. The tuning of the solution vectors are dependent on the important key parameters p_a (probability ∈ [0, 1]) and α (step size), which are used to adjust the convergence rate of the algorithm. The standard CS algorithm uses a constant value of p_a and α, which are initially set in the beginning of the algorithm and do not change during further executions. The performance of the CS, degrades with a small value of p_a and a large value of α, which requires large number of iterations. On the other hand, higher speed of convergence can be achieved with large value of p_a and smaller value of α, but lacks in finding the best solution.

The major distinction between the ECS and the standard CS lies in the approach of tuning the parameters p_a and α. In order to eliminate the drawback of the fixed values of the parameters p_a and α, the ECS algorithm utilizes variable p_a and α, for enhancing the performance of the algorithm. In the initial generations, the values of p_a and α should be large in order to push the CS algorithm for enhancing the diversity of the solution vectors. The parameter values are decreased in the final generations in order to improve the fine tuning of

the solution vectors.

The parameters p_a and α are dynamically varied with the generation number, as given in equation (6.18) and equation (6.19).

$$p_a(gn) = p_{a\max} - \left(\frac{gn}{NI}\right)\left(p_{a\max} - p_{a\min}\right) \tag{6.18}$$

$$\alpha(gn) = \alpha_{\max} \exp(c.gn) \tag{6.19}$$

$$c = \frac{1}{NI} Ln\left(\frac{\alpha_{\min}}{\alpha_{\max}}\right) \tag{6.20}$$

These parameters are incorporated in the cuckoo search algorithm in order to enhance its performance.

The ECS algorithm is applied to CCELD problem. The objective function is to reschedule the generators with the minimum fuel cost, such that the severity index is minimized under critical contingencies, subjected to power units and system constraints.

6.6.1 Procedure of ECS Algorithm for CCELD Problem

1) Initialize the population, maximum number of iterations and dimensions of the problem.

2) Create N-1 transmission line outage and calculate the line flows, losses and slack bus power.

3) Under N-1 line outage contingency, the limit violations of transmission line power flow, voltage magnitude at the load bus bars and slack bus unit need to be considered. To include these violations, a penalty-function approach is used. Thus, the new objective function with the addition of penalty terms is given by equation (6.20).

$$F_T^*(P_{gi}) = F_T(\mathrm{P}) + K_a \times \sum_{i=1}^{N_b} (\mathrm{V}_i - \mathrm{V}_i^{\max})^2 + K_b \times \sum_{i=1}^{N_l} (S_{li} - S_{li}^{\max})^2 + K_c \times (\mathrm{P}_s - P_s^{\max})^2 \tag{6.21}$$

Where, K_a, K_b and K_c are the positive penalty coefficients.

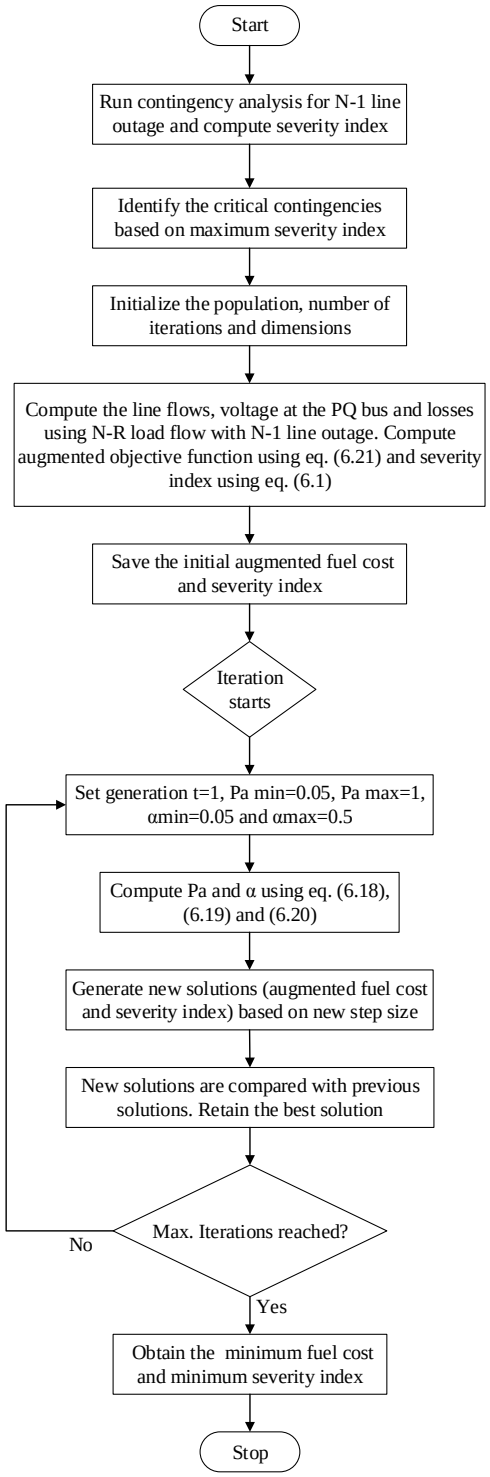

Figure 6.3: Flow chart of the ECS based CCELD approach

4) Compute the augmented objective function and obtain the fuel cost and active powers of the generators and compute the severity index using the N-R load flow method. These are taken as the initial solutions.

5) Set generation t=1; set the parameters $P_{a\,min}$=0.05, $P_{a\,max}$=1, α_{min}=0.05 and α_{max}=0.5.

6) Compute P_a and α for this generation by using equations (6.18), (6.19) and (6.20).

7) Compute $v_i = v_i + \alpha_j \times randn$[D]

8) Compute the augmented fuel cost. Compute voltage on the load bus, transmission line flows and slack bus power using N-R load flow method under the N-1 line outage contingency and obtain the severity index.

9) The new solution is compared with the previous solution.

10) If *NP*<=*max NP*, terminate and generate the augmented fuel cost and severity index in the population, else, set generation t=t+1 and go to step 4.

11) If t= t_{max}, go to step 12, else, go to step 4

12) Obtain the optimum generation with the minimum fuel cost and the minimum severity index. The entire approach is explained in a flow chart as shown in Figure 6.3.

6.7 Simulation Results and Discussion

This Section presents the details of the study carried out on an IEEE 30-bus test system for the security enhancement. Two distinctive cases are considered in this study. In the first case, contingency analysis is carried out for the base case load condition in order to recognize the critical contingencies. At each critical contingencies, the economic load dispatch is carried out. In the second case, the proposed enhanced cuckoo search algorithm is implemented in order to alleviate the overloaded transmission lines by generator rescheduling. Once the critical overloaded lines are relieved by the algorithm, simultaneously the algorithm relieves the less critical contingencies.

The ECS algorithm along with the other state-of-the-art algorithms namely the CS, BA

and PSO are applied in order to obtain optimal control parameters under contingency scenario. The proposed ECS algorithm code was written in Matlab 2010a environment and executed on a PC with Windows 7 professional operating system with Intel core I7 processor and 2GB of RAM.

The IEEE 30-bus system consists of 6 generators and 41 transmission lines. The generator data required for the study are taken from [16]. The upper voltage limit is 1.05 p.u. and lower voltage limit is 0.95 p.u. at all the busbars, whereas the slack busbar voltage is taken as 1.06 p.u.

Step-1 : contingency analysis and economic load dispatch:

As explained in the design of CCELD architecture, the first step is to obtain the critical contingencies.

Table 6.1: Contingency analysis for the IEEE 30-bus system

Outage Line	Overloaded line	Line flow (MVA)	Line flow limit (MVA)	Severity Index
L1 - L2	L1 - L3 L3 - L4 L4 - L6	192.1120 180.1815 110.8805	130 130 90	5.6227
L1 - L3	L1 - L2	181.6383	130	1.9522
L3 - L4	L1 - L2 L2 - L6	178.8614 65.5192	130 65	2.9090
L2 - L5	L2 - L6 L5 - L7	76.8053 83.3212	65 70	2.8130

The contingency analysis is carried out in order to figure out the critical contingencies. From the contingency analysis, it is identified that the line outages L1-L2, L1-L3, L3-L4 and L2-L5 are the critical contingencies, which causes the other lines to be over loaded. For these critical contingencies, the power flow of the overloaded lines along with the severity index is given in Table 6.1.

From Table 6.1, it can be observed that the outage L1-L2, causing the lines L1 - L3, L3 - L4 and L4 - L6 to overload. The MVA line flow limit for L1 - L3, L3 - L4 and L4 - L6 are 130, 130 and 90 respectively. However, the corresponding MVA lines flows during contingency is observed to be 192.1120, 180.1815 and 110.8805, which violated the line flow limit. Thus the severity index computed using equation (6.1) obtained for this case is 5.6227. Thus, these overloaded lines needs to be relieved in order to minimize the severity index.

Similarly, the line overloading can be observed for the other line outage cases giving severity index of 1.9522, 2.9090 and 2.8130 for L1 - L3, L3 - L4 and L2 - L5 respectively.

Under the critical contingencies given in Table 6.1, the economic load dispatch is carried out using the ECS algorithm as shown in Table 6.2. The load demand on the system is 283.4 MW and the losses under each contingency case are 24.84 MW (L1-L2), 13.79 MW (L1-L3), 13.453 MW (L3-L4) and 17.78 MW (L2-L5).

Table 6.2: Generator scheduling using ECS algorithm under the critical contingencies (without rescheduling)

	L1 - L2	**L1 - L3**	**L3 - L4**	**L2 - L5**
P1 (MW)	199.9997	194.3146	194.1211	196.6336
P2 (MW)	50.2824	48.7837	48.7401	49.2777
P3 (MW)	20.0707	19.6597	19.6473	19.7975
P4 (MW)	15.6369	12.4370	12.3445	13.4742
P5 (MW)	10.2503	10.0000	10.0000	10.0000
P6 (MW)	12.0000	12.0000	12.0000	12.0000

The Table 6.2, shows the generator scheduling under contingency. These generators need to reschedule, such that the overloaded lines are relieved from the stress.

Step- 2: Overload alleviation by generation rescheduling:

The ECS algorithm is applied to alleviate the overloaded transmission lines for all the four critical contingencies through generation rescheduling. To test the ability of the ECS algorithm, state-of-the-art algorithms namely the CS, BA and PSO have been applied to alleviate the overloaded lines. The Table 6.3 shows the optimal control parameters for all the critical contingencies along with the minimum fuel cost and the minimum severity index obtained after generator rescheduling. Also, Table 6.4 shows the line flows before and after rescheduling.

From Table 6.4, it can be observed under outage L1-L2, the new line flows obtained after generator rescheduling for the lines L1 - L3, L3 - L4 and L4 - L6 are 87.1691, 81.9316 and 55.5156 respectively, which are below the line flow limit, relieving the overloaded lines and thus the severity index obtained is zero. Similarly, for the other line outage cases, the line flows after rescheduling are below the line flow limits, proving that the over loaded lines are relieved and thus the severity index is zero. From Table 6.3, it can be observed that the generators are rescheduled with minimum fuel cost of 1359.5538 ($/h), 3553.8043 ($/h)

885.1073 ($/h) and 1089.2472 ($/h) under L1 - L2, L1 - L3, L3 - L4 and L2 - L5 outage contingency case respectively.

Table 6.3: Optimal power flow using ECS algorithm under critical contingencies (With rescheduling)

	L1 - L2	**L1 - L3**	**L3 - L4**	**L2 - L5**
P1 (MW)	104.9357	78.9527	86.2853	88.2479
P2 (MW)	69.5336	77.1004	80.0000	69.8681
P3 (MW)	44.7906	46.3480	49.7750	48.1451
P4 (MW)	32.6457	28.5060	10.7925	25.4422
P5 (MW)	21.7012	30.0000	30.0000	29.7924
P6 (MW)	34.6329	36.3146	40.0000	39.6871
Minimum fuel cost ($/h)	1359.5538	3553.8043	885.1073	1089.2472
Severity Index	0	0	0	0

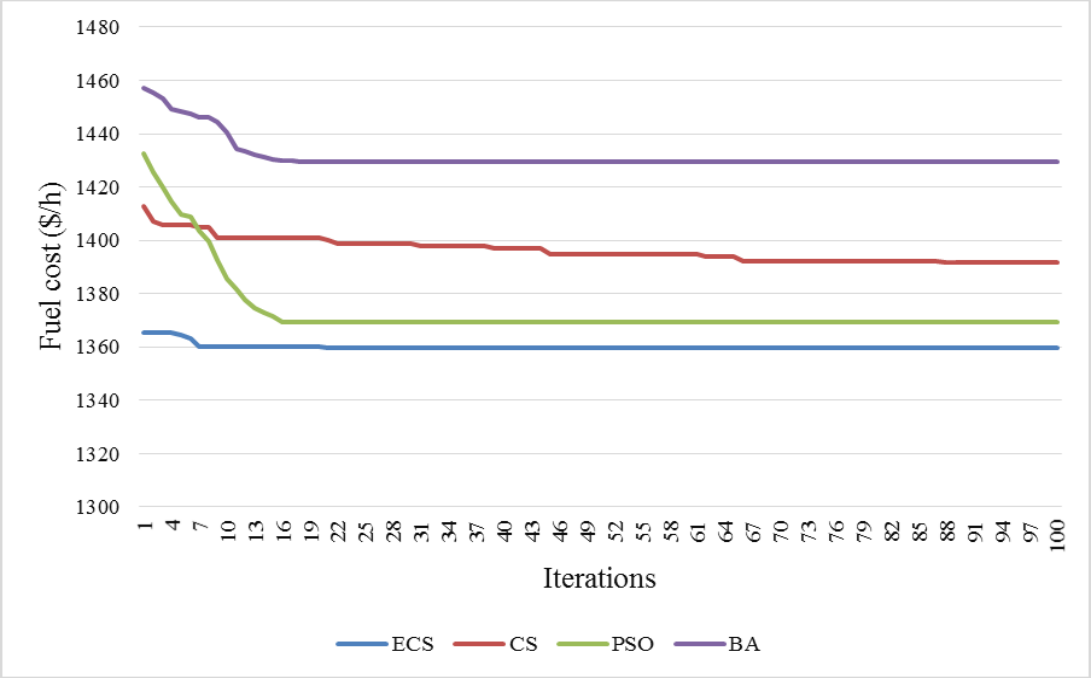

Figure 6.4: Convergence nature of ECS compared with CS, PSO and BA (With rescheduling for L1-L2 outage)

Table 6.4: Line flows after rescheduling (ECS) for IEEE 30-bus system

Outage Line	Overloaded line	Line flow (MVA) (Before)	Line flow (MVA) (After)	Line flow limit (MVA)	Severity Index
L1 - L2	-	192.1120 180.1815 110.8805	87.1691 81.9316 55.5156	130 130 90	0
L1 - L3	-	181.6383	44.2131	130	0
L3 - L4	-	178.8614 65.5192	47.9684 34.3323	130 65	0
L2 - L5	-	76.8053 83.3212	48.9601 51.7433	65 70	0

Table 6.5: Results of the algorithms in 100 Iterations

Methods	Line Outage	Minimum fuel cost ($/h)	Severity Index	Time (sec)
PSO	L1 - L2	1369.4021	0	0.55
BA		1429.7031	0	0.61
CS		1391.5791	0	0.58
ECS		1359.5538	0	0.52
PSO	L1 - L3	3577.6113	0	0.44
BA		3604.4297	0	0.57
CS		3601.5444	0	0.45
ECS		3553.8043	0	0.35
PSO	L3 - L4	932.4986	0	0.51
BA		989.8570	0	0.65
CS		946.5402	0	0.53
ECS		885.1073	0	0.40
PSO	L2 - L5	1113.0803	0	0.42
BA		1142.3212	0	0.56
CS		1134.1637	0	0.50
ECS		1089.2472	0	0.38

The Table 6.5, shows the minimum fuel cost and minimum severity index for 100 iterations. The Figure 6.4 shows the convergence nature of ECS, compared with CS, PSO and BA algorithms. It can be observed that the ECS algorithm has better convergence characteristics to achieve the minimum fuel cost in 100 iterations. From Table 6.5 and Figures 6.5, 6.6, 6.7 and 6.8 , it can be observed that the ECS algorithm gives minimum fuel cost with rescheduled generators with least execution time (for 100 iterations) to obtain minimum severity index when compared to CS, BA and PSO algorithms. From the simulation results, it is observed that the ECS algorithm is efficient in providing a solution to the contingency constrained economic load dispatch for security enhancement.

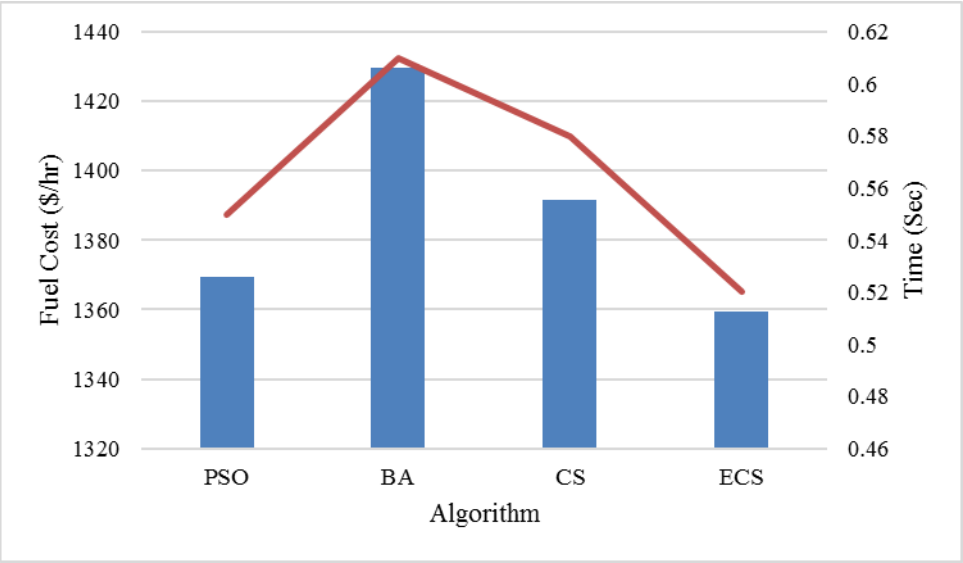

Figure 6.5: Comparison of fuel cost and time taken by each algorithm for outage L1 - L2 (100 iterations

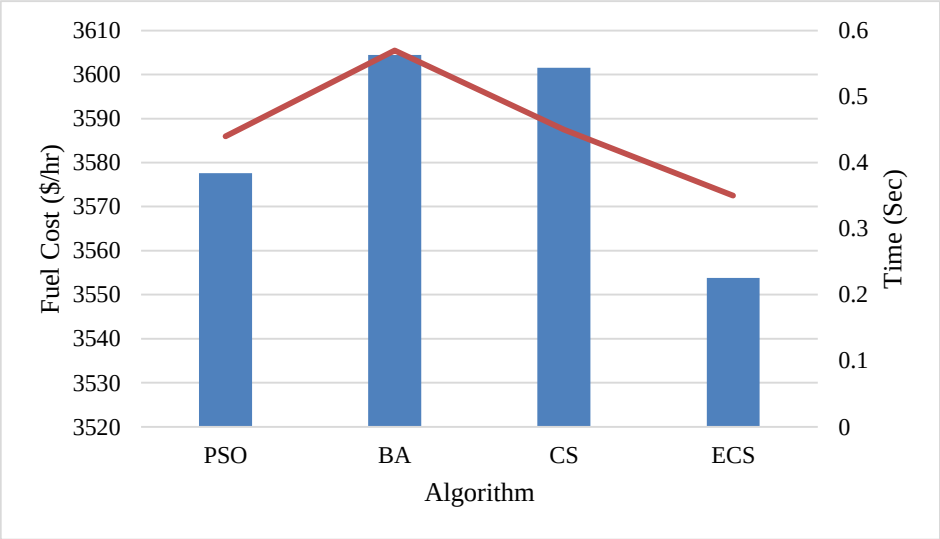

Figure 6.6: Comparison of fuel cost and time taken by each algorithm for outage L1 – L3 (100 iterations)

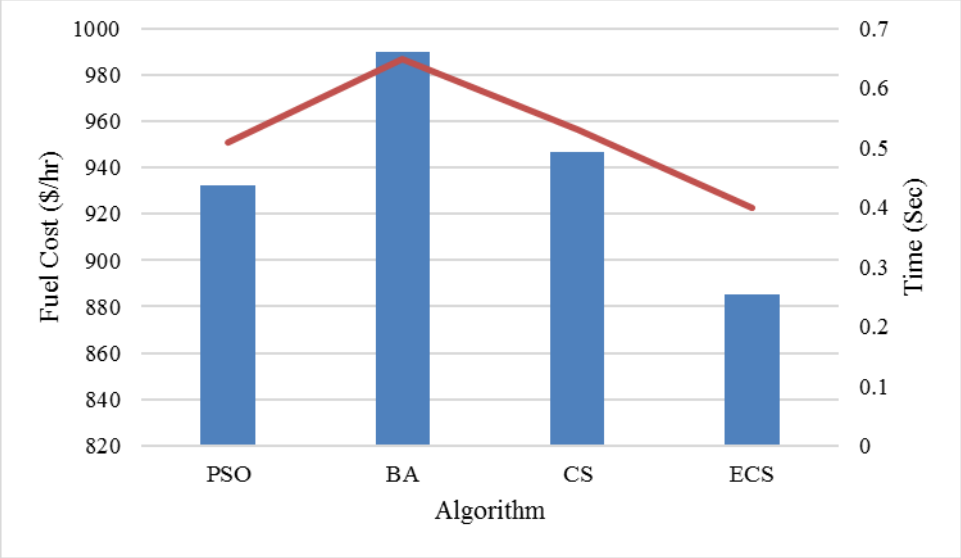

Figure 6.7: Comparison of fuel cost and time taken by each algorithm for outage L3 – L4 (100 iterations)

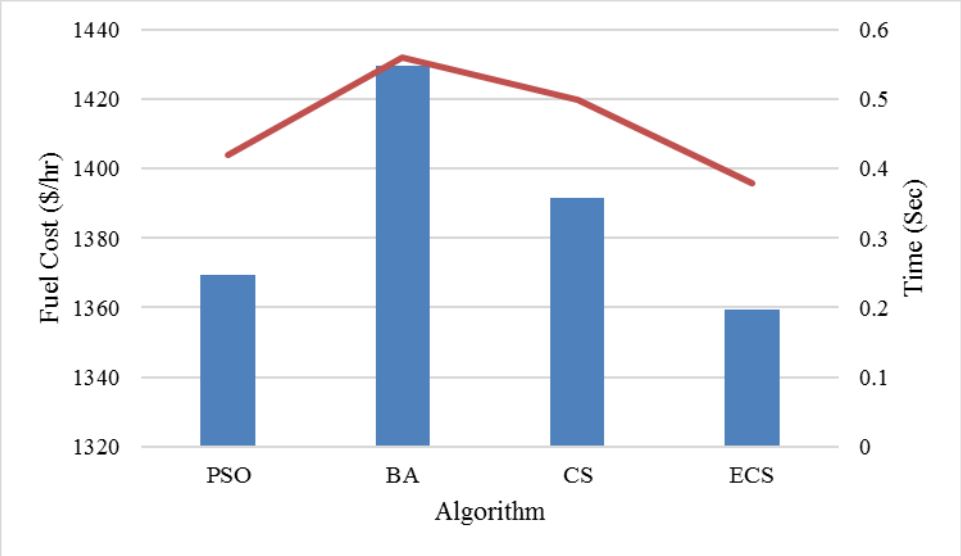

Figure 6.8: Comparison of fuel cost and time taken by each algorithm for outage L2 – L5 (100 iterations)

6.8 Summary

In this chapter, an enhanced cuckoo search algorithm (ECS) is presented for the contingency constrained economic load dispatch. The contingency analysis is performed in order to obtain the severity index and the critical contingencies are identified. Then the generators are rescheduled in such a way that the severity index is minimized with minimum fuel cost. The simulations are conducted on standard IEEE-30 bus test system, where the ECS algorithm is found to be efficient and quick (in 100 iterations) when compared to PSO, BA and CS algorithms.

Chapter 7

Conclusions and Future Scope

7.1 Conclusions

In this research work the main objective is, the assessment and the enhancement of the power system security under contingency scenario. The thesis work started with the introduction to power system security, operating states and control mechanism. Initially, security assessment is performed by contingency ranking approach using conventional NRLF analysis on IEEE-30 bus (base load case) and IEEE-57 bus (60% load variation) system. However, the conventional approach is not feasible for the real time implementation because of the complexity involved in solving the load flow problem for each contingency case. Also, the system parameters changes from time to time, which needs accurate monitoring approach, which can predict the system severity under N-1 contingency scenario for security assessment. In order to achieve this objective, a ranking module is designed with two neural network models namely, the MFNN and the RBFN. These neural network models are trained with variable load conditions under contingency scenario to predict the performance indices for unseen network conditions. The trained ANN models are tested with base case load condition and 60% load variation condition, which is not used in training phase. The obtained simulation results are compared with the conventional NRLF method. It is observed that the ranking module with MFNN and RBFN models are quite efficient in predicting the performance indices for unknown network conditions in less time, making it feasible for real time implementation.

Based on the requirement of the security monitoring process, the security assessment include classification of the security states in secure, critically secure, insecure and highly

insecure. As discussed previously, there exists several approaches in order to achieve this objective. But in security assessment, the accuracy of the approach is key for proper evaluation. Thus, research is focused on designing an efficient pattern classifier model to classify the security status. A DT classifier model is developed and implemented to classify the security status. In order to achieve this task, the simulations are carried on IEEE-30 bus and IEEE-57 bus systems. A large number of security patterns are generated at variable load and generating conditions under contingency scenario. Each security pattern is assigned to one of the security class. Out of the total security patterns, 70% security patterns are used to train and design the classifier and the remaining 30% patterns are used for testing the classifier. The simulation results prove that the DT classifier fast and efficient in classifying the unseen security patterns when compared to MLP, RBFN and SVM classifier. However, to improve the classification accuracy, a RF classifier model is developed, which uses multiple decision trees. From the simulation results, it is observed that the classification accuracy is improved when compared to single DT, MLP, RBF and SVM classifier models. Thus, the DT and the RF classifiers are found efficient in classifying the security states, which makes them feasible for the online implementation.

Further, the research has also focused on the important aspect of control mechanism for the security enhancement. During the N-1 line outage contingency scenario, the transmission lines will be overloaded. In such a case, one of the control strategy is generation rescheduling. But, the important aspect at this instance is security enhancement with minimum fuel cost. Several algorithms do exists to perform the task. However, an efficient algorithm will yield the desired objectives. In order to achieve this objective, a meta-heuristic algorithm known as enhanced cuckoo search algorithm is developed to reschedule the generators with minimum cost, such that the severity is minimized. Initially, contingency analysis is performed and critical contingencies are identified based on severity index. For a specific N-1 critical contingency, generators are rescheduled to alleviate the overloaded lines with minimum fuel cost. In order to prove the accuracy of the ECS algorithm, the results are compared with CS, PSO and BA. From the simulation results it is observed that the ECS algorithm is efficient in providing a solution to the contingency constrained economic load dispatch for security enhancement.

On summary, all these results assure the effectiveness and robustness of the proposed approaches for efficient security assessment and enhancement.

7.2 Future Scope

This research has explored some good ideas and suitable solutions in the area of power system security. Based on the experience gained from this work, the following aspects require for further investigation.

- With the increased penetration of distributed generation, the uncertainty provides a scope to investigate the security aspects with the combination of conventional energy sources.
- Investigations can be carried out to find suitable approaches or control strategies against cyber-attacks on power systems.
- Investigations can be carried to find out efficient techniques for transient and dynamic security assessment.
- Investigations can be carried out for the security assessment under multiple line outage and generator outage conditions.

Bibliography

[1] L. Wehenkel. Machine Learning Approaches to Power System Security Assessment. *IEEE Intelligent Systems Magazine*, 12(5):60 -- 72, September/October 1997.

[2] D. S. Kirschen. Power system security. *Power Engineering Journal*, 16(5):241 -- 248, October 2002.

[3] K. Morison, L. Wang, and P. Kundur. Power system security assessment. *IEEE Power and Energy Magazine*, 2(5), 30 -- 39, September/October. 2004.

[4] M. Shahindehpour and Y. wang. *Communications and control in Electric Power Systems.* Newyork: wiley, 2003.

[5] P. Kundur. *Power System Stability and Control*. Mc Graw-Hill Professional Publishing, 1994.

[6] L. A. Zadeh. Soft computing and fuzzy logic. *IEEE Software*, 11(6), 48 -- 56, November 1994.

[7] T. Mitchell. *Machine Learning*. McGraw-Hill, 1997.

[8] U. M. Fayyad, G. P. Shapiro, P. Smyth, and R. Uthurusamy. *Advances in knowledge discovery and data mining*, American Association for Artificial Intelligence, 1996.

[9] A. J. Wood and B. F. Wollenberg. *Power generation, operation and control*, John Wiley & Sons, pp. 410-415, 2009.

[10] B. Stott, O. Alsac and A. J. Monticelli. Security analysis and optimization. *Proceedings of IEEE*, 75(12):1623 -- 1644, December 1987.

[11] Hadi Saadat. *Power System Analysis*. Tata McGraw-Hill. Edition 2002.

[12] N.M. Peterson W.F. Tinney and D.W. Bree. Iterative linear AC power flow for fast approximate outage studies. *IEEE Transactions on Power Apparatus and Systems*, 91(5):2048 -- 2058, October 1972.

[13] K.R.C. Mamandur and G.J. Berg. Efficient Simulation of Line and Transformer Outages in Power System. *IEEE Transactions on Power Apparatus and Systems*, 101(10):3733 -- 3641, October 1982.

[14] M.S. Sachdev and S.A. Ibrahim. A Fast Approximate Technique for Outage Studies in Power System Planning and Operating. *IEEE Transactions on Power Apparatus and Systems*, 93: 1133 -- 1042, May 1974.

[15] B. Stott and O. Alsac. Fast Decoupled Load Flow. IEE Transactions on Power Apparatus and Systems, 93:859 -- 869, June 1974.

[16] O. Alsac and B. Stott. Optimal Load Flow with Steady- State Security. *IEEE Transactions on Power Apparatus and Systems*, 93:745 -- 751, June, 1974.

[17] C. Lee and N. Chen. Distribution factors of reactive power flow in transmission line and transformer outage studies. *IEEE Transactions on Power Systems*, 7(1):194 -- 200, February 1992.

[18] S.N. Singh and S.C. Srivastava. Improved voltage and reactive power distribution for outage studies. *IEEE Transactions on Power Systems*, 12(3): 1085 -- 1093, August 1997.

[19] G. C. Ejebe and B. F. Wollenberg. Automatic Contingency Selection. *IEEE Transactions on Power Apparatus and Systems*, 98(1): 97 -- 109, January 1979.

[20] T. A. Mikolinnas and B. F. Wollenberg. An Advanced Contingency Selection Algorithm. *IEEE Transactions on Power Apparatus and Systems*, 100(2): 608 -- 617, February 1981.

[21] G. D. Irisarri and A. M Sasson. Automatic Contingency Selection Method for On-Line Security Analysis. *IEEE Transactions on Power Apparatus and Systems*, 100(4):1838 -- 1844, April 1981.

[22] T. F Halpin, R. Fischl, and R. Fink. Analysis of Automatic Contingency Selection Algorithms. *IEEE Transactions on Power Apparatus and Systems*, 103(5):938 -- 945, May 1984.

[23] B. Stott, O. Alsac, and F. Alvarado. Analytical and Computational Improvements in Performance-Index Ranking Algorithms for Networks. *International Journal of Electrical Power and Energy Systems*, 7(3):154 -- 160, July 1985.

[24] I. Dabbaghchi and G. D. Irisarri. AEP Automatic Contingency Selector. *IEEE Transactions on Power Systems*, 1(2), 37 -- 45, May 1986.

[25] M. G. Lauby. Evaluation of a Local DC Load Flow Screening Method for Branch Contingency Selection of Overloads. *IEEE Transactions on Power Systems*, 3(3):923 -- 928, August 1988.

[26] M. G. Lauby, T. A. Mikolinnas, and N. D. Reppen. Contingency Selection of Branch Outages Causing Voltage Problems. *IEEE Transactions on Power Apparatus and Systems*, 102(12):3899-3904, December 1983.

[27] J. Zaborsky, K. W. Whang, and K. Prasad. Fast Contingency Evaluation Using Concentric Relaxation. *IEEE Transactions on Power Apparatus and Systems*, 99(1):28 -- 36, January 1980.

[28] F. Albuyeh, A. Bose**,** and B. Heath. Reactive Power Considerations in Automatic Contingency Selection. *IEEE Transactions on Power Apparatus and Systems*, 101(1), 107 -- 112, January 1982.

[29] F. D. Galiana. Bound Estimates of the Severity of Line Outages in Power System Analysis and Ranking. *IEEE Transactions on Power Apparatus and Systems*, 103(9):2612 -- 2622, September 1984.

[30] K. Nara, K. Tanaka, H. Kodama, R. Shoults, M. S. Chen**,** V. Olinda, and D. Bertagnolli. On-Line Contingency Selection for Voltage Security Analysis. *IEEE Transactions on Power Apparatus and Systems*, 104(4):846 -- 856, April 1985.

[31] V. Brandwajn. Efficient Bounding Method for Linear Contingency Analysis. *IEEE Transactions on Power Systems*, 3(3):38 -- 43, February 1988.

[32] V. Brandwajn and M. G. Lauby. Completing bounding method for AC contingency screening. *IEEE Transactions on Power Systems*, 4(2):724 -- 729, May 1989.

[33] R. Bacher and W.F. Tinney. Faster local power flow solutions: the zero mismatch approach. *IEEE Transactions on Power Systems*, 4(4):1345 -- 1354, October 1989.

[34] G. D. Irisarti, D. Levner, and A. M. Sassoq. Automatic contingency selection for on-line contingency analysis-real time tests. *IEEE Transactions on Power Apparatus and Systems*, 98(5):1552 -- 1559, September 1979.

[35] G. K. Stefopoulos, F. Yang G. J. Cokkinides, and A. P. S. Meliopoulos, Advanced contingency selection methodology, *Proceedings of the 37th Annual North American Power Symposium*, 67 -- 73, October 2005.

[36] A. O. Ekwue. A review of automatic contingency selection algorithms for online security analysis. *Third International Conference on Power System Monitoring and Control*, 152 -- 155, June 1991.

[37] R. Fischil, T.F. Halpin and A. Guvenis. The application of decision theory to contingency selection. *IEEE Transactions on circuits and systems*, 29(11):712 -- 723, November 1982.

[38] G. C. Ejebe, G. D. Irisarri, S. Mokhtari, O. Obadina, P. Ristanovic and J. Tong. Methods for contingency screening and ranking for voltage stability analysis of power systems. *IEEE Transactions on power systems*, 11(1):350 -- 356, February 1996.

[39] N. Amjady and M. Esmaili. Application of new sensitivity analysis frame work for voltage contingency ranking. *IEEE Transactions on power systems*, 20(2):973 – 983, May 2005.

[40] C. L. Chang and Y. Y. Hsu. A new approach to dynamic contingency selection. *IEEE Transactions on power systems*, 5(4):1524 – 1528, November 1990.

[41] Y. Chen and A. Bose, Direct ranking for voltage contingency selection. *IEEE Transactions on power systems*, 4(4):1335 -- 1344. October 1989.

[42] A. Mohamed and G. B. Jasmon. Voltage contingency selection technique for security assessment. *IEE proceedings Generation, Transmission and Distribution*, 136(1):24 -- 28, January 1989.

[43] P. Zhang, F. Li, and N. Bhatt. Next-Generation Monitoring, Analysis, and Control for the Future Smart Control Center. *IEEE Transactions on Smart Grid*, 1(2):186 -- 192, September 2010.

[44] C. A. Jensen, M. A. El-Sharkawi, and R. J. Marks. Power system security assessment using neural networks: Feature selection using fisher discrimination. *IEEE Transactions on Power Syst*ems, 16(4):757 -- 763, November 2001.

[45] L. H. Hassan, M. Moghavvemi, H. A. F. Almurib and O. Steinmayer. Current state of neural networks applications in power system monitoring and control, *International Journal of Electrical Power and Energy Systems*, 51:134 -- 144, October 2013.

[46] V. S. S. Vankayala and N. D. Rao. Artificial neural network and their application to power system-A bibliographical survey. *Electric Power System Research*, 28(1):67 -- 79, October 1993.

[47] K. S. Swarup and P. B. Corthis. ANN approach assesses system security. *IEEE Transactions on Computer Applications in Power*, 15(3):32 -- 38, July 2002.

[48] T. S. Sidhu and C. Lan. Contingency screening for steady-state security analysis by using FFT and artificial neural networks. *IEEE Transactions on Power Systems*, 15(1):421 -- 426, February 2000.

[49] 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 system. *IEEE Transactions on Power Systems*, 27(3):1253 -- 1263, August 2012.

[50] K. R. Niazi, C. M. Arora and S.L. Surana. Power system security evaluation using ANN: feature selection using divergence. *Electric Power System Research,* 69(2):161 -- 167, May 2004.

[51] S. N. Singh, L. Srivastava and J. Sharma. Fast voltage contingency screening and ranking using cascade neural network. *Electric Power System Research*, 53(3):197 -- 205, March 2000.

[52] L. Srivastava, S. N. Singh and J. Sharma. A hybrid neural network model for fast voltage contingency screening and ranking. *International Journal of Electrical Power and Energy Systems,* 22(1):35 -- 42, January 2000.

[53] R. Singh and L. Srivastava. Line flow contingency selection and ranking using cascade neural network. *Neuro computing*, 70(16):2645 -- 2650, October 2007.

[54] K. L. Lo, L. J. Peng, J. F. Macqueen, A. O. Ekwue, D. T. Y. Cheng. Fast real power contingency ranking using a counter propagation network. *IEEE Transactions on Power Systems*, 13(4):1259 -- 1264, November 1998.

[55] S. Chauhan. Fast real power contingency ranking using counter propagation network: feature selection by neuro-fuzzy model. *Electric Power System Research*, 73(3):343 -- 352, March 2005.

[56] M. Pandit, L. Srivastava, and J. Sharma. Contingency ranking for voltage collapse using parallel self-organizing hierarchical neural network. *International Journal of Electrical Power and Energy Systems*, 23(5):369 -- 379, June 2001.

[57] M. Pandit, L. Srivastava and J. Sharma. Fast voltage contingency selection using fuzzy parallel self-organizing hierarchical neural network. *IEEE Transactions on Power Syst*ems, 18(2):657 -- 664, May 2003.

[58] D. Niebur, and A. Germond. Power system static security assessment using the Kohonen neural network classifier. *IEEE Transactions on Power Syst*ems, 7(2): 865 -- 872, May 1992.

[59] S. Kalyani, and K. S. Swarup. Pattern analysis and classification for security evaluation in power networks. *International Journal of Electrical Power and Energy Systems,* 44(1):547 -- 560, January 2013.

[60] T. K. P. Medicherla, R. Billington, and M. S. Sachdev. Generation rescheduling and load shedding to alleviate line overload-analysis. *IEEE transactions on Power Apparatus and Systems,* 98(6):1876 -- 1884, November 1979.

[61] W. R. Lachs. Transmission line overloads: real-time control. *IEE Proceedings Generation, Transmission and Distribution,* 134(5):342 -- 347, September 1987.

[62] A. N. Udupa, G. K. Purushothama, K. Parthasarathy, and D. Thukaram. A fuzzy control for network overload alleviation. *International Journal of Electrical Power and Energy Systems*, 23(2):119 -- 128, February 2001.

[63] H. W. Dommel and W. F. Tinney. Optimal power flow solutions. *IEEE transactions on Power Apparatus and Systems*, 87(10):1866 -- 1876, October 1968.

[64] D. I. Sun, B. Ashley, B. Brewer, A. Hughes, and W. F. Tinney. Optimal power flow by Newton approach. *IEEE transactions on Power Apparatus and Systems*, 103(10):2864 -- 2880, October 1984.

[65] P. Acharjee and S. Goswami. A decoupled power flow algorithm using particle swarm optimization technique. *Energy Conversion and Management*, 50(9):2351 -- 2360, September 2009.

[66] F. Capitanescu and L. Wehenkel. Experiments with the interior-point method for solving large scale optimal power flow problems. *Electric Power System Research*, 95:276 -- 283, February 2013.

[67] W. Ongsakul and T. Tantimaporn. Optimal power flow by improved evolutionary programming. *Electric Power Components and Systems*. 34(1):79 -- 95, 2006.

[68] U. Kılıc, K. Ayan, and U. Arifoglu. Optimizing reactive power flow of HVDC systems using genetic algorithm. *International Journal of Electrical Power and Energy Systems*, 55:1 -- 12, February 2014.

[69] M. S. Kumari and S. Maheswarapu. Enhanced genetic algorithm based computation technique for multi-objective optimal power flow solution," *International Journal of Electrical Power and Energy Systems,* 32(6):736 -- 742, July 2010.

[70] R. H. Liang, S. R. Tsai, Y. T. Chen, and W. T. Tseng. Optimal power flow by a fuzzy based hybrid particle swarm optimization approach. *International Journal of Electrical Power and Energy Systems*, 81(7):1466 -- 1474, July 2011.

[71] A. Abou El Ela, M. Abido, and S. Spea. Optimal power flow using differential evolution algorithm. *Electric Power System Research,* 80(7):878 -- 885, July 2010.

[72] J. A. Momoh, J. Z. Zhu, G. D. Boswell, and S. Hoffman, Power system security enhancement by OPF with phase shifter. *IEEE transactions on power systems*, 16(2):287 -- 293, May 2001.

[73] D. Devaraj and B. Yegnanarayana. Genetic-algorithm based optimal power flow for security enhancement. *IEE Proceedings Generation, Transmission and Distribution,* 152(6):899 -- 905, November 2005.

[74] P. Somasundram and P. Kuppusamy. Application of evolutionary programming to security constrained economic dispatch. *International Journal of Electrical Power and Energy Systems*, 27(5):343 -- 351. June/July 2005.

[75] P. Venkatesh, R. Nanadass, and N. P. Padhy. Comparison and application of evolutionary programming techniques to combined economic emission dispatch with line flow constraints. *IEEE transactions on power systems*, 18(2):688 -- 697, May 2003.

[76] K. Y. Lee and J. B. Park. Application of Particle Swarm Optimization to Economic Dispatch Problem: Advantages and Disadvantages. *Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES*, 188 -- 192, October/November 2006.

[77] Engineering Applications of Neural Networks. *Proceedings of 14th International Conference,* Halkidiki, Greece, Springer-Verlag Berlin Heidelberg, September 2013.

[78] Robert Hecht-Nielsen, *Neurocomputing*, Addison-Wesley Publishing Company, Inc. USA, 1990.

[79] D. E. Rumelhart and J. L. McClelland Eds. *Parallel distributed processing: Explorations in the microstructure of cognition*, Vol. 1, MIT Press, 1986.

[80] M. G. Danikas, N. Gao, and M. Aro. Partial discharge recognition using neural networks: A review", *Electrical Engineering*, 85(2):87 -- 93, 2003.

[81] L. Kanal. Patterns in pattern recognition: 1968–1974. *IEEE Transactions on Information Theory*, 20(6):697 -- 722, November 1974.

[82] Sa Da Costa J and N. Munro. Pattern recognition in power system security. *International Journal of Electrical Power and Energy Systems*, 6(1):31 -- 36, 1984.

[83] S. Oh. A pattern recognition and associative memory approach to power system security assessment. *IEEE Transactions on Systems, Man and Cybernetics*, 16(1):62 -- 72, January 1986.

[84] L. Breiman, J. Friedman, R. A. Olshen, and C. J. Stone. *Classification and Regression Trees*. Boca Raton, FL, USA: Chapman &Hall/CRC, 1984.

[85] J. R. Quinlan. C4.5: *Programs for Machine Learning*. Morgan Kaufman publishers: USA, 1993.

[86] K. Sun, S. Likhate, V. Vittal, V. S. Kolluri, and S. Mandal. An online dynamic security assessment scheme using phasor measurements and decision trees. *IEEE transactions on power systems*, 22(4):1935 -- 1943, November 2007.

[87] V. Krishnan, J. D. McCalley, S. Henry, and S. Issad. Efficient database generation for decision trees based power system security assessment. *IEEE transactions on power systems* 26(4):2319 -- 2327, November 2011.

[88] R. Diao , k. Sun, V. Vittal, R. J. O'Keeefe, M. R. Richardson, N. Bhatt, D. Stradford, and S. K. Sarawgi. Decision tree-based online voltage security assessment using PMU measurements. *IEEE transactions on power systems*, 24(2):832 -- 839, May 2009.

[89] R. Diao, V. Vittal, and N. Logic. Design of a real-time security assessment tool for situational awareness enhancement in modern power systems. *IEEE transactions on power systems* 25(2):957 -- 965, May 2010.

[90] E. E. Bernabeu, J. S. Thorp, and V. Centeno. Methodology for a security/dependability adaptive protection scheme based on data mining. *IEEE Transactions on Power Delivery,* 27(1):104 -- 111, January 2012.

[91] E. M. Voumvoulakis, A. E. Gavoyiannis, and N. D. Hatziargyriou. Decision trees for dynamic security assessment and load shedding scheme. *Power Engineering Society General Meeting*, 2006.

[92] C. Liu, K. Sun, Z. H. Rather, Z. Chen, C. L. Bak, P. Thogersen, and P. Lund. A systematic approach for dynamic security assessment and the corresponding preventive control scheme based on decision trees. *IEEE transactions on power systems*, 29(2):717 -- 730, March 2014.

[93] L. Breiman. Random forests. Machine Learning 45:5 – 32, 2001.
[Online] Available:http://www.stat.berkeley.edu/users/breiman/RandomForests

[94] X. S. Yang, and S. Deb. Cuckoo search via Levy flights. *World Congress on Nature & Biologically Inspired Computing, 2009, NaBIC 2009,* 210 – 214, December 2009.

[95] A. B. Mohamad, A. M, Zain, and N. E. N. Bazin. Cuckoo Search Algorithm for optimization problems—A Literature Review and its Applications. *Applied Artificial Intelligence*, 28(5):419 -- 448, May 2014.

[96] S. K. Injeti, V. K. Thunuguntla, and M. shareef. Optimal allocation of capacitor banks in radial distribution systems for minimization of real power loss and maximization of network savings using bio-inspired optimization algorithms. Electrical Power Energy Systems, vol. 69, pp. 441 -- 455, July 2015.

[97] T. T. Nguyen and A. V. Truong, "Distribution network reconfiguration for power loss minimization and voltage profile improvement using cuckoo search algorithm. *International Journal of Electrical Power and Energy Systems*, 68:233 -- 242, June 2015.

[98] P. Dash, L. C. Saikia, and N. Sinha. Comparison of performances of several FACTS devices using Cuckoo search algorithm optimized 2DOF controllers in multi-area AGC," *International Journal of Electrical Power and Energy Systems*, 65:316 -- 324, February 2015.

[99] S. Berrazouane and K. Mohammedi. Parameter optimization via cuckoo optimization algorithm of fuzzy controller for energy management of a hybrid power system. *Energy Conversion and Management*, 78:652 -- 660, February 2014.

[100] P. Dash, L. C. Saikia, and N. Sinha. Comparison of performances of several Cuckoo search algorithm based 2DOF controllers in AGC of multi-area thermal system. *International Journal of Electrical Power and Energy Systems*, 55:429 -- 436, February 2014.

[101] A. A. El-Fergany and A. Y. Abdelaziz. Capacitor allocations in radial distribution networks using cuckoo search algorithm. *IET Generation, Transmission & Distribution*, 8(2), 223 -- 232, February 2014.

[102] Z. Moravej and A. Akhlaghi. A novel approach based on cuckoo search for DG allocation in distribution network," *International Journal of Electrical Power and Energy Systems*, 44(1):672 -- 679, January 2013.

[103] D. N. Vo, P. Schegner, and W. Ongsakul. Cuckoo search algorithm for non-convex economic dispatch. *IET Generation, Transmission & Distribution*, 7(6), 645 -- 654, June 2013.

[104] Power system test cases at https://www.ee.washington.edu/research/pstca/

[105] The Math Works Inc, MATLAB R2010a.

Appendix

Appendix A

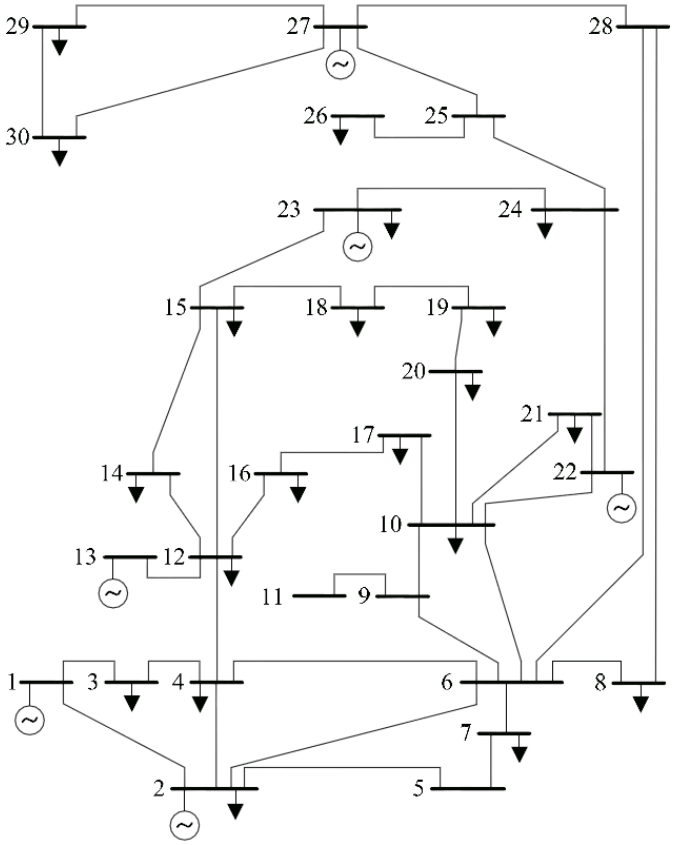

Figure A.1: Topology of the IEEE-30 bus test system

IEEE-30 bus system test data:

A.1 Bus data:

Bus No.	Bus Code	Voltage magnitude	Angle (Degree)	Load		Generator				Injected Mvar
				MW	Mvar	MW	Mvar	Qmin	Qmax	
1	1	1.06	0	0	0	260.2	-16.1	0	0	0
2	2	1.043	0	21.7	12.7	40	50	50	-40	0
3	0	1.021	0	2.4	1.2	0	0	0	0	0
4	0	1.012	0	7.6	1.6	0	0	0	0	0
5	2	1.01	0	94.2	19	0	37	40	-40	0
6	0	1.01	0	0	0	0	0	0	0	0
7	0	1.002	0	22.8	10.9	0	0	0	0	0

8	2	1.01	0	30	30	0	37.3	40	-10	0
9	0	1.051	0	0	0	0	0	0	0	0
10	0	1.045	0	5.8	2	0	0	0	0	0.19
11	2	1.082	0	0	0	0	16.2	24	-6	0
12	0	1.057	0	11.2	7.5	0	0	0	0	0
13	2	1.071	0	0	0	0	10.6	24	-6	0
14	0	1.042	0	6.2	1.6	0	0	0	0	0
15	0	1.038	0	8.2	2.5	0	0	0	0	0
16	0	1.045	0	3.5	1.8	0	0	0	0	0
17	0	1.04	0	9	5.8	0	0	0	0	0
18	0	1.028	0	3.2	0.9	0	0	0	0	0
19	0	1.026	0	9.5	3.4	0	0	0	0	0
20	0	1.03	0	2.2	0.7	0	0	0	0	0
21	0	1.033	0	17.5	11.2	0	0	0	0	0
22	0	1.033	0	0	0	0	0	0	0	0
23	0	1.027	0	3.2	1.6	0	0	0	0	0
24	0	1.021	0	8.7	6.7	0	0	0	0	0.043
25	0	1.017	0	0	0	0	0	0	0	0
26	0	1	0	3.5	2.3	0	0	0	0	0
27	0	1.023	0	0	0	0	0	0	0	0
28	0	1.007	0	0	0	0	0	0	0	0
29	0	1.003	0	2.4	0.9	0	0	0	0	0
30	0	0.992	0	10.6	1.9	0	0	0	0	0

A.2 Line data:

Start Bus	End Bus	R (pu)	X (pu)	B/2 (pu)	Tap setting Value
1	2	0.0192	0.0575	0.0528	0
1	3	0.0452	0.1652	0.0408	0
2	4	0.057	0.1737	0.0368	0
3	4	0.0132	0.0379	0.0084	0
2	5	0.0472	0.1983	0.0418	0
2	6	0.0581	0.1763	0.0374	0
4	6	0.0119	0.0414	0.009	0
5	7	0.046	0.116	0.0204	0
6	7	0.0267	0.082	0.017	0
6	8	0.012	0.042	0.009	0
6	9	0	0.208	0	0.978
6	10	0	0.556	0	0.969
9	11	0	0.208	0	0
9	10	0	0.11	0	0
4	12	0	0.256	0	0.932
12	13	0	0.14	0	0
12	14	0.1231	0.2559	0	0
12	15	0.0662	0.1304	0	0
12	16	0.0945	0.1987	0	0
14	15	0.221	0.1997	0	0
16	17	0.0524	0.1923	0	0

15	18	0.1073	0.2185	0	0
18	19	0.0639	0.1292	0	0
19	20	0.034	0.068	0	0
10	20	0.0936	0.209	0	0
10	17	0.0324	0.0845	0	0
10	21	0.0348	0.0749	0	0
10	22	0.0727	0.1499	0	0
21	22	0.0116	0.0236	0	0
15	23	0.1	0.202	0	0
22	24	0.115	0.179	0	0
23	24	0.132	0.27	0	0
24	25	0.1885	0.3292	0	0
25	26	0.2544	0.38	0	0
25	27	0.1093	0.2087	0	0
28	27	0	0.396	0	0.968
27	29	0.2198	0.4153	0	0
27	30	0.3202	0.6027	0	0
29	30	0.2399	0.4533	0	0
8	28	0.0636	0.2	0.0428	0
6	28	0.0169	0.0599	0.013	0

A.3 Generator data:

Bus No.	P_g^{min} (MW)	P_g^{max} (MW)	Cost Coefficients		
			a	b	c
1	50	200	0	2.0	0.00375
2	20	80	0	1.75	0.0175
5	15	50	0	1.0	0.0625
8	10	35	0	3.25	0.00834
11	10	30	0	3.0	0.025
13	12	40	0	3.0	0.025

Appendix B

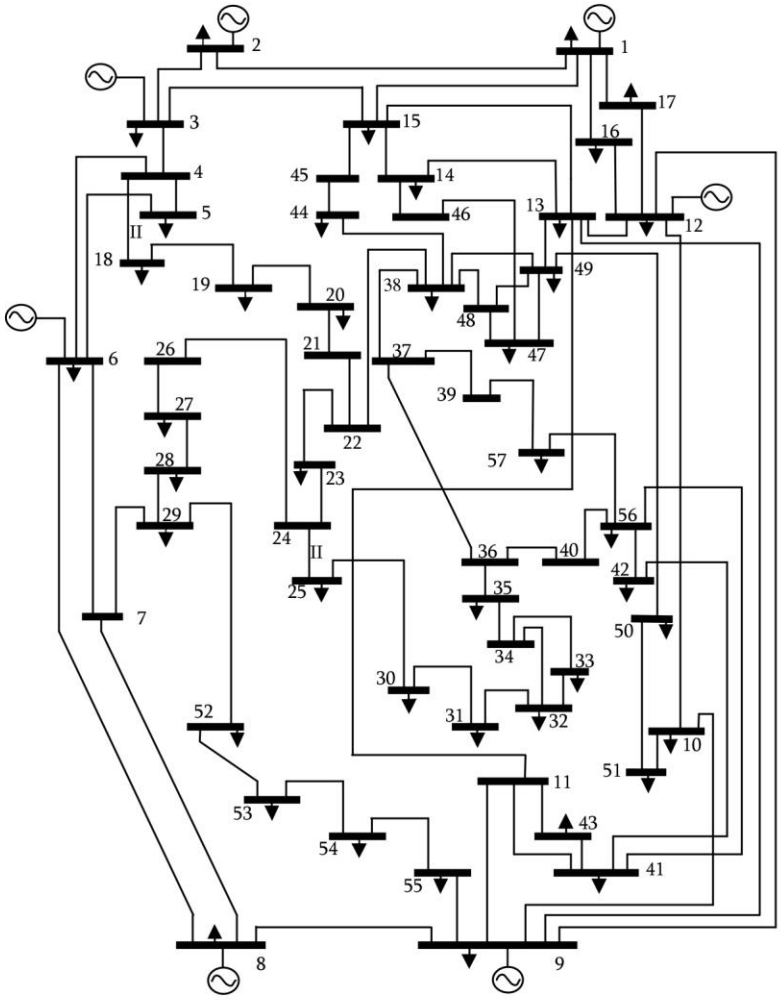

Figure A.2: Topology of the IEEE-57 bus test system

IEEE-57 bus system test data:

B.1 Bus data:

Bus No.	Bus Code	Voltage magnitude	Angle (Degree)	Load		Generator				Injected Mvar
				MW	Mvar	MW	Mvar	Qmin	Qmax	
1	1	1.04	0	55	17	128.9	-16.1	-140	200	0
2	2	1.01	0	3	88	0	-0.8	-17	50	0
3	2	0.985	0	41	21	40	-1	-10	60	0

4	0	0.981	0	0	0	0	0	0	0	0
5	0	0.976	0	13	4	0	0	0	0	0
6	2	0.98	0	75	2	0	0.8	-8	25	0
7	0	0.984	0	0	0	0	0	0	0	0
8	2	1.005	0	150	22	450	62.1	-140	200	0
9	2	0.98	0	121	26	0	2.2	-3	9	0
10	0	0.986	0	5	2	0	0	0	0	0
11	0	0.974	0	0	0	0	0	0	0	0
12	2	1.015	0	377	24	310	128.5	-150	155	0
13	0	0.979	0	18	2.3	0	0	0	0	0
14	0	0.97	0	10.5	5.3	0	0	0	0	0
15	0	0.988	0	22	5	0	0	0	0	0
16	0	1.013	0	43	3	0	0	0	0	0
17	0	1.017	0	42	8	0	0	0	0	0
18	0	1.001	0	27.2	9.8	0	0	0	0	10
19	0	0.97	0	3.3	0.6	0	0	0	0	0
20	0	0.964	0	2.3	1	0	0	0	0	0
21	0	1.008	0	0	0	0	0	0	0	0
22	0	1.01	0	0	0	0	0	0	0	0
23	0	1.008	0	6.3	2.1	0	0	0	0	0
24	0	0.999	0	0	0	0	0	0	0	0
25	0	0.982	0	6.3	3.2	0	0	0	0	5.9
26	0	0.959	0	0	0	0	0	0	0	0
27	0	0.982	0	9.3	0.5	0	0	0	0	0
28	0	0.997	0	4.6	2.3	0	0	0	0	0
29	0	1.01	0	17	2.6	0	0	0	0	0
30	0	0.962	0	3.6	1.8	0	0	0	0	0
31	0	0.936	0	5.8	2.9	0	0	0	0	0
32	0	0.949	0	1.6	0.8	0	0	0	0	0
33	0	0.947	0	3.8	1.9	0	0	0	0	0
34	0	0.959	0	0	0	0	0	0	0	0
35	0	0.966	0	6	3	0	0	0	0	0
36	0	0.976	0	0	0	0	0	0	0	0
37	0	0.985	0	0	0	0	0	0	0	0
38	0	1.013	0	14	7	0	0	0	0	0
39	0	0.983	0	0	0	0	0	0	0	0
40	0	0.973	0	0	0	0	0	0	0	0
41	0	0.996	0	6.3	3	0	0	0	0	0
42	0	0.966	0	7.1	4.4	0	0	0	0	0
43	0	1.01	0	2	1	0	0	0	0	0
44	0	1.017	0	12	1.8	0	0	0	0	0
45	0	1.036	0	0	0	0	0	0	0	0
46	0	1.05	0	0	0	0	0	0	0	0
47	0	1.033	0	29.7	11.6	0	0	0	0	0
48	0	1.027	0	0	0	0	0	0	0	0
49	0	1.036	0	18	8.5	0	0	0	0	0
50	0	1.023	0	21	10.5	0	0	0	0	0
51	0	1.052	0	18	5.3	0	0	0	0	0
52	0	0.98	0	4.9	2.2	0	0	0	0	0
53	0	0.971	0	20	10	0	0	0	0	6.3

54	0	0.996	0	4.1	1.4	0	0	0	0	0
55	0	1.031	0	6.8	3.4	0	0	0	0	0
56	0	0.968	0	7.6	2.2	0	0	0	0	0
57	0	0.965	0	6.7	2	0	0	0	0	0

B.2 Line data:

Start Bus	End Bus	R (pu)	X (pu)	B/2 (pu)	Tap setting Value
1	2	0.0083	0.028	0.0645	1
2	3	0.0298	0.085	0.0409	1
3	4	0.0112	0.0366	0.0190	1
4	5	0.0625	0.132	0.0129	1
4	6	0.043	0.148	0.0174	1
6	7	0.02	0.102	0.0138	1
6	8	0.0339	0.173	0.0235	1
8	9	0.0099	0.0505	0.0274	1
9	10	0.0369	0.1679	0.0220	1
9	11	0.0258	0.0848	0.0109	1
9	12	0.0648	0.295	0.0386	1
9	13	0.0481	0.158	0.0203	1
13	14	0.0132	0.0434	0.0055	1
13	15	0.0269	0.0869	0.0115	1
1	15	0.0178	0.091	0.0494	1
1	16	0.0454	0.206	0.0273	1
1	17	0.0238	0.108	0.0143	1
3	15	0.0162	0.053	0.0272	1
4	18	0	0.555	0	0.970
4	18	0	0.43	0	0.978
5	6	0.0302	0.0641	0.0062	1
7	8	0.0139	0.0712	0.0097	1
10	12	0.0277	0.1262	0.0164	1
11	13	0.0223	0.0732	0.0094	1
12	13	0.0178	0.058	0.0302	1
12	16	0.018	0.0813	0.0108	1
12	17	0.0397	0.179	0.0238	1
14	15	0.0171	0.0547	0.0074	1
18	19	0.461	0.685	0	1
19	20	0.283	0.434	0	1
21	20	0	0.7767	0	1.043
21	22	0.0736	0.117	0	1
22	23	0.0099	0.0152	0	1
23	24	0.166	0.256	0.0042	1
24	25	0	1.182	0	1.001
24	25	0	1.23	0	1.001
24	26	0	0.0473	0	1.043
26	27	0.165	0.254	0	1
27	28	0.0618	0.0954	0	1

28	29	0.0418	0.0587	0	1
7	29	0	0.0648	0	0.967
25	30	0.135	0.202	0	1
30	31	0.326	0.497	0	1
31	32	0.507	0.755	0	1
32	33	0.0392	0.036	0	1
34	32	0	0.953	0	0.975
34	35	0.052	0.078	0.0016	1
35	36	0.043	0.0537	0.0008	1
36	37	0.029	0.0366	0	1
37	38	0.0651	0.1009	0.0010	1
37	39	0.0239	0.0379	0	1
36	40	0.03	0.0466	0	1
22	38	0.0192	0.0295	0	1
11	41	0	0.749	0	0.955
41	42	0.207	0.352	0	1
41	43	0	0.412	0	1
38	44	0.0289	0.0585	0.0010	19900
15	45	0	0.1042	0	0.955
14	46	0	0.0735	0	0.900
46	47	0.023	0.068	0.0016	1
47	48	0.0182	0.0233	0	1
48	49	0.0834	0.129	0.0024	1
49	50	0.0801	0.128	0	1
50	51	0.1386	0.22	0	1
10	51	0	0.0712	0	0.930
13	49	0	0.191	0	0.895
29	52	0.1442	0.187	0	1
52	53	0.0762	0.0984	0	1
53	54	0.1878	0.232	0	1
54	55	0.1732	0.2265	0	1
11	43	0	0.153	0	0.958
44	45	0.0624	0.1242	0.0020	1
40	56	0	1.195	0	0.958
56	41	0.553	0.549	0	1
56	42	0.2125	0.354	0	1
39	57	0	1.355	0	0.980
57	56	0.174	0.26	0	1
38	49	0.115	0.177	0.0015	1
38	48	0.0312	0.0482	0	1
9	55	0	0.1205	0	0.940

Dissemination

SCI International Journal Articles

[1] P. Sekhar and S. Mohanty. An Online Power System Static Security Assessment Module Using Multi-Layer Perceptron and Radial Basis Function Network. *International Journal of Electrical power and Energy systems*, 76:165 -- 173, March 2016.

[2] P. Sekhar and S. Mohanty. Classification and assessment of power system static security using decision tree and random forest classifiers. *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, Published online, August 2015. (DOI: 10.1002/jnm.2096)

[3] P. Sekhar and S. Mohanty. An enhanced cuckoo search algorithm based contingency constrained economic load dispatch for security enhancement. *International Journal of Electrical power & Energy systems*, 75:303 -- 310, February 2016.

Conference Presentations

[1] P. Sekhar and S. Mohanty. Power system contingency ranking using Newton Raphson load flow method. *International IEEE India Conference (INDICON)*, IIT Bombay, 1 -- 4, December 2013.

[2] P. Sekhar and S. Mohanty. Overall performance index based power system contingency ranking using Gauss-Seidal load flow method. *Proceedings of Recent advances in power, energy and control (RAPEC)*, NIT Rourkela, November 2013.

Electrical Power and Energy Systems 76 (2016) 165–173

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

An online power system static security assessment module using multi-layer perceptron and radial basis function network

Pudi Sekhar *, Sanjeeb Mohanty

Dept. of Electrical Engineering, National Institute of Technology, Rourkela, India

ARTICLE INFO

Article history:
Received 3 August 2015
Received in revised form 14 September 2015
Accepted 4 November 2015

Keywords:
Artificial neural network
Power system security
Contingency ranking module
Security assessment

ABSTRACT

Efficient contingency screening and ranking method has gained importance in modern power systems for its secure operation. This paper proposes two artificial neural networks namely multi-layer feed forward neural network (MFNN) and radial basis function network (RBFN) to realize the online power system static security assessment (PSSSA) module. To assess the severity of the system, two indices have been used, namely active power performance index and voltage performance index, which are computed using Newton–Raphson load flow (NRLF) analysis for variable loading conditions under $N-1$ line outage contingencies. The proposed MFNN and RBFN models based PSSSA module, are fed with power system operating states, load conditions and $N-1$ line outage contingencies as input features to train the neural network models, to predict the performance indices for unseen network conditions and rank them in descending order based on performance indices for security assessment. The proposed approaches are tested on standard IEEE 30-bus test system, where the simulation results prove its performance and robustness for power system static security assessment. The comparison of severity obtained by the neural network models and the NRLF analysis in terms of time and accuracy, signifies that the proposed model is quick, accurate and robust for power system static security evaluation for unseen network conditions. Thus, the proposed PSSSA module implemented using MFNN and RBFN models are found to be feasible for online implementation.

Introduction

The power system is a complex network, where the security of the power system has gained importance for reliable operation. The power system security assessment is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation [1]. The power system security assessment involves three major tasks, namely security monitoring, contingency analysis and security control. Security monitoring is a mechanism, which provides the system operating conditions to the operational engineers. The contingency analysis plays a vital role in the power system security assessment, the importance of which is discussed in [2,3]. This stage includes contingency screening and ranking. If the power system is found to be insecure, necessary control actions are implemented to bring back the insecure state of the system to secure.

The research in this area has been carried out extensively in the past few years, which includes contingency ranking or screening methods for security assessment. The most ranking methods are based on the evaluation by means of performance indices (PI), which is the measure of the system stress. In this approach, the contingencies are ranked based on the severity obtained from network variables and are directly assessed. The static security assessment inspect the severity under post contingency scenario, which includes solving various load flow methods for base case and $N-1$ line outage conditions. These methods are highly complex and time consuming for online implementation. Also, the system operating conditions vary from time to time, which makes the conventional methods are infeasible for online implementation. Thus, there is a need to develop efficient online tool (which monitor the system security under variable system conditions) for power system security assessment to ensure safe operation of the power system [4]. The deregulation has compelled the utilities to function their systems closer to their security limits, which demands quick and efficient approach for security assessment [5]. Thus, this paper focused on the design of a model that is quick and accurate which can predict the system severity for security evaluation, which is feasible for real time implementation in order to aid the operational engineers.

* Corresponding author.
E-mail addresses: pudisekhar@yahoo.com (P. Sekhar), sanjeeb.mohanty@nitrkl.ac.in (S. Mohanty).

http://dx.doi.org/10.1016/j.ijepes.2015.11.009
0142-0615/

INTERNATIONAL JOURNAL OF NUMERICAL MODELLING: ELECTRONIC NETWORKS, DEVICES AND FIELDS
Int. J. Numer. Model. 2015
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/jnm.2096

Classification and assessment of power system static security using decision tree and random forest classifiers

Pudi Sekhar*,† and Sanjeeb Mohanty

Department of Electrical Engineering, National Institute of Technology, Rourkela, India

SUMMARY

The power system static security classification and assessment is essential in order to identify the post-contingency problems and take corrective measures and to protect the system from blackout. In this paper, application of two data mining classifiers have been proposed for the security classification and assessment of a multiclass security problem. To design the security problem, contingency analysis is carried out under N-1 line outage, and static severity index (SSI) is computed, which is a function of the line overload and the voltage deviation using Newton–Raphson load flow method, considering the variable load and generating conditions. Corresponding to the computed values of SSI, the voltage, phase angle, Mega Volt Ampere line flow and so on, a 1×7 pattern vector is generated. The generated pattern vectors are used to design a multiclass security problem. The designed security pattern vectors are given as inputs to the decision tree (DT) and random forest (RF) model in order to classify the security status of the power system. The proposed classifiers are investigated on an IEEE 30-bus test system. The classification accuracy of the DT and the RF are compared with state-of-the-art classifier models, namely, multilayer perceptron (MLP), radial basis function (RBF), and support vector machine (SVM).The simulation results clearly indicate that the proposed DT and RF classifiers are more efficient, reliable, and out performs MLP, RBF, and SVM classifiers for the assessment of the security status of the power system. Hence, DT and RF classifiers are found to be suitable for online implementation.

Received 5 November 2014; Revised 29 June 2015; Accepted 31 July 2015

KEY WORDS: classifier; contingency analysis; static security; decision tree; random forest

NOMENCLATURE

S_{pq}	power flow in branch $p-q$ (MVA)
$S_{pq}^{\max}$	maximum power flow limit in branch $p-q$ (MVA)
$\left\|V_p^{\min}\right\|$	minimum voltage limit of the p^{th} bus
$\left\|V_p^{max}\right\|$	maximum voltage limit of the p^{th} bus
$\|V_p\|$	voltage magnitude of the p^{th} bus
N_l	number of transmission lines
N_b	number of buses
θ_b	voltage angle of the p^{th} bus
S_{Gp}	power generation of the p^{th} bus (MVA)
S_{Lp}	load of the p^{th} bus (MVA)
Φ_k	random vector of the k^{th} tree
T_r	training set
n_t	number of trees
T_r^*	data sample from the training set
C_k	vote of the k^{th} tree to a specific class

*Correspondence to: Pudi Sekhar, Department of Electrical Engineering, National Institute of Technology, Rourkela, India.
†E-mail: sekharresearchwork@gmail.com

Electrical Power and Energy Systems 75 (2016) 303–310

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

An enhanced cuckoo search algorithm based contingency constrained economic load dispatch for security enhancement

Pudi Sekhar *, Sanjeeb Mohanty

Dept. of Electrical Engineering, National Institute of Technology, Rourkela, India

ARTICLE INFO

Article history:
Received 25 May 2015
Received in revised form 15 September 2015
Accepted 19 September 2015

Keywords:
Contingency analysis
Enhanced cuckoo search
Overload alleviation
Power system control
Severity index

ABSTRACT

This paper propose a meta-heuristic algorithm known as the enhanced cuckoo search (ECS) algorithm for contingency constrained economic load dispatch (CCELD) in order to relieve transmission line overloading. The power system security assessment deals with finding out the secure and the insecure operating states, whereas the security enhancement deals with the necessary control action against overloads under contingency scenario. By generation rescheduling the overloaded lines can be relieved from the severity. In the proposed ECS algorithm, in order to improve the solution vectors, dynamically variable parameters namely the step size and the probability are incorporated instead of the fixed values of the parameters. The CCELD problem includes scheduling of generators to minimize the severity index with minimum fuel cost. A standard IEEE-30 bus system is considered to study the effectiveness of the proposed ECS algorithm for CCELD problem. Numerical results reveals that, for 100 iterations the proposed ECS algorithm out performs the other state-of-the-art algorithms, namely cuckoo search (CS), Bat algorithm (BA) and particle swarm optimization (PSO) algorithm in obtaining the minimum fuel cost and the minimum severity index in minimum time. Thus, the proposed ECS algorithm is found to be efficient to obtain the solution of contingency constrained economic load dispatch problem.

Introduction

The power system is a complex network, where there is a continuous increase in power demand. In this context, the power system operation has gained importance in security assessment and its control. The security assessment is the task of ascertaining whether the system operating under normal condition can withstand the contingencies (outage of transmission lines, generators, etc.) or not without violating the operating limits. If the current operating state is found insecure under contingency, then necessary control steps must be taken in order to avoid limit violation. In such a case, re-routing of power flows will relieve the transmission lines from overload. The authors in [1] have used the linearized relationship between power flows in the overloaded transmission lines and the generated power to reschedule the power generation. An efficient straight forward algorithm has been modeled in [2] for real time security control. In order to relieve the overload, the authors in [3] have proposed the concept of fuzzy-set-theory-based approach through active power generation rescheduling. Further, the classical optimization techniques have been developed to obtain the optimal power flow (OPF) problem, such as the gradient method [4], Newton method [5], decoupling technique [6] and the interior point method [7]. However, the gradient method has poor convergence characteristics, whereas the Newton method is bounded to continuity of the problem definition and constraints. The interior point method is time consuming and converges to local optima. Thus, the classical methods suffers from several drawbacks to obtain the OPF solution.

In view of the drawbacks of the classical methods, the research has focused on the application of evolutionary programming (EP) [8], genetic algorithm (GA) [9,10], particle swarm optimization (PSO) [11], differential evolution (DE) [12] and many other meta-heuristic algorithms to solve the OPF problem. From these literatures, it can be the observed that the heuristic search algorithms are well-suited to solve the OPF problem. However, research has also revealed the premature convergence of some of these algorithms, which reduces the performance of these algorithms. To improve the performance, modification of some parameters of these existing algorithms were implemented. However, several new heuristic search algorithms are developed to solve the drawbacks. Thus, the heuristic search algorithms are well-suited for solving the OPF problem and can also be extended for the application under contingency scenario for security enhancement.

* Corresponding author.
E-mail addresses: pudisekhar@yahoo.com (P. Sekhar), sanjeeb.mohanty@nitrkl.ac.in (S. Mohanty).

http://dx.doi.org/10.1016/j.ijepes.2015.09.018
0142-0615/

Vitae

Name	:	Pudi Sekhar
Date of Birth	:	30th June 1986
Permanent Address	:	D. No. 30-55-8, Appikonda R. H. C, Vadlapudi Post, Visakhapatnam (District), Andhra Pradesh - 530046, India.
E-mail	:	pudisekhar1@gmail.com

Academic Qualifications:

- Pursuing **Ph. D** in Electrical Engineering, National Institute of Technology, Rourkela.
- **M.Tech** in Power systems and Automation, GITAM University, Visakhapatnam.
- **B.Tech** in Electrical and Electronics Engineering (EEE) from A.I.E.T. Vizianagaram, JNTUK, Andhra Pradesh.