ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

DYNAMIC SECURITY ENHANCEMENT OF POWER SYSTEMS VIA POPULATION BASED OPTIMIZATION METHODS INTEGRATED WITH ARTIFICIAL NEURAL NETWORKS

Ph.D. THESIS

Cavit Fatih KÜÇÜKTEZCAN

Department of Electrical Engineering

Electrical Engineering Programme

MARCH 2015

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

DYNAMIC SECURITY ENHANCEMENT OF POWER SYSTEMS VIA POPULATION BASED OPTIMIZATION METHODS INTEGRATED WITH ARTIFICIAL NEURAL NETWORKS

Ph.D. THESIS

Cavit Fatih KÜÇÜKTEZCAN
(504072003)

Department of Electrical Engineering

Electrical Engineering Programme

Thesis Advisor: Assoc. Prof. Dr. İstemihan GENÇ

MARCH 2015

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

YAPAY SİNİR AĞLARININ ENTEGRE EDİLDİĞİ POPÜLASYON TABANLI OPTİMİZASYON YÖNTEMLERİYLE GÜÇ SİSTEMLERİNİN DİNAMİK GÜVENLİĞİNİN İYİLEŞTİRİLMESİ

DOKTORA TEZİ

Cavit Fatih KÜÇÜKTEZCAN
(504072003)

Elektrik Mühendisliği Anabilim Dalı

Elektrik Mühendisliği Programı

Tez Danışmanı: Doç. Dr. İstemihan GENÇ

MART 2015

Cavit Fatih Küçüktezcan, a **Ph.D.** student of ITU **Graduate School of Engineering and Technology** student ID **504072003**, successfully defended the **dissertation** entitled "**DYNAMIC SECURITY ENHANCEMENT OF POWER SYSTEMS VIA POPULATION BASED OPTIMIZATION METHODS INTEGRATED WITH ARTIFICIAL NEURAL NETWORKS**", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Assoc. Prof. Dr. İstemihan GENÇ** İstanbul Technical University	....
Jury Members :	**Prof. Dr. Mustafa BAĞRIYANIK** İstanbul Technical University	....
	Prof. Dr. Tülay YILDIRIM Yıldız Technical University	....
	Prof. Dr. Belgin EMRE TÜRKAY İstanbul Technical University	....
	Assoc. Prof. Dr. Ayşen BASA ARSOY Kocaeli University	....

Date of Submission : 25 January 2015
Date of Defense : 23 March 2015

To my mother and father,

FOREWORD

This doctoral thesis is the result of my research studies completed at Istanbul Technical University, Department of Electrical Engineering. During my studies, considerable number of valuable people has contributed to this doctoral thesis.

First of all, I would like to express my gratitude to my supervisor Assoc. Prof. Dr. İstemihan Genç, for giving me a chance to work with him in this challenging research area. I have benefited from his deep knowledge and valuable recommendations in each step of this study. I will never forget our discussions and effort to bring novelty and contribute to my research area. Experiences I have earned from our collaboration during the past few years will be very helpful for my future studies.

My gratitude is extended to Prof. Dr. Mustafa Bağrıyanık and Prof. Dr. Tülay Yıldırım for their valuable suggestions and comments that have helped me to develop this study.

In addition, I also want to thank Prof. Dr. Istvan Erlich who gave me an opportunity to study in his institute at the University of Duisburg-Essen.

Moreover, I thank a great leader and founder of the Turkish Republic, Mustafa Kemal Atatürk. Without his vision, reforms and modernization efforts, my beautiful country would have never been as it is today.

I also want to thank my lovely İpek, Demircan family and my real friends who always encourage and support me even in my worst days.

At last, I would like to dedicate this thesis to my beloved parents, my lovely mother Saadet Küçüktezcan and my lovely father Cengiz Küçüktezcan. Their labor on me cannot be defined by words. They deserve my biggest gratitude. I love you all.

This thesis is supported by The Scientific and Technical Research Council of Turkey (TUBITAK) project no. 114E157.

March 2015 Cavit Fatih KÜÇÜKTEZCAN

TABLE OF CONTENTS

Page

ABBREVIATIONS

ABC	: Artificial Bee Colony
ANFIS	: Adaptive Neuro-Fuzzy Inference Systems
ANN	: Artificial Neural Network
ASM	: Active Set Method
BB-BC	: Big Bang-Big Crunch
BP	: Back Propagation
CCT	: Critical Clearing Time
CT	: Clearing Time
DE	: Differential Evolution
DSA	: Dynamic Security Assessment
DSE	: Dynamic Security Enhancement
DT	: Decision Trees
GA	: Genetic Algorithm
KB	: Knowledge Base
LS	: Learning Set
MAE	: Mean Absolute Error
MDR	: Minimum Damping Ratio
MF	: Membership Function
MLP	: Multi-Layer Perceptron
MVMO	: Mean Variance Mapping Optimization
OP	: Operating Point
PNN	: Probabilistic Neural Network
PSO	: Particle Swarm Optimization
TS	: Training Set

LIST OF TABLES

Page

LIST OF FIGURES

Page

DYNAMIC SECURITY ENHANCEMENT OF POWER SYSTEMS VIA POPULATION BASED OPTIMIZATION METHODS INTEGRATED WITH ARTIFICIAL NEURAL NETWORKS

SUMMARY

Increasing consumption of electricity, penetration of renewable energy sources into electric power systems, uncertainties caused by the nature of these sources, enforcements of economics and energy markets, bring various and unplanned power flow patterns, which represents different and more stressed conditions than planned operating conditions of power systems. These new power flow patterns and their increasing diversity should be redesigned, to satisfy an acceptable security level for power systems. When a power system is operated under stressed conditions that are close to security limits, the system can be vulnerable from disturbances (contingencies), which can cause loss of synchronism and cascading blackouts. Therefore, online monitoring of dynamic security of the system becomes an important task for detecting an insecure current operating condition and applying proper control actions to regain the ability of the system to withstand contingencies such as faults, or sudden loss of any system component.

Electric power is extremely important for economy and daily life. Safe and sustainable operation of power systems requires fast and accurate dynamic security assessment methods. Accurate methods with mathematical background exist for determining angular instability in power systems. Time-domain-simulation is the most straightforward method that directly shows the behavior of the system dynamics in time domain. However, dynamic model of power system involves linear and nonlinear equations that include large number of continuous and discrete state variables. When time domain simulations are applied for the stability analysis, the calculations required for recursively solving nonlinear differential equations of the system model over thousands of time steps, require significant time for the occurrence of one critical contingency. This drawback reduces the practicability of using time domain simulations. Although, direct methods based on energy function assess the stability of the system without solving differential equations, they involve modeling limitations for large-scale power systems, which make them impractical. Probabilistic methods are considered as a suitable method for system planning due to their detailed considerations and computation requirements.

Measurable features of power systems can be associated with the stability of the system through machine learning methods. This study suggests using data collected from different buses of the system and processing these measurements by designed fast and accurate artificial neural networks to assess the dynamic security of the current operating point of the system. Several, recent studies suggest using machine learning methods for dynamic security assessment. Nevertheless, it is still a challenging task for large sized power systems. Large sized systems involve large number of critical contingency, which increase the computational complexity. In

addition, large set of various system topologies and wide range of loading conditions should be taken into account by the designed security assessment tool.

After the detection of insecure current operating point, system operator should apply control actions to move the system to a secure operating point, where the system can withstand contingencies. Objective of security enhancement is preventing the system from undesired situations, and avoiding large blackouts. Generally, security enhancement is categorized into two sub-categories such as preventive control and corrective control.

The objective of preventive control is successfully preventing the power system from losing its stability against uncertain disturbances (contingencies). In this thesis, applications of generation rescheduling and load curtailment preventive control actions for enhancing the dynamic security of the power system are studied. Generation rescheduling is a useful preventive control action to restore and enhance the system security by shifting the generation among controllable generators. System operator can monitor the generation and demand of electric power. When an insecure operating point is detected, the system operator can request from available loads to curtail their electric power demand. This load curtailment action can collaborate with generation rescheduling and a proper adjustment of these preventive control actions can change the power flow patterns within the network. Then, power system can move to a secure operating point so that the stability of the system is preserved despite of the occurrence of a critical contingency.

If preventive control actions cannot move the system to a secure point for any critical contingency, or the cost of preventive control is considered as high, power system can be armed by corrective control actions, which are ready to be applied in case of occurrence of any contingency. In this thesis, load shedding method is studied as a corrective control action to regain the stability of the system if preventive control action cannot be applied and protect the system against critical contingencies. Although both load shedding and load curtailment methods decrease the electrical power consumption in the related load buses, they are different methods by means of their application schedules, magnitudes and costs. As different from load curtailment method, load shedding is a fast switching operation that applied after the occurrence of contingency, and the amount of load to be shed is relatively larger than curtailment, since the maximum amount of load to be curtailed is based on the amount of available loads in the selected load buses.

Dynamic security assessment and enhancement is under the responsibility of system operator. The complexity of the large sized power systems does not let the system operators to determine a proper control action, immediately. In addition, deregulation of power systems, integrates many participants into the market, and control actions designed for security enhancement, are generally contrary to the market-based strategies of participants. In other words, enhancing the system security brings a cost. Although, system operator may find a proper control action to enhance the system security, generally, the operator may not determine a cost effective control action, immediately. To overcome that problem, dynamic security enhancement can be considered as a constrained optimization problem to minimize the costs of required control actions.

Due to the size of the real power systems, mentioned optimization problem involves multi-dimensional search space with many continuous and discrete control variables, many local optimum solutions and large number of equality and inequality constraints. In addition, constraints related with dynamic security of the system are highly nonlinear and too complex to be defined mathematically. Therefore, conventional optimization methods may not converge to a satisfactory solution for dynamic security enhancement. This study suggests using evolutionary algorithms to solve mentioned optimization problem. In addition, previously suggested artificial neural networks based dynamic security assessment methodology is integrated into the optimization process for estimating the violations of security based system constraints for candidate solutions. This integration can enable optimization methods to find a proper and cost effective solution for control actions within an acceptable time. Since the mentioned optimization problem involves too many constraints due to the size of the power systems, optimization methods should use constraint-handling methods. This study suggests applying an adaptive penalization technique to infeasible candidate solutions during the optimization. Adaptive penalization reduces the parameter adjustment process of static penalty function, which requires considerable effort and significantly affects the result of optimization.

The main objective of this study is to research the applications of heuristic, population based optimization methods and their collaboration with artificial neural networks to develop a fast and powerful methodology to assess and enhance dynamic security of power systems.

Different artificial neural networks are designed for dynamic security assessment, which are considered as both regression and classification problems. In regression approach, designed multi-layer perceptron neural networks estimates defined security indexes such as critical clearing time and minimum oscillatory damping value for each operating point. In classification approach, designed probabilistic neural network classify operating points as secure or insecure.

Proposed artificial neural networks are designed to capture various topological changes in the system according to *N-1* criterion and different loading conditions. For monitoring of a power system where all system parameters continuously change, ability of capturing topological and loading level changes is mandatory. In addition, artificial neural networks with that ability can directly be used during the optimization to enhance the security of insecure initial operating point with any topology and loading condition.

Designed artificial neural networks process the data collected from different buses of the system. To increase the accuracy of the artificial neural networks, feature selection process is applied to all measurements. In addition, the feature set is enriched with an additional index that involves relevant information about the stability of the system such as inertia constants of synchronous generators, which cannot be obtained from measurements.

The proposed methodology for dynamic security enhancement involves both preventive and corrective control strategies with mixture of various control actions such as generation rescheduling, load curtailment and load shedding. For the designed control strategies, various optimization methods such as genetic algorithms, differential evolution, particle swarm optimization, artificial bee colony, big bang-big crunch and mean variance mapping optimization are used.

This study proposes artificial neural networks based dynamic security assessment methodology to estimate the security based constraint violations of candidate solution during the optimization of control actions. This will speed up the optimization, reduce the required time to find a cost-effective control action for enhancing the security of the system to an acceptable security level and increase the online applicability of proposed methodology. During the latter iterations of optimization, search methods tend to converge to an operating point near security boundary. To prevent the misdetection of an insecure operating point, artificial neural networks based dynamic security assessment tools are trained by using the training data that is enriched around the security boundary.

Proposed dynamic security assessment and enhancement methods are demonstrated on the 16-generator, 68-bus system, 17-generator, 163-bus Iowa system and on the IEEE 50-generator, 145-bus system. The results of the studies are represented in Sections 4,5 and 6.

YAPAY SİNİR AĞLARININ ENTEGRE EDİLDİĞİ POPÜLASYON TABANLI OPTİMİZASYON YÖNTEMLERİYLE GÜÇ SİSTEMLERİNİN DİNAMİK GÜVENLİĞİNİN İYİLEŞTİRİLMESİ

ÖZET

Elektrik enerjisi tüketimindeki artışa rağmen, güç sistemlerinin coğrafi sebeplerle aynı oranda genişleyememesi, sisteme entegre edilen ve üretim oranı gün geçtikçe artan yenilenebilir enerji kaynaklarının doğası gereği sahip olduğu belirsizlikler, enerji piyasasının ve ekonomiklik kriterlerinin getirdiği kısıtlamalar sebebiyle, günümüz elektrik güç sistemleri tasarım ve planlama aşamasında öngörülen güç akışı senaryolarından farklı ve stres edilmiş birçok yeni noktada çalışmaktadır. Bu yeni çalışma noktalarının, sistemin kabul edilebilir güvenlik sınırlarını ihlal etmeyecek şekilde yeniden planlanması gerekmektedir. Elektrik güç sistemi, güvenlik sınırlarına yakın, stress edilmiş bir çalışma noktasında iken, senkron generatörlerin senkronizma kaybına sebep olabilecek ve sistemin büyük bir bölümünü devre dışı bırakabilecek bazı bozucu etkilere karşı sistem savunmasız durumda olabilir. Bu sebeple, sistemin dinamik güvenliğinin takibi ve güvensiz bir çalışma noktasının tespiti anında doğru kontrol yöntemleri uygulanarak, sistemin bozucu etkilerle başedebileceği güvenli bir çalışma noktasına hızlı bir şekilde getirilmesi, günümüz güç sistemleri için oldukça önemlidir.

Elektrik enerjisi, günlük yaşam ve ülke ekonomisi için hayati öneme sahiptir. Elektrik güç sistemlerinin sürekli ve güvenli çalışması, dinamik güvenlik analizinin hızlı ve doğru olarak yapılabilmesini gerektirir. Matematiksel altyapıya sahip yöntemler, bu tez çalışmasında ele alınan kararlılık sınıfı olan açısal kararlılığın belirlenmesinde, kesin ve doğru sonuçlar vermektedir. Zaman domeni simülasyonları, bir bozucuya maruz kalmış sistemin dinamik davranışını en açık şekilde gösteren yöntemdir. Güç sistemlerinin dinamik modelleri, oldukça fazla sayıda sürekli ve süreksiz değişken içeren, doğrusal ve doğrusal olmayan birçok cebirsel ve diferansiyel eşitlikten oluşur. Zaman domeni simülasyonlarının en büyük dezavantajı, oldukça fazla sayıdaki diferansiyel denklemlerin, binlerce zaman adımında çözülmesi için ihtiyaç duyulan işlem gücü ve zamandır. Bu işlemin, güç sisteminin boyutuna bağlı olarak artan bozucu etkiler için ayrı ayrı tekrarlanacak olması da, zaman domeni simülasyonlarının uygulanabilirliğini güçleştirmektedir. Bu yöntemden farklı olarak, diferansiyel denklem takımlarının çözüme ihtiyaç duymayan, enerji fonksiyonlarına dayalı direkt yöntemler ve sistem kararlılığını bir olasılık değerine bağlı olarak tanımlayan olasılıksal yöntemler de, modelleme kısıtlamaları ve işlem yükleri sebebiyle büyük güç sistemlerinin genellikle planlama aşamasında tercih edilirler.

Güç sistemindeki bara gerilimlerinin genlikleri, açıları, hatlar üzerinden iletilen aktif ve reaktif güç miktarları gibi değerler ile sistemin açısal kararlılığı, makina öğrenmesi tabanlı yöntemler ile ilişkilendirebilir. Son yıllarda bu doğrultuda yapılan araştırmalar mevcuttur. Büyük boyutlu güç sistemlerinde meydana gelebilecek

önemli bozucu etkilerin sayısı, arıza veya bakım gibi nedenlerle sistemin çalışabileceği farklı topolojilerin sayısı, sistemdeki tüketicilerin farklı tüketim karakteristiklerinden kaynaklanan geniş aralıktaki yüklenme durumları, sistemin çok çeşitli çalışma noktalarında çalışmasına sebep olur. Güç sistemlerinin bu geniş yelpazedeki çalışma koşulları dikkate alındığında, makina öğrenmesi tabanlı yöntemlerin, güç sisteminin güvenlik ve kararlılık analizi amacıyla kullanılması halen ilgi çekici ve zorlu bir konudur. Tasarlanan yöntemin güç sistemlerine ilişkin çok farklı çalışma noktalarında da kesin sonuçlar vermesi gerekmektedir. Bu tez çalışmasının bir bölümünde, makina öğrenmesi tabanlı yöntemlerden olan çeşitli yapay sinir ağları yöntemleri kullanılarak, güç sisteminin açısal kararlılığı, bahsi geçen farklı çalışma koşullarında dahi hızlı ve kesin bir şekilde belirlenmeye çalışılmıştır.

Güç sistemi operatörleri, sistemin güvensiz bir çalışma noktasında bulunduğunu tespit ettikten sonra, sistemi güvenli bir çalışma noktasına getirmekle yükümlüdürler. Sistemin dinamik güvenliğini iyileştirmenin amacı, istenmeyen bozucuların etkilerinden sistemi korumaktır. Genellikle, sistem güvenliğinin iyileştirilmesi, önleyici ve düzeltici kontrol uygulamaları ile gerçekleştirilir.

Önleyici kontrol uygulamaları, sistem istenmeyen bir bozucuya maruz kalmadan uygulanarak, sistemin kararlılığını kaybetmesine engel olan uygulamalardır. Bu çalışmada, üretimin yeniden düzenlenmesi ve yük kısıtlaması yöntemlerine dayalı bir önleyici kontrol uygulaması ile güç sisteminin dinamik güvenliği iyileştirilmeye çalışılmıştır. Üretimin yeniden düzenlenmesi, kontrol edilebilen generatörlerin sisteme enjekte ettiği elektriksel gücün, belirli kısıtlar altında yeniden düzenlenmesine dayanır. Sistem operatörü, bazı generatörlerin üretim değerlerini önleyici kontrol amacıyla yeniden düzenleyebildiği gibi, sistemdeki bazı yüklerin de tüketim değerleri için, yine belirli sınırlar içerisinde bir düzenleme yapabilir. Böylece, sistem operatörü önemli bozucu etkilerin meydana geldiği bölgeleri de düşünerek, önemli iletim hatları üzerindeki güç akışını belli oranda değiştirebilir ve olası bozucuların etkilerine karşı sistemi koruyabilir.

Bazı durumlarda, önleyici kontrol uygulamalarıyla sistemi güvenli bir çalışma noktasına taşımak mümkün olmayabilir. Bu gibi durumlarda güç sistemleri, her bir bozucu için önceden belirlenmiş düzeltici kontrol uygulamalarıyla donatılmış halde çalışmaya devam edebilir. İstenmeyen bir bozucu olay meydana geldikten çok kısa bir süre sonra, bu bozucu olay için önceden planlanmış düzeltici kontrol uygulaması devreye girerek sistem kararlılığı korunmuş olur. Bu çalışmada, yük atımı düzeltici kontrol uygulamasıyla, güç sisteminin olası bozuculara maruz kaldıktan sonra kararlılığını koruyabilmesi sağlanmıştır.

Güç sisteminin dinamik güvenliğinin analizi ve iyileştirilmesi, güç sistemi operatörünün sorumluluğundadır. Günümüzde, bir çok ülkenin ulusal güç sistemininin üretim, iletim ve dağıtım hizmetlerini hem devlete bağlı kurumlar, hem de özel şirketler sağlamaktadır. Güvenlik iyileştirici kontrol uygulamaları genellikle, enerji piyasasındaki bu kurumların bir kısmının stratejileri ile zıt yönde olabilir. Başka bir deyişle, sistemi güvenli bir çalışma noktasına taşımanın, sistem operatörüne bir maaliyeti olacaktır. Günümüz büyük boyutlu güç sistemlerinin karmaşık yapısı, sistemi kabul edilebilir bir maaliyetle güvenli bir çalışma noktasına götürecek bir çözümü kısa sürede hesaplama imkanını sistem operatörlerine tanımayabilir. Bu çalışmada, dinamik güvenlik iyileştirmesi problemi, kontrol uygulamalarının maaliyetini eniyilemeyi amaçlayan, çok kısıtlı bir optimizasyon problemi olarak tanımlanmıştır.

Gerçek güç sistemlerinin boyutları sebebiyle, bahsi geçen optimizasyon problemi, sürekli ve ayrık parametrelerden oluşan, çok boyutlu bir arama uzayına sahip, yerel en iyi çözümlerin bulunduğu, çok sayıda eşitlik ve eşitsizlik kısıtlamalarına sahip bir problemdir. Ayrıca, dinamik güvenliğe ilişkin, doğrusal olmayan kısıtlar, matematiksel olarak kolayca ifade edilmek için fazla karmaşıktır. Bu sebeplerden ötürü, geleneksel optimizasyon yöntemleri, her başlangıç noktası için, dinamik güvenliği iyileştirici ve düşük maaliyetli bir sonuca yakınsayamayabilir. Bu çalışmada, bahsi geçen optimizasyon probleminin çözümü için evrimsel algoritmaların kullanımı önerilmiştir. Ayrıca, optimizasyon sırasında üretilen aday çözümlerin dinamik güvenlik kısıtlarını ihlal edip etmediğini tespit etmek amacıyla, yapay sinir ağları tabanlı araçlar optimizasyon yöntemine entegre edilerek, optimizasyon süreci hızlandırılmıştır. Güç sisteminin boyutlarına bağlı olarak, problemin içerdiği yüksek miktardaki kısıtlar sebebiyle, bu çalışmada adaptif cezalandırmaya dayalı kısıt ele alma yöntemi kullanılmıştır. Bu yöntem, optimizasyon esnasında kısıtları ihlal eden çözümlere uygulayacağı ceza fonksiyonunu, diğer çözümlerin kısıt ihlallerine bağlı olarak tayin ederek, optimizasyon yönteminin kısa sürede, kısıtları ihlal etmeyen çözüm uzayına ulaşmasını amaçlamaktadır.

Bu çalışmanın ana amacı, populasyon tabanlı, sezgisel optimizasyon yöntemleri ve yapay sinir ağlarının beraber kullanımına dayalı, hızlı ve güçlü bir dinamik güvenlik değerlendirmesi ve iyileştirmesi yöntemi oluşturmaktır. Dinamik güvenlik değerlendirmesi, birer regresyon ve sınıflandırma problemi olarak ayrı ayrı ele alınmıştır. Regresyon probleminde, tasarlanan çok tabanlı algılayıcı yapay sinir ağı, tanımlı kararlılık endekslerini tahmin ederek sistem güvenliğini belirler. Her bir bozucuya (3 faz-toprak kısa devre) ilişkin geçici hal kararlılığı için endeks değeri, bozucuyu temizleyen kesicilere ait kritik açma zamanıdır. Küçük işaret kararlılığı için endeks değeri ise, kritik moda ilişkin minimum salınım değeri olarak tanımlanmıştır. Sınıflandırma probleminde ise, olasılıksal yapay sinir ağları ile her bir çalışma noktası güvenli ve güvensiz olarak sınıflandırılmaya çalışılmıştır.

Çalışmada, yapay sinir ağları, sistem topolojisindeki değişimleri (N-1 kriterine göre) ve farklı yüklenme durumlarını algılayabilecek şekilde tasarlanmıştır. Tasarlanan yapay sinir ağlarının performanslarını artırmak amacıyla, güç sisteminden toplanan ölçümler, öznitelik seçim yöntemleri ile işlenmiştir. Kararlılık indeksleriyle bağlantılı olan değerler, yapay sinir ağlarının eğitimi ve uygulamasında kullanılmıştır. Çalışmada ayrıca, sistemden toplanan ölçümlerde bulunmayan ancak sistemin açısal kararlılığı ile yakında ilişkili olan, generatörlerin atalet sabitlerini içeren bir değişken tanımlanmış ve bu değişkenin önemi, öznitelik seçimi sonuçlarıyla incelenmiştir.

Dinamik güvenliği iyileştirmek için önerilen önleyici ve düzeltici kontrol uygulamalarını içeren metodoloji, üretimin yeniden düzenlenmesi, yük kısıtlaması ve yük atımı yöntemlerinin koordineli bir şekilde uygulanmasını sağlamaktadır. Tasarlanan kontrol uygulamalarının optimizasyonunda, genetik algoritmalar (GA), diferansiyel evrim (DE), parçaçık sürü optimizasyonu (PSO), yapay arı kolonisi (ABC), büyük patlama-büyük çöküş (BB-BC) optimizasyonu, ortalama varyans eşleme optimizasyonu (MVMO) gibi popülasyon tabanlı yöntemler kullanılmıştır.

Optimizasyon sırasında üretilen çözümlerin dinamik güvenlik kısıtlarına ilişkin ihlalleri, hesap yükü fazla olan zaman domen simulasyonları yerine, yapay sinir ağları ile elde edilmiştir. Böylece, güç sistemini kabul edilebilir bir maaliyetle güvenli bir çalışma noktasına taşıyacak kontrol uygulaması parametrelerini bulması için, optimizasyon yönteminin ihtiyaç duyacağı süreyi azaltarak, tüm metodolojinin uygulanabilirliği artırılmaya çalışılmıştır. Dinamik güvenlik değerlendirmesi ve iyileştirmesi amacıyla önerilen yöntemler, 16-generatör, 68-bara güç sistemi, 17-generatör, 173-bara Iowa güç sistemi ve 50-generatör, 145-bara IEEE güç sistemi modellerine uygulanmış ve elde edilen sonuçlar 4, 5 ve 6. bölümlerde açıklanmıştır.

1. INTRODUCTION

1.1 Motivation

Increasing consumption of electricity, penetration of renewable energy sources into power systems, uncertainties caused by the nature of these sources, enforcements of economics and energy markets, bring various and unplanned power flow patterns, which represents different and more stressed conditions than planned operating conditions of power systems [1]. These new power flow patterns and their increasing diversity should be redesigned, to satisfy an acceptable security level for power system. When a power system is operated under stressed conditions that are close to security limits, the system may be vulnerable to disturbances (contingencies), which can cause loss of synchronism and cascading blackouts [2]. Monitoring of dynamic security of the system becomes an important task for detecting an insecure current operating condition and applying proper control actions to regain the ability of the system to withstand contingencies such as faults, or sudden loss of any system component.

Electric power is extremely important for economy and daily life. Safe and sustainable operation of power systems requires fast and accurate dynamic security assessment (DSA) methods. Accurate methods with mathematical background exist for determining angular instability in power systems, which is the main stability concern in this study. Time-domain-simulation (TDS) is the most straightforward method that directly shows the behavior of the system dynamics in time domain, but this method requires intensive computation effort, which reduces the practicability. Although, direct methods based on energy function assess the stability of the system without solving differential equations, they involve modeling limitations for large-scale power systems which make them impractical [3]. Probabilistic methods are considered as suitable for system planning due to their detailed considerations and computation requirements [4]. This study suggests using measurement collected from different parts of the system and processing them by fast and accurate Artificial

Neural Networks (ANNs) to assess the dynamic security of the current operating point (OP) of the system. Several, recent studies suggest using computational intelligence methods for online DSA [5-11]. Nevertheless, it is still a challenging task for large sized power systems. Large sized systems involve a large number of critical contingencies, which increase the computational complexity. On the other hand, large set of various system topologies and wide range of loading conditions should be taken into account by the designed security assessment tool. In addition, considering mentioned variety of contingencies, topologies and loading conditions may requires significant number of features. Designed DSA tool should give satisfactory results by using available features.

After the detection of insecure current OP, system operator should apply control actions to move the system to a secure OP, where the system can withstand contingencies. DSA and dynamic security enhancement (DSE) is under the responsibility of system operator. The complexity of the large sized power systems does not let system operators to decide a proper control action immediately. In addition, deregulation of power system integrates many participants into the market, and control actions designed for security enhancement are generally contrary to the market-based strategies of participants. Therefore, enhancing the system security brings a cost. Although, system operator may find a proper control action to enhance the system security, generally, the operator may not determine a cost effective control action, immediately. Therefore, DSE can be considered as a constrained optimization problem to minimize the costs of applied control actions.

Due to the size of the real power systems, mentioned optimization problem involves multi-dimensional search space with many continuous and discrete control variables, many local optimum solutions and large number of equality and inequality constraints. In addition, some constraints related with dynamic security of the system are highly nonlinear and too complex to be defined mathematically. Conventional optimization methods may not converge to a satisfactory solution for DSE. This study suggests using evolutionary algorithms (EAs) to solve mentioned real time optimization problem. In addition, previously suggested ANN based DSA methodology is integrated into the optimization process for estimating the security based system constraints for candidate solutions. This integration can enable optimization methods to find a proper and cost effective solution for control actions within an acceptable time [12]. Since the mentioned optimization problem involves too many constraints due to the size of the power systems, optimization methods should use constraint handling methods. This study suggests applying adaptive penalization technique to infeasible candidate solution during the optimization. Adaptive penalization reduces the parameter adjustment process of static penalty function, which requires considerable effort and dramatically affects the result of optimization [13].

1.2 Objectives and Contributions

According to the motivation mentioned above, the main objective of this study is to research the applications of heuristic optimization methods and their collaboration with artificial neural networks to develop a fast and powerful methodology to assess and enhance dynamic security of power systems. Specific objectives and contributions are briefly explained below:

- *Dynamic security assessment:* Different ANNs are designed for DSA tasks, which are considered as both regression and classification problems. In regression approach, designed multi-layer perceptron neural networks [14] estimates defined security indexes such as critical clearing time and minimum oscillatory damping value for each OP. In classification approach, designed probabilistic neural networks [15] classify OPs as secure or insecure.

- *Considering changes in system topology and loading condition:* Proposed ANNs are designed to capture various topological changes in the system according to *N-1* criterion and different loading conditions. For online monitoring of a power system where all system parameters continuously change, ability of capturing topological and loading level changes is mandatory. In addition, ANNs with that ability can directly be used during the optimization to enhance the security of insecure initial OP with any topology and loading condition.

- *Requirement of important features for DSA:* Designed ANNs process the data collected from different buses of the system. ANNs should use the available data and make accurate estimation for DSA. To increase the accuracy of the ANNs, feature selection process is applied to large sized data. In addition, study proposes an additional indices that involves relevant information about the stability of the system, which cannot be obtained from measurements.

- *Optimization of control actions for DSE via heuristic optimization methods:* The proposed methodology for DSE involves both preventive and corrective control strategies with mixture of various control actions such as generation rescheduling, load curtailment and load shedding. For the designed control strategies, various optimization methods such as Genetic Algorithms (GAs) [14], Differential Evolution (DE) [15], Particle Swarm Optimization (PSO) [16], Artificial Bee Colony (ABC) [17], Big Bang-Big Crunch (BB-BC) [18] and Mean Variance Mapping Optimization (MVMO) [19] are used. With this study, ABC, BB-BC, MVMO are used for the first time to solve mentioned optimization problem.

- *Improving the optimization of control actions:* This study uses the same ANN based DSA methodology to estimate the security based constraint violations of candidate solution during the optimization of control actions. This will speed up the optimization, reduce the required time to find a cost-effective control action for enhancing the security of the system to an acceptable level and increase the online applicability of proposed methodology. During the latter iterations of optimization, search methods tend to converge to an OP near security boundary. To prevent the misdetection of an insecure OP, ANN based DSA tools are trained by training data that is enriched around the security boundary.

1.3 Organization

Section 2 introduces the concept of power system stability and security. Definitions of these terms and a general classification of power system stability are given. Additionally, factors that may cause different types of instabilities, methods for analyzing the stability and security of power systems and possible control strategies to enhance the system security are briefly explained in this section.

Section 3 represents various ANN structures and population based heuristic optimization methods, which are used for DSA and DSE tasks in this study, respectively. In addition, penalization based adaptive constraint handling technique which is used for feasible solutions during the optimization is explained in this section.

During the doctoral studies, methodologies proposed for DSA and DSE have been enhanced, updated and applied to various test systems. To make this thesis more understandable, Section 4 and 5 introduce the final methodology proposed for DSA and DSE respectively. In Section 4, the design of ANN based DSA framework is explained. The methodology involves selection of critical contingencies, creation of knowledge base by considering different contingencies, system topologies and loading levels, feature selection process, determining best ANN structures and training process of ANN. Finally, the performances of designed ANNs on DSA are presented.

Section 5 introduces a preventive control strategy that combines both generation rescheduling and load curtailment approaches. In addition, the optimization problem related with the mentioned preventive control strategy is introduced by the means of control variables, objective function, constraints and penalty functions. In the end of Section 5, detailed results for the application of various population based optimization methods to solve the defined optimization problem is given.

Section 6 represents the previous methodologies proposed to assess and enhance the dynamic security of power systems. Although, there are similarities between final methodology and previous ones, there are also noticeable differences. In this section, classification based DSA is considered. Design and enhancement processes of employed PNN structure for DSA of various power systems are explained. In addition to preventive control, load shedding is introduced as a corrective control strategy in this section. Optimization procedure for control actions with various objective functions is explained. This section also introduce time domain simulation based DSA which is also used for the optimization of both preventive and corrective control actions solved by various population based optimization methods and also one conventional optimization method. Section 6 ends with the investigation of proposed optimizaiton methods’s robustness to the uncertainties in the loading conditions. Finally, Section 7 concludes the thesis with discussion of obtained results and possible future research directions.

2. DYNAMIC SECURITY OF THE POWER SYSTEM

2.1 Power System Stability and Security

Power system stability and security are the most frequently used terms in this study. Therefore, exact definitions of these terms, conceptual relationship between them and their essential differences should be explained.

CIGRE Study Committee 38 and the IEEE Power System Dynamic Performance Committee, define the power system stability, as "the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact" [22].

Same committees define power system security as the ability of the power system to withstand sudden disturbances (contingencies) [22]. Alternative definition for power system security is "satisfying a set of inequality constraints over a subset of the possible disturbances called the next contingency set [23]. The disturbances mentioned here could be short circuits, load changes or unexpected loss of any power system components.

As seen from the definitions, power system stability refers to the persistence of unharmed operation of the system after subjected to a contingency (disturbance). Stability depends on the condition of initial operating point (OP) and the severity of the contingency. On the other hand, power system security refers to the risk level in systems capability to stand against credible disturbances without any failure on user service. Security term relates to robustness of the system against credible disturbances, it also depends on the condition of initial OP and the severity of the contingency, as power system stability.

Security of the system is different from stability from the point of consequence of instability. Let's assume that two OPs of a power system are both stable and their stability margins are also equal, but the first point can be more secure than the second point because the consequences of instability for the second point can be more critical [24].

Although power system stability is a single problem, it is complex and multi-dimensional problem. Therefore, different forms of instabilities related with power systems may not be fully understood and analyzed without simplifying and specifying the problem. Stability analysis which involves identifying the main parameters causes instability and contriving techniques to improve the stability, is eased by classification of power system stability into specific types [24]. Figure 2.1 identifies the categories and subcategories of power system stability problem.

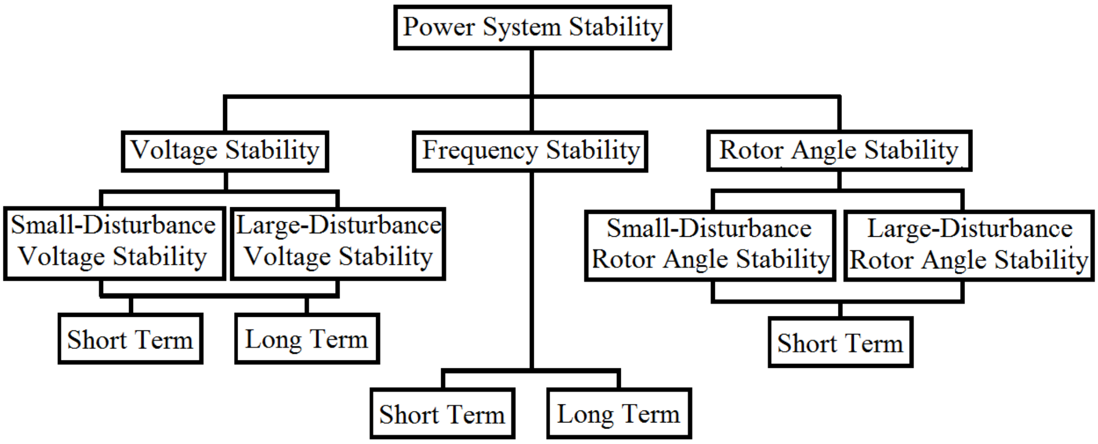


Figure 2.1 : Classification of power system stability [24].

As seen from Figure 2.1, power system stability is classified into their subcategories such that rotor angle stability, frequency stability and voltage stability.

Voltage stability can be described as the system's ability to resume steady state values of all bus voltages between an acceptable bandwidth after the occurrence of any disturbance. Voltage stability problem can be caused by large or small disturbances, and they are called large disturbance voltage stability and small disturbance voltage stability, respectively [22].

Voltage stability phenomenon can also be short term or long term. Fast acting devices such as, induction machines, power electronic devices, HVDC etc. can causes voltage fluctuations as short-term phenomenon in the range between 10 and 20 seconds. Overloading of transmission lines, operation of generators near the limits of reactive power generation, slow changing loads etc. cause long term voltage instabilities which are investigated between one and several minutes. Unlike angle stability, voltage stability is related with the balance on the generation and consumption of the reactive power, since angle stability is generally related with the balance of active power [25].

Frequency stability is the ability of the system to continue steady frequency after the occurrence of a large disturbance between electric power consumption and generation [22]. It is based on the system's ability to restore a balance between consumption and generation with minimum interruption of load. Frequency instability can causes continuous frequency fluctuations that lead to disconnection loads or generation units from the system.

Large disturbances cause large deviations of frequency, voltage, power flow and other variables of the system. Protection and control actions are different than classical voltage and angle stability studies. Generally, instability problems are related with inadequate reserve of generation, insufficient device responses, bad coordination of protection and control devices [26].

Frequency stability can be investigated over a wide range time interval between a few seconds and several minutes, so frequency stability is also considered as short-term or long-term phenomenon, like voltage stability. Inadequacy of under frequency load shedding, in the case of under generated island operation can be an example of short-term frequency instability, where frequency quickly decays and leads to island blackouts only in a few seconds [26]. Differently, long-term frequency instability problem is caused by speed controllers of steam turbines, boiler control and protection devices, and for that phenomenon, period can goes up to several minutes [27].

Rotor angle stability based security assessment and enhancement is the main interest of this study, and the next section explained angle stability in detail.

2.2 Rotor Angle Stability

Angle stability is defined as the ability of synchronous generators in the power system to remain in synchronism after the occurrence of a disturbance [24]. Angle stability is based on the ability to restore balance between mechanical torque and electromagnetic torque of each generator. Angle instability can be observed when angle swings of a group of generators increases and this leads synchronism loss with other ones.

In steady-state situation, there is a balance between the input (mechanical) and output (electromagnetic) torques of each synchronous generator. When a disturbance occurs, this balance breaks down and rotor of the generators starts to accelerate or decelerate, with respect to the laws of motion.

If one synchronous generator runs relatively faster than other one, rotor angle position of fast generator will advance with respect to the slower generator. Thus, this angle difference leads a load transfer from slow generator to fast generator, with respect to the highly nonlinear power angle relationship. This action tries to decrease the angle separation and speed difference. Above an angle difference limit, which is 90 degrees, increase in angle separation causes decrease of power transfer, thus, angle separation increases more. This leads to angle instability that observed if kinetic energy related with the rotor speed difference couldn't be absorbed by the system. Loss of synchronism can be observed between groups of generators or between one generator and the rest of the system. The angle stability is separated into two subcategories, such as large disturbance angle stability, and small disturbance angle stability. All types of rotor angle stability are considered as short-term phenomenon [22].

2.2.1 Large disturbance angle stability

Large disturbance stability (transient stability) is described as the ability of synchronous machines to remain in synchronism after the system is subjected to a large transient disturbance. It depends on severity of the disturbance and initial OP [23]. Large disturbances can be faults, switching of large loads, large generators tripping etc. In transient stability studies, generally, disturbances are considered as three-phase-to-ground, phase-to-ground or phase-to-phase-to-ground faults that are assumed to occur on transmission lines. Proper circuit breakers open to clear the fault and isolate the related transmission line from the rest of the system.

Insufficient synchronizing torque is not the only cause of instability by usually it leads to instability as an aperiodic separation of rotor angles (first swing instability).

If large disturbances occur, they cause big changes on the rotor angle deviations. These deviations cannot be estimated by a linear representation like in small disturbance stability situation. Therefore, time domain of interest is carried out for large and small disturbance stability. Period of interest for large disturbance stability is usually up to 10 seconds [24].

2.2.2 Small disturbance angle stability

Small disturbance angle stability (small signal stability) is the ability of synchronous machines to remain in synchronism after the occurrence of small disturbance. Disturbances are assumed very small, so, linearization of system equations can be tolerated for small signal stability (SSS) analysis.

Small disturbance stability is based on the initial OP of the system. Instability is caused by both insufficient synchronizing torque and insufficient damping torque. In today's power systems, voltage regulators of generators eliminate effects of insufficient synchronizing torque, and small disturbance stability problem is generally caused by insufficient damping torque [22].

Instability problems can be global or local. Interactions between groups of generators cause global stability problems. In global problems, oscillations of a generator group in one-area swings against another generator group in another area. Characteristics of these “inter-area mode oscillations” are complex and differ from “local plant mode oscillations”. Local plant mode oscillations can be described as oscillations of a single plant against all system. Damping of that kind of oscillations is based on the power of the excitation control system of generators, power plant and its output [22]. Period of interest for small signal stability is between 10 and 20 seconds.

2.3 Dynamic Security Assessment

Security assessment determines the vulnerability of the power system considering probable disturbances. After the occurrence of a disturbance, moving into a new operating condition with satisfying all physical constraints is mandatory for the power system security. In addition, the power system should survive the transition to these new operating conditions. These mentioned criteria for the system security emphasizes two cases of security analysis such as static security analysis and dynamic security analysis.

Static security analysis involves steady-state analysis of pre-disturbance and post-disturbance system state to confirm that system continue to meet the demand and operating conditions are violated. Pre-disturbance system state is related with the availability of transfer capability of lines and identification of congestion. On the other hand, post-disturbance state is related with the limits of transferred power flow and bus voltages.

Dynamic security analysis involves examining previously mentioned categories of system stability. It measures the ability of the system to withstand severe disturbances and moves into an acceptable steady state condition. Dynamic security analysis is always performed to determine if the level of security decreased under a acceptable safety level and to apply appropriate control action.

Since rotor angle instabilities have greater impacts on the continuity of power system operation, this study deals with rotor angle stability related DSA and enhancement. Therefore, dynamic security analysis term in this study only involves examining large and small disturbance angle stability.

2.3.1 Large disturbance angle stability assessment

There are various approaches for large disturbance angle (transient) stability assessment, such as time domain simulations, direct methods, probabilistic methods, and machine learning methods.

Time-domain-simulation (TDS) is the most straightforward method for transient stability assessment. TDS directly shows the behavior of the system dynamics in time domain. Then, these behaviors are used to compute a stability index for transient stability assessment. Method can deal with detailed system model to enhance the accuracy of the stability assessment, but also increases the computational burden, which is the main drawback of the method. Thousands of nonlinear, algebraic and differential equations are solved to determine the stability for each severe contingency. This process requires intensive computation effort and

TDS cannot be used for online applications by considering today's microprocessor technology.

Direct methods assess the stability of the system without solving differential equations. Methods employ special form of Lyapunov function, which is called transient energy function [3]. Between the occurrence and clearance time of a disturbance, kinetic energy starts to accumulate in power systems. Energy function is used to calculate the critical kinetic energy for the system, which is the maximum amount of energy that can be absorbed by the components of the system. If accumulated energy becomes larger than critical kinetic energy before the clearance of the disturbance, the system is considered as unstable [3]. Although, direct methods avoid the time consuming calculation, they are considered as impractical, because of modeling limitation for large-scale power systems.

Probabilistic methods, determine the probability distributions for the stability of the system. Probability of the stability can be defined as the probability that the system remains stable when considered disturbance occur [4]. Method considers, large number of faults at various locations with various clearing time. These detailed considerations make the method suitable only for power system planning purposes.

Selected (or measured) features of the power system can also be associated with system's stability through machine learning methods. In recent years, machine learning methods such as neural networks, decision trees, support vector machines have been successfully applied for security assessment of the power systems [5-11]. Machine learning methods also need an offline training process via properly generated data involves adequate number of different examples of system behavior. These methods tradeoff between the accuracy of the assessment and required computation time. They are not as accurate as TDS, but their implementation is much faster than TDS. Enhancing the accuracy and decreasing the offline training process, increases the applicability of machine learning methods for online applications [12].

2.3.2 Small disturbance angle stability assessment

To determine the small disturbance angle (small signal) stability, three main methods can be used, such as modal analysis, TDS and identification methods.

Modal analysis is a common method to analyze the oscillatory modes in the system. When the amplitude of the disturbance is quite small, post disturbance response of models of system components can be considered as linear. This linear behavior eases the analysis of oscillations, such that, the system model, which involves nonlinear equations, can be linearized around steady state OP. Then, modal analysis is easily applied to a linear system model and oscillations are characterized in an accurate way [28].

Identification methods are also used for analyzing the oscillatory modes. Methods use recorded signals, which are measured and collected by measurement units or TDS [29]. Methods obtain and use the parameters of modulated electric signals to determine the small signal stability [30].

In addition, TDS can be used to assess the small signal stability. TDS can be preferred for small sized test system, but it is obvious that the used of TDS to analyze the oscillations caused by a small disturbance in large power systems is very time consuming because of the same reasons explained in transient stability assessment. In addition, larger systems may involve inter-area oscillations with similar frequencies and it is not easy to separate them by using TDS [28].

2.4 Dynamic Security Enhancement

Objective of security enhancement is preventing the system from undesired situations, and avoiding large blackouts. Generally, security enhancement is categorized into two sub-categories such as preventive control and corrective control.

2.4.1 Preventive control

The objective of preventive control is successfully preventing the network from losing its stability against uncertain disturbances (critical contingencies). These are generally open loop control actions such as generation rescheduling, load curtailment, reactive power control, high-speed excitation. System state is known, but disturbances are considered as uncertain in preventive control [31].

In this thesis, applications of generation rescheduling and load curtailment preventive control actions for enhancing the dynamic security of the power system are studied.

Generation rescheduling is a useful preventive control action to restore and enhance the system security by shifting the generation among controllable generators [32]. System operator can monitor (real time) the generation and demand of electric power. When insecure OP is detected, the system operator can request from some smart loads to curtail their electric power demand [33]. This load curtailment action can integrated with generation rescheduling and a proper adjustment of these preventive control actions changes the power flow patterns within the network. Then, power system moves to a secure OP so that the stability of the system is preserved despite the occurrence of a critical contingency.

2.4.2 Corrective control

If preventive control actions cannot move the system to a secure OP for any critical contingency, or the cost of preventive control is considered as high, power system can be armed by corrective control actions, which are ready to be applied in case of occurrence of any contingency.

As different from preventive control, the disturbance has already occurred in corrective control. The objective of the corrective control is minimizing the effects of occurred disturbance on the dynamics of the system and regaining the large disturbance angle stability of the system. In corrective control, disturbances are known, but system state is uncertain [31].

In this thesis, load shedding method is studied as a corrective control action to regain the stability of the system if preventive control action cannot be applied and protect the system against critical contingencies [9]. Although both load shedding and load curtailment methods decrease the electrical power consumption in the related load buses, they are different methods by means of their application schedules, magnitudes and costs. As different from load curtailment method, load shedding is a fast switching operation that applied after the occurrence of contingency, and the amount of load to be shed is relatively larger than curtailment, since the maximum amount of load to be curtailed is based on the amount of intelligent loads in the selected load buses.

3. METHODS FOR SECURITY ASSESSMENT AND ENHANCEMENT

3.1 Introduction

Dynamic model of power system involves linear and nonlinear equations that include a huge number of continuous and discrete state variables. When time domain simulations are used for transient stability analysis, the calculations required for recursively solving nonlinear differential equations of the system model over thousands of time steps, can take significant amount of time even for the occurrence of one critical contingency. These requirements make time domain simulation impracticable for real time applications. Similar problem is valid for small signal stability assessment of real power system models with thousands of buses.

Artificial Neural Networks, is one of the computational intelligence method that have shown promising results for many power system applications. To enhance the practicability of online monitoring of power system dynamics by dealing high computational burden, ANN based DSA methodology is proposed.

After the assessment of an insecure state for the current OP of the system, preventive control actions should be taken, otherwise some generators may lose their synchronism and the system can be drifted to instability after the occurrence of a critical contingency. In this study, while the studied preventive control actions move the power system to a new OP at which the system's security is regained, the proposed method also involves an optimization procedure that offers minimization of determined objective function. In other words, proposed preventive and corrective control actions are considered as constrained, multi-dimensional optimization problem, with both continuous and discrete variables. In real, large sized power systems, the size of the control variable vector (dimension of the search space), number of equality and inequality constraints, nonlinearity of constraints related with dynamic behavior of the system, force us to use alternative methods to conventional optimization methods.

In this chapter, brief summary for the applied artificial neural networks structures and population based optimization methods in this study is given.

3.2 Artificial Neural Networks For Dynamic Security Assessment

In last two decades, ANN have been used for various power system applications and have been shown satisfactory performance. Various ANN topologies have been developed, and these topologies can be grouped as feed forward and recurrent neural networks. The signal can just flow in one (forward) direction, in feed forward neural networks. Most recent feed forward type neural networks are, Single Layer Perceptron Neural Network [34], Multilayer Perceptron Neural Network (MLP) [14], Probabilistic Network [35], Radial Basis Function Network [36], General Regression Network [37], Self-Organizing Feature Map [38], Learning Vector Quantization Network [39], Adaline and Madaline [40]. On the other hand, the signal can also flow in the backward or the lateral direction in recurrent neural networks. A few of the neural network architectures explained by Haykin [41], as well as some more recent ones are listed as follows. Hopfield Network [42], Echo state network [43], Elman Network and Jordan Network [44], Adaptive Resonance Theory Network [45] and Bi-Directional Associative Memory Network [46] can be considered as the most recent examples for recurrent neural networks.

In this thesis, DSA problem is considered as both a regression and a classification task. A stability index value can be estimated in the regression task, or it can be used as a threshold to define secure and insecure classes, then the problem is transformed to a classification task.

3.2.1 Multilayer perceptron neural networks

The structure of a MLP involves a system of interconnected neurons (nodes). As shown in Figure 3.1, the neuron connections are weighted by parameters w. The direction of the signal flow is forward, since MLPs are feed forward neural networks. Output of all neurons in the layer x are scaled by the related connection weights then fed forward for the input of neurons in the layer y. Output of a particular neuron in layer y is the function of the sum of the input signals of the neuron (3.1). These functions are simple formed transfer functions which are also called activation functions. Some widely used activation functions are hyperbolic tangent, logistic sigmoid, linear and ramp. As an example, hyperbolic tangent activation function is given in (3.2), and details about various activation functions can be found in [41]. If all transfer functions used in the structure were linear, MLP could only approximate linear functions. Super positioned of nonlinear activation functions, enables the approximation of extreme non-linear functions. Study in [41] proves that, if a layer with enough nonlinear neurons is followed by a layer consisting of linear neurons, this MLP structure becomes a universal function approximator that can approximate any nonlinear, smooth function, including dynamic behavior of power system.

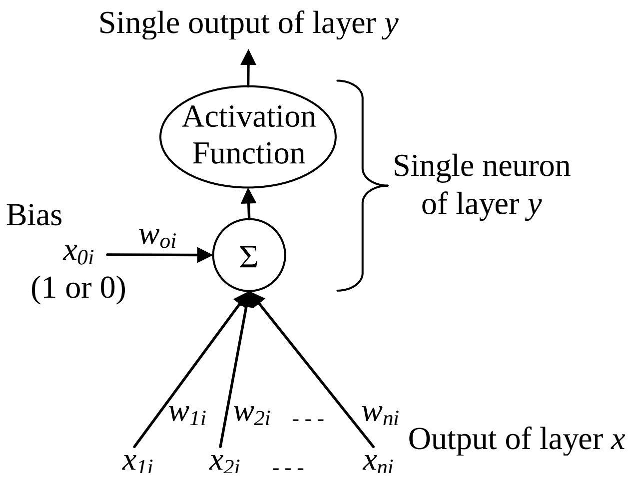


Figure 3.1 : Structure of single unit of MLP.

$$out(x_i) = f\left(\sum_{j=1}^{n} x_{ji} w_{ji} + x_{0i} w_{0i}\right) \quad \textbf{(3.1)}$$

$$f(x) = \frac{1-e^{-x}}{1+e^{-x}} \quad \textbf{(3.2)}$$

The number of neurons in the input layer is equal to the number of input features used. Number of neurons in the output layer depends on how many target values to be estimated by MLP. The number of hidden layers and size of the hidden layers (number of neuron in each layer) are based on the complicacy of the function to be approximated. Generally, MLP structures have one or more hidden layers.

The training process is used to find suitable weights and bias values of MLP for establishing the relation between output and inputs. MLPs are generally uses back-propagation training and learn in supervised mode. It means that, they need a training data includes different examples of input and output values. In the training process, the ANN is fed by a set of inputs and related target (desired outputs). Then, ANN try to learn from these different examples. The back propagation training can be summarized as,

1. Initialize weight and bias values
2. Feed the network with one input set from the training data
3. Propagate the input signal through the network and obtain the output
4. Calculate difference (error) between target and obtained output
5. Back-propagate the error through the network in opposite direction (3.3)
6. Adjust weight and bias values via learning method (3.4)
7. Repeat steps 2 to 7 using other input sets, until achieving acceptable error.

The objective of the training process is adjusting the best set of weights and bias values which provide minimum error (step 6). Gradient descent is the one possible methods to be used in that step [47, 48].

The training explained with the seven steps above, is called online (sequential) training where each input vector is given to ANN individually. In an alternative method called batch training, summed error values are used to adjust the weights. Advantages and disadvantages of both methods are presented in [49]. During the back-propagating the error and adjusting the weights, the steepest descent can be written as,

$$E_t(w) = \frac{1}{2N_d} \sum_{k=1}^{N_d} \sum_{m=1}^{M} y_k^m - \hat{y}_k^m (y_k^m w)^2 \qquad \textbf{(3.3)}$$

$$w_{ij} \leftarrow \left(w_{ij} - \eta \frac{\partial E_t}{\partial w_{ij}} \right) \qquad \textbf{(3.4)}$$

where N_d is the number of instances in the training data, M is the number of output neurons of network, y represents the targets in training set, $\hat{y}$ is the obtained ouput (step 3), E_t is the overall error to be minimized and n is learning rate.

After the training, inputs of unseen test set are given to the network and testing error is calculated to investigate the accuracy of the designed network. Details can be found in Section 4.

3.2.2 Probabilistic neural networks

In 1991, Specht introduced PNNs, which are designed for supervised multi-class classification tasks. PNN is a nonparametric probability density function estimator, which is based on the Bayesian classification rule and the Parzen window [15]. One of the advantages of using a PNN is the training speed, since the training set (TS) is stored in its pattern layer and it needs one epoch for a total training. The size of the pattern layer in a PNN structure is directly dependent on the size of the TS. Therefore, the obvious disadvantages of PNNs are the large storage requirements and slow execution speeds in the applications involving large training sets.

The PNN structure consists of four layers, as illustrated in Figure 3.2. Let $c=1,2...C$ be the number of classes and S_c be the size of class c in a given TS. Let X be an n dimensional input vector and $X_{c,s}$ be the sth pattern of the TS which belongs to class c. In the pattern layer, a pattern neuron is created for each $X_{c,s}$, and these neurons are grouped by their classes. The activation function for each neuron $G_{c,s}$ is selected such that $X_{c,s}$ is located at the center of the activation function. Generally, the activation function is selected as Gaussian,

$$G_{c,s}(X) = \frac{1}{(2\pi\sigma)^{n/2}} exp\left(-\frac{\|X-X_{c,s}\|^2}{2\sigma^2}\right) \quad \textbf{(3.5)}$$

where σ is an adjustable smoothing parameter for determining the shape of activation function. If input vector X is close to $X_{c,s}$ pattern, then the output of related neuron will be close to its maximum value. All pattern neurons of class c are connected to the same summation neuron Y_c, which belongs to the class c in the summation layer. The outputs of all neurons of class c are summed in the summation layer as in (3.6).

$$Y_c(X) = \sum_{s=1}^{S_c} w_{c,s} G_{c,s}(X) \quad \textbf{(3.6)}$$

where $w_{c,s}$ is the weight for the sth pattern neuron of class c, and the sum of all weights belonging to class c equals 1. Finally, the competitive layer determines the summation neuron with the maximum output, and the input vector X is appointed to a class accordingly.

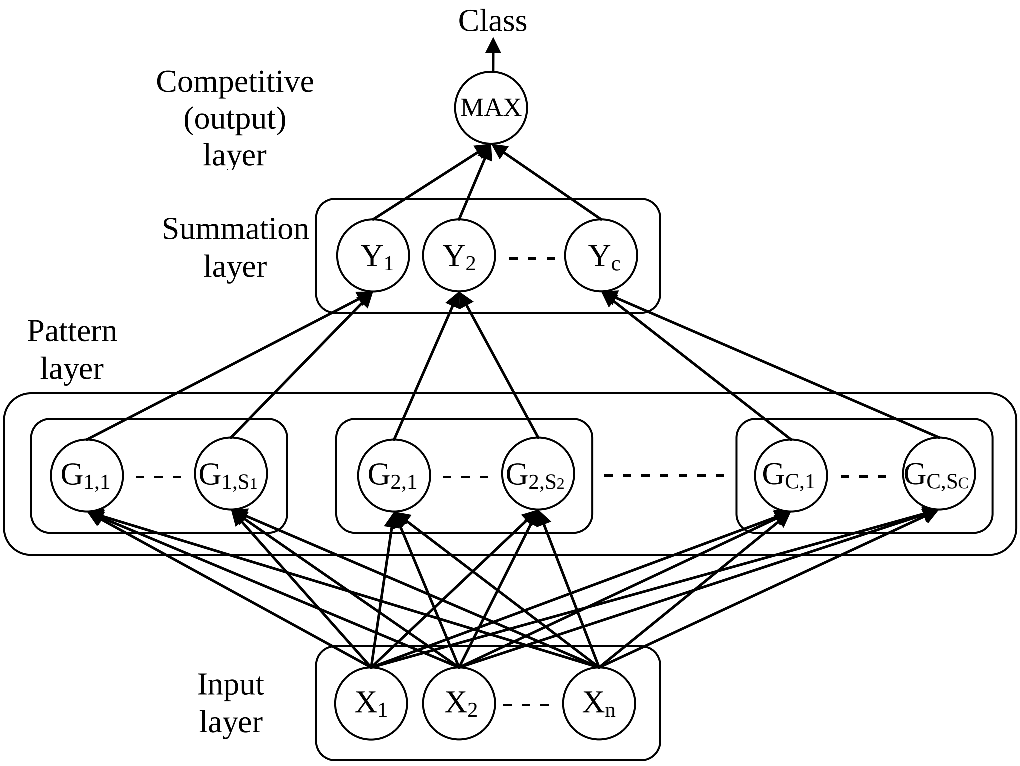


Figure 3.2 : Structure of PNN [15].

3.2.3 Adaptive neuro fuzzy inference systems

In 1993, Jang introduced Adaptive Neuro Fuzzy Inference Systems (ANFIS), which combine fuzzy inference systems with learning techniques developed for ANNs [50]. ANFIS uses a TS to create a FIS and adjust parameters (premise parameters) of membership function (MF) in backward pass and rule parameters (consequent parameters) in forward pass by using a hybrid technique including both back-propagation and least squares methods. This ANN approach gives a high performance in nonlinear function modeling and is implemented into many applications of system modeling, and fuzzy control. For the sake of illustration, a typical n- input-single-output ANFIS structure with two fuzzy MFs for each input is shown in Figure 3.3, where the square nodes represent the adaptive nodes, and the circle nodes represent the fixed nodes. First order Sugeno fuzzy model is widely used for rule structure, and the *k*th fuzzy rule of this ANFIS can be expressed as;

$$If\ x_1\ is\ A_{1,j} and\ x_2\ is\ A_{2,j}\ ...\ x_n\ is\ A_{n,j};\ then \qquad \textbf{(3.7)}$$

$$y_k = p_{k,1}x_1 + p_{k,2}x_2 + \cdots + p_{k,n}x_n + p_{k,n+1} \quad i = 1 \ldots n, \quad j = 1,2, \quad k = 1 \ldots K$$

where $A_{1,j}$ to $A_{n,j}$ are the input MFs for input features x_1 to x_n. The consequent parameters of the rule implementation layer are denoted by $p_{k,1}$ to $p_{k,n+1}$,which are updated by the least squares method.

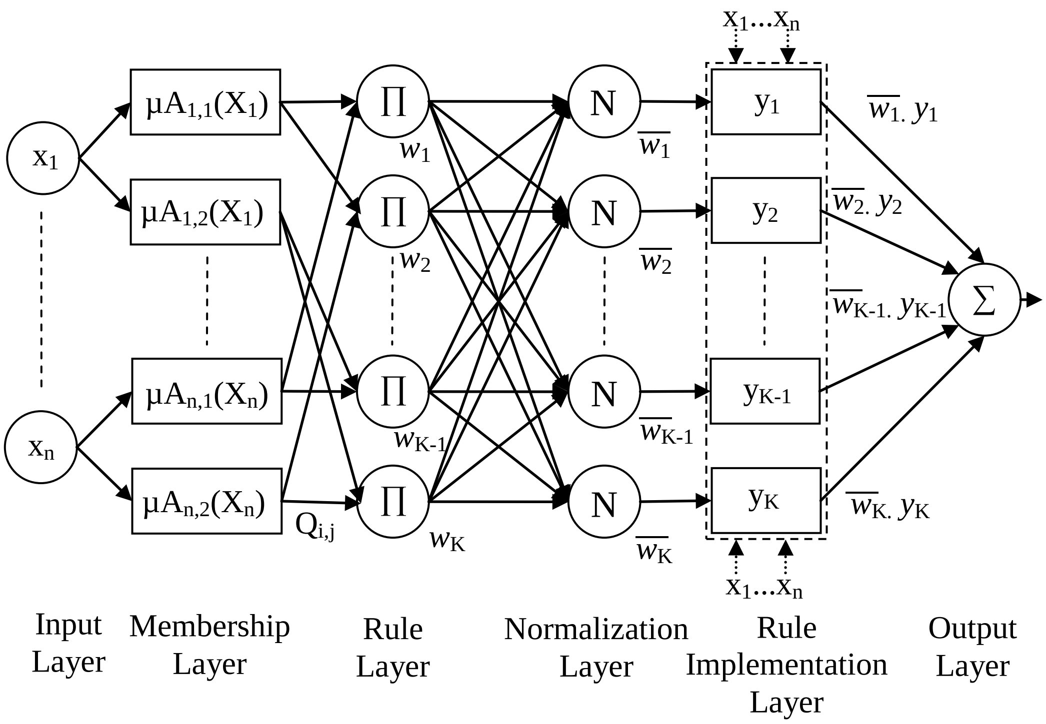


Figure 3.3 : Structure of n-input single-output ANFIS [50].

MFs in the membership layer calculate the membership degrees of the related input node. The output of *j*th MF associated with the *i*th input node can be described as follows,

$$Q_{i,j} = \mu A_{i,j}(x_i) \quad i = 1 \dots n, \quad j = 1,2 \tag{3.8}$$

For calculation of $Q_{i,j}$, MFs can be chosen as Gaussian, generalized bell-shaped, triangle and trapezoidal shaped functions. A generalized bell-shaped function can be given as,

$$\mu A_{i,j}(x_i) = \frac{1}{1+\left|\frac{x_i - c_{i,j}}{a_{i,j}}\right|^{2b_{i,j}}} \quad i = 1 \dots n, \quad j = 1,2 \tag{3.9}$$

where $a_{i,j}$, $b_{i,j}$, and $c_{i,j}$ are three adjustable parameters which are called the premise parameters and are updated via back propagation learning method. If the consequent parameters are fixed, then gradient descent algorithm can be used to adjust premise parameters. The outputs of the nodes in the rule layer are called rule firing strengths, which are calculated by the product of all incoming signals according to predetermined rules. The firing strength of the kth rule can be described as,

$$w_k = \mu A_{1,j1}(x_1).\mu A_{2,j2}(x_2) \ldots . \mu A_{n,jn}(x_n) \quad j_m = 1,2, \; m = 1..n, \; k = 1..K \quad \textbf{(3.10)}$$

In the normalization layer, all firing strengths are normalized as,

$$\overline{w}_k = \frac{w_k}{\sum_{k=1}^{K} w_k} \quad \textbf{(3.11)}$$

The output of the rule implementation layer is the product of normalized firing strengths and adaptive node functions,

$$\overline{w}_k y_k = \overline{w}_k (p_{k,1}x_1 + p_{k,2}x_2 + \cdots + p_{k,n}x_n + p_{k,(n+1)}) \quad \textbf{(3.12)}$$

In the output layer, the overall output of ANFIS, which is the summation of all incoming signals, is computed through a summation operator,

$$Y = \sum_{k=1}^{K} \overline{w}_k y_k. \quad \textbf{(3.13)}$$

3.3 Optimization Methods For Security Enhancement

In this study, while the power system is moved to a new OP at which the system's security is regained, the proposed method also involves an optimization procedure that offers minimization of determined objective function. In other words, proposed preventive and corrective control actions are considered as constrained, multi-dimensional optimization problem, with both continuous and discrete variables. In real, large sized power systems, the size of the control variable vector (dimension of the search space), number of equality and inequality constraints, nonlinearity of constraints related with dynamic behavior of the system, force us to use alternative methods to conventional optimization methods. In this chapter, brief summary of population based optimization methods that are used in this study is given.

3.3.1 Genetic algorithms

GAs are stochastic search techniques based on Darwin's theory of evolution and the principles of genetics. The algorithm creates a population of individuals, which are potential solutions to an optimization problem, and mimics the evolution process in nature to maximize an objective function [16].

The flowchart of a typical GA optimization is shown in Figure 3.4. In most of the GA applications, an initial population is created randomly in accordance with the constraints on the individuals within the population. After creating the initial population, the fitness values of the individuals are calculated to determine the capability of initial solutions to maximize the objective function. Then, a loop consisting of genetic operators begins to run until a predetermined stopping criterion is met. The first operator in the loop is the selection operator that is based on "survival of the fittest" principle, which means that better individuals continue to live and transfer their genetic code to new generations. According to the fitness values of individuals, the selection operator determines the individuals that become parents for the crossover process, which is based on Mendel's gene transfer law. The crossover operator recombines the genetic codes of the selected parents and produce new children, which will take place of the worst individuals in the population. The mutation operator is inspired by the mutation process in nature and can be described as a random change in the genetic code of individuals. Generally, this operator is used with small probability but can keep the algorithm away from local optimums. Creating a proper stopping criterion prevents the algorithm from terminating before the global solution is found.

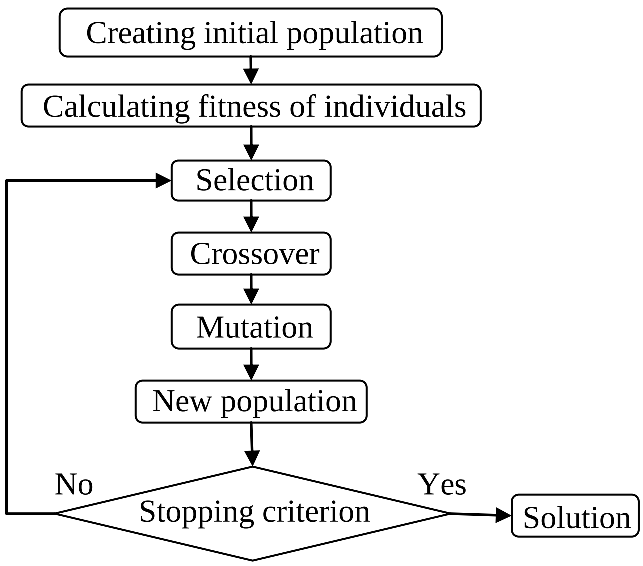


Figure 3.4 : Flowchart of a basic GA [16].

GA structure varies depending on the characteristic of the optimization problem of interest. For the optimization procedure of GAs, the types and parameters of genetic representation, selection operator, crossover operator, mutation operator and stopping criterion must be specified. As seen from that list, the major drawback of GA is the number of parameters needs to be adjusted, to achieve a satisfactory search performance. After selecting the genetic representation type for candidate solutions, proper genetic operator should be determined with respect to genetic representation type. Since there are large number of choices for genetic operators, they are not explained in this thesis. More information can be found in [16].

3.3.2 Differential evolution

Differential Evolution is a population based, stochastic optimization method introduced by Price and Storn [17]. The development of the algorithm started with the idea of using the differences of position vectors to change the recent vector population. Popularity of the algorithm increases due to its powerful convergence results, robustness and its simplicity. The implementation of the algorithm is very simple and has only a few control parameters such as population size, scaling (mutation) factor, and crossover rate. The algorithm adds the weighted difference between two population vectors to a third (base) vector for creating a mutant vector, such that,

$$v_i^G = x_b^G + F_i(x_c^G - x_d^G) \tag{3.14}$$

where $b \neq c \neq d$ are integers randomly generated by uniform distribution from a set $\{1,2,\ldots,S\}$, S is the size of the population F_i is the scaling factor for ith individual of population, and G is the generation number.

After mutant population is created, similarly to GA, crossover operator is applied to mutant vectors and the target vector from the population, and trial vector is created. Generally, binomial type crossover is used in application, since it is claimed that binomial is never worse than exponential. In the last step, objective function values of target and trial vectors are compared by greedy search method which only hold the better one [17].

1. Initialize the vector of population
2. Select target and base vectors from population
3. Calculate weighted difference of two randomly choosen vectors from population
4. Add weighted difference to base vector to create mutant vector

5. Apply crossover to target and mutant vector to create trial vector
6. Compare target and trial vectors and hold the better one
7. Repeat steps 2 to 6, until stopping criterion is achieved

DE also offers different mutation strategies. Basic strategy is **DE/rand/1**, which is explained by (3.14). This strategy enables good diversification for scanning the search space, because base vector x_b^G is randomly selected from the population. Second strategy is **DE/best/1** where the base vector x_b^G is selected as the vector of best solution x_{best}^G. This strategy provides good intensification for searching process. On the other hand, all search algorithms should provide a balance between intensification and diversification. To improve that criterion, **DE/rand-to-best/1** is proposed. The mutant vectors are created such that,

$$v_i^G = x_i^G + F_i(x_{best}^G - x_i^G) + F_i(x_c^G - x_d^G) \qquad \textbf{(3.15)}$$

where x_i^G represents the current position vector of *i*th individual at *G*th generation. For each individual *i*, mutation strategy calculates difference of two randomly selected individual, and difference between vectors of best individual and *i*th individual. These differences are weighted by F_i and added to the position vector of *i*th individual. Adding information about best vector increases the convergence speed. **DE/rand/2** and **DE/best/2** strategies are similar to **DE/rand/1** and **DE/best/**. Instead of using $(x_c^G - x_d^G)$ for the calculation of difference, these modified strategies uses $(x_c^G - x_d^G + x_e^G - x_f^G)$ where $c \neq d \neq e \neq f$ is randomly generated integers by using uniform distribution between the range of 1 to *S*. These strategies are used to increase the diversification of search process if needed.

After the mutation process, the crossover operator is applied to the mutant vector and the target vector and the trial vector is created such that,

$$u_{i,j}^G = \begin{cases} v_{i,j}^G & if \;\; CR_i \geq rand \\ x_{i,j}^G & else \end{cases} \qquad j = 1,2,\dots,D \qquad \textbf{(3.16)}$$

where $u_{i,j}^G$ is the *j*th parameter of *i*th trial vector created in generation *G*, *D* is the dimension of the search space, and CR_i is the crossover rate for the *i*th vector. This rate changes between 0 and 1, and determines fraction of the mutated parameters. *CR*, *F* and *S* are the only parameters to be selected.

3.3.3 Big bang-big crunch optimization

The BB-BC optimization method is based on Big Bang and Big Crunch theory, which is developed to explain the evolution of the universe. In the Big Bang phase, the universe is developed from a very tiny dense state by an explosion. Energy dissipation generates disorder and randomness in this phase, whereas randomly distributed particles are drawn into an order during the Big Crunch phase [20].

Similar to the original theory, BB-BC optimization method involves two sequential phases, a Big Bang phase and a Big Crunch phase. The method generates candidate solutions (individuals) which are randomly distributed over a search space during the Big Bang phase, which corresponds to dissipation of energy in nature. Then, the randomly generated solutions are shrunk to a single point via a center of mass calculation in the Big Crunch phase where the convergence to an optimum point resembles the gravitational attraction. Disorder is created from ordered particles by energy dissipation, thus the method uses randomness as a conversion to the generation of new candidate solutions (disorder) from a converged solution (order) [8]. A flowchart for the BB-BC optimization procedure is given in Figure 3.5.

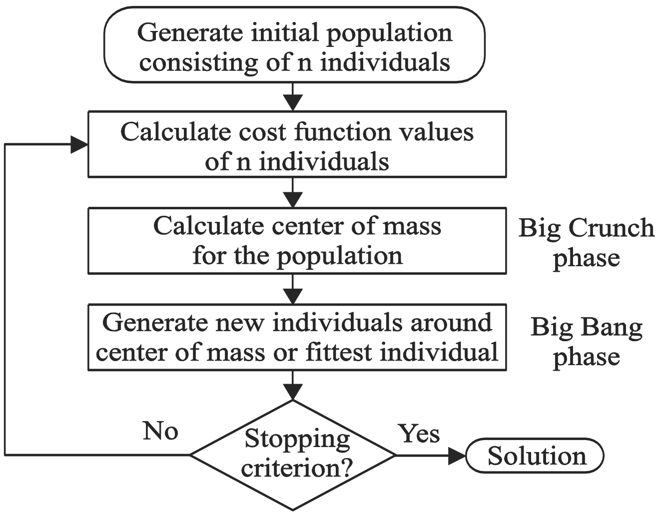


Figure 3.5 : Flowchart of BB-BC method [20].

Similar to other population based search algorithms, the initial population with a uniform distribution is spread over the search space. For latter iterations, candidate solutions are normally distributed around the center of mass of the population or the fittest solution. Then, the cost function values of each member of the new population are calculated. This step is followed by the Big Crunch Phase where the cost function value and the position of each candidate solution are used to calculate the center of mass of the population consisting of N individuals,

$$x^c = \sum_{i=1}^{N} \frac{x_i}{f_i} \left(\sum_{i=1}^{N} \frac{1}{f_i} \right)^{-1} \tag{3.17}$$

where f_i and x_i are the cost function value and position vector of the ith candidate solution, respectively [8]. This squeezing operation in the Big Crunch phase takes the candidate solutions as a whole and it is found to be more effective than selecting two solutions and finding their center of gravity. Followed by the Big Crunch phase, in the Big Bang phase, the method creates new candidate solutions around x^c,

$$x_n = x^c + r\beta(x_{max} - x_{min}) \left(1 + \frac{j}{s}\right)^{-1}, n = 1, \dots, N \tag{3.18}$$

where x_n represents the position vector of a new candidate solution, r is a random number drawn from the standard normal distribution, β is a parameter used to restrict the size of the search space, j is the iteration number, s is the smoothing factor that corresponds to how fast the size of the search space will be reduced, x_{max} and x_{min} are the upper and lower limits of the search space, respectively. When an optimization method starts to converge to an optimal point, most of the candidate solutions are generated around the optimal point. If the method is used to find an optimum point, the population must involve a number of different points from the other parts of the search space with a decreasing probability. Therefore, new candidate solutions are spread around x^c with a distribution whose standard deviation decreases while the iterations go forward. The key point of the method is always generating new solutions, which are far from the center of mass with a decreasing nonzero probability. This action prevents sticking into local optimum center of mass points and provides the global convergence. The explosion (Big Bang) and contraction (Big Crunch) operations are repeated until the method meets a stopping criterion, which may depend on the difference between the cost function values or locations of the optimum points calculated in two consecutive Big Crunch phases.

3.3.4 Particle swarm optimization

In 1995, Kennedy and Eberhat introduced Particle Swarm Optimization [18]. The development of the algorithm starts with mathematical simulation of social behavior of bird flocks and fish schools. Convergence characteristic of PSO is analyzed and mathematical foundation is represented to describe the searching behavior of a simple PSO structure in [18].

In [51] swarm intelligence is defined as “any attempt to design algorithms or distributed problem-solving devices inspired by the collective behavior of social insect colonies and other animal societies”. In PSO, a candidate solution is called individual or particle of swarm. Particles share their information with their neighbors and each particle tends to move to the best position achieved by neighbor particles or best position of the whole swarm. The swarms fly through the multidimensional search space with a velocity to find optimum solutions in the feasible subspace. The velocity of particles is calculated with respect to their previous positions and behaviors. In *n* dimensional search space, each particle is represented by its position vectors and velocity vectors,

$$x_i^k = \left[x_{i1}^k, x_{i2}^k, \dots, x_{in}^k\right] \tag{3.19}$$

$$v_i^k = \left[v_{i1}^k, v_{i2}^k, \dots, v_{in}^k\right] \tag{3.20}$$

where x_i^k and v_i^k are the position and velocity vectors of *i*th particle in *k*th iteration, respectively. The velocity of each particle is updated by considering last velocity value, best position achieved by relevant particle and best position achieved by the swarm,

$$v_i^{k+1} = wv_i^k + c_1 r_1\left(pbest_i^k - x_i^k\right) + c_2 r_2\left(gbest_i^k - x_i^k\right) \tag{3.21}$$

where w represents the inertia weight, $pbest_i^k$ is the position of best of *i*th particle after k iterations, $gbest_i^k$ is the position of global best particle achieved after k iterations, r_1 and r_2 are random numbers generated by uniform distribution between 0 and 1, c_1 and c_2 are positive constants. Then, position of each particle is updated such that,

$$x_i^{k+1} = x_i^k + v_i^{k+1} \tag{3.22}$$

Basic steps of PSO can be explained as,

1. Initial value of position and velocity vectors of each particle are initialized using uniform distribution, considering the parameter limits
2. Objective function value of each particle is calculated, then position and objective function values of p_{best} and g_{best} are stored/updated
3. Velocity and position vectors of particles are updated by using (3.21) and (3.22)
4. Steps 3 and 4 are repeated until a stopping criterion is satisfied.

3.3.5 Artificial bee colony optimization

Promising convergence performance of PSO and its variants on various optimization problems in different disciplines, has been increased the research interest on swarm intelligence in last decades. Artificial Bee Colony is one of the swarm based search algorithm, influenced by the foraging behavior of honeybees. Karaboğa, first introduced this meta-heuristic search algorithm [19].

The algorithm involves three types of bees, such as employed bees, onlooker bees and scout bees. Employed bees are related with food sources, onlooker bees monitors the behavior of employed bees in the hive and select a food source. Scout bees randomly look for food sources. Scout bees and onlooker bees are also named as unemployed bees.

In the first step, scout bees explore positions of food sources (candidate solutions). Then, employed bees and onlooker bees collected the nectar of food sources (fitness of solutions). This continuous process finishes the food sources, and then employed bees that exhaust the food source become a scout bee to look for a new food sources. One employed bee is associated with exactly one food source. Common progress of ABC algorithm is given below [19],

1. Initialization phase
2. Employed bees phase
3. Onlooker bees phase
4. Scout bees phase
5. Memorizing the best solution achieved up to now
6. Repeat steps 2 to 5 until, stopping criterion is achieved.

In the initialization phase, the algorithm randomly creates first candidate solution within the range of upper and lower parameter constraints, by using uniform distribution.

Employed bees look for new food sources with more nectar near food sources in their achieve. More nectar means better fitness values. New neighbor food sources are calculated such as,

$$v_{mi} = x_{mi} + s_{mi}(x_{ri} - x_{mi}) \qquad \textbf{(3.23)}$$

where i represents the parameter number of position vectors and it is randomly determined. x_{mi} is the ith parameter of current food source m in the achieve, v_{mi} is the i th parameter of new food sources near mth source, x_{ri} is the i th parameter of randomly selected food sources and s_{mi} is a factor to determine the range of neighborhood search distance for ith parameter. When v_m is generated, greedy selection method is applied for v_m and x_m, and x_m is replaced by v_m only if v_m is a food source with more nectar.

Onlooker bees in the hive use the food information of employed bees and onlooker bees choose food sources with respect to a probability that depends on the fitness or objective function value of the food sources. In other words, the probability of generating new solution near good (fit) solutions is bigger than the probability of generating new solution near bad solutions. Various types of probability functions can be used for food sources. This action is similar to the selection operator of GA. In this study, selection probability of food mth source $prob_m$ is calculated such that,

$$prob_m = 0.2 + \frac{f(x)_{max} - f(x_m)}{f(x)_{max}} 0.8 \qquad \textbf{(3.24)}$$

where $f(x_m)$ is the objective function value of mth food source, and $f(x)_{max}$ is the maximum and also the worst objective function value of all food sources, since optimization problem is considered as a minimization problem. When onlooker bees select their food sources, **(3.23)** is used to create new solutions, where x_m becomes the selected food source. After new v_m is generated, greedy selection method is applied again, as explained in employee bee phase.

Generally, number of new solutions generated by employed bees and onlooker bees are same, but this conditions can be modified by using a dynamic parameter that characterize the converge behavior during the optimization.

In the latter iterations of the optimization, solutions of some employed bees cannot be enhanced after a specific number of trials. Then, these employed bees and related food sources are replaced by scout bees. Scout bees randomly search new solutions all over the search space using uniform distribution function. Then, scout bees start to act like employed bees, until their food sources cannot be enhanced after multiple trials.

As seen from the structure of ABC, the algorithm is influenced by different population based methods. Probability of selection of food sources to create new solutions is similar to GA's selection strategy. On the other hand, (3.23) that is used to generate new solutions is similar to crossover operator of DE. ABC algorithm has just few parameters to be adjusted, such as scale factor s, size of the population, number of iterations and type of the probability function used in onlooker bee phase.

3.3.6 Mean variance mapping optimization

Mean Variance Mapping Optimization (MVMO) is population-based stochastic optimization technique. The unique feature of the algorithm is the transformation used for mutating the solutions based on mean-variance of the population (archive) that involves *n* best solution. Although the search focuses around the mean values, the algorithm also looks for solutions outside the mean areas. It means, "the method performs global search but the emphasis is almost around the means" [21].

For all parameters of the solution vector, search range is defined between 0 and 1. During the function evaluation, solution vector is denormalized to its original value. Key point of the algorithm is the mapping function which is defined by two variables such as mean and shape variables. These variables are calculated by using n best solutions stored in the archive. Figure 3.6 shows the mapping function used to transform random variable x_i^* into x_i which is concentrated close to the mean.

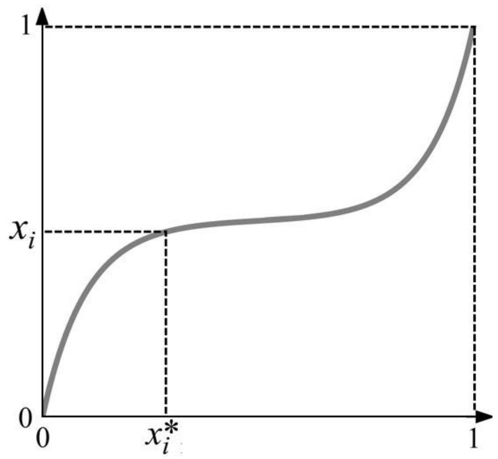


Figure 3.6 : Mapping function h.

Then, *i*th variable of new candidate solution *x* is described as follows:

$$x_i = h_x + (1 - h_1 + h_0)x_i^* - h_0 \quad \textbf{(3.25)}$$

where x_i^* is a random variable generated by uniform distribution and the *h* function is computed as,

$$h(\bar{x}, s_1, s_2, x) = \bar{x}(1 - e^{-x.s_1}) + (1 - \bar{x_i})e^{(x-1)s_2} \quad \textbf{(3.26)}$$

h_0, h_1 and h_x are the outputs of the *h* function with different inputs such that,

$$h_0 = h(x = 0), \;\; h_1 = h(x = 1), \;\;\; h_x = h(x = x_i^*) \quad \textbf{(3.27)}$$

x_i is always generated between [0,1]. The shape (s) and mean variable determine the characteristic of *h* function, as seen from Figure 3.7.

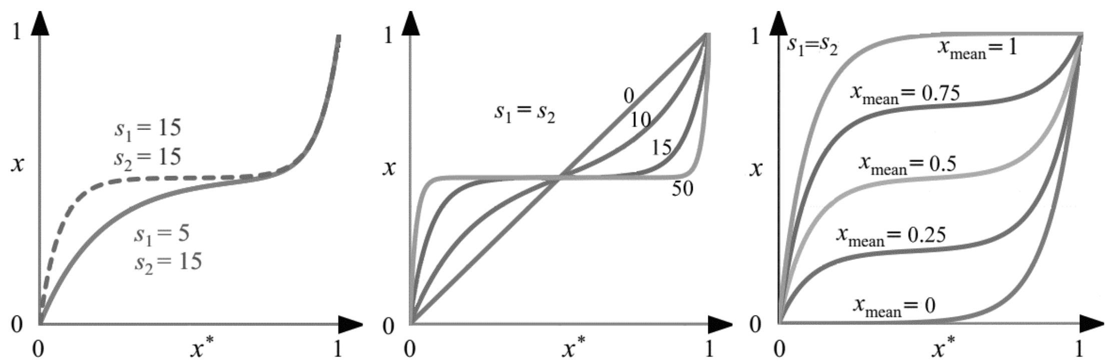


Figure 3.7 : Effects of parameters on the mapping function.

Mean and shape variables are calculated by using the solution in the archive where the n best solutions are stored.

$$\overline{x_i} = \frac{1}{n}\sum_{j=1}^{n} x_i(j) \tag{3.28}$$

$$s_i = -\ln(v_i) f_s \tag{3.29}$$

where v represents the variance as follows,

$$\overline{v_i} = \frac{1}{n}\sum_{j=1}^{n}(x_i(j) - \overline{x_i})^2 \tag{3.30}$$

The variance v is calculated by using only different variables in the archive. The factor f_s changes h function shape. If algorithm requires to enhance accuracy $fs>1$. If algorithm requires global search $fs<1$.

The variance and mean values are computed after the archive is filled up. Before that phase, s_{i1} and s_{i2} are equal to 0. This indicates a straight line between 1 and 0 for mapping function. Generally, size of the archive is selected between 5 and 2, for satisfactory results. Increasing the size of the archive causes more conservative convergence behavior. First position of the archive is reserved for the best solution reached so far. In the original MVMO algorithm, only best solution of the archive is used as parent solution to create new solutions. Variants of MVMO such as MVMOS (swarm variant) and MVMOSH (swarm hybrid variant) use multiple solutions as parents instead of using one [52]. After selecting parents, a few variables of parents are determined and updated by using mapping function. To determine variables to be updated, there are four different alternatives such as random selection, neighbor group selection (block step), neighbor group selection (single step) and sequential selection of the first variable then selection of the rest randomly [21]. General progress of MVMO algorithm is given below,

1. Initialization: Randomly initialize an initial solution vector x between 1 and 0, using uniform distribution
2. Fitness evaluation: Denormalize x, and evaluate the fitness function
3. Update archive: If x is better than any solution in the archive, store x in the archive and remove the worst one
4. Compute mean and variance: Based on updated archive
5. Parent assignment: Select parents to create new solutions
6. Variable selection: Select m variables of parents to update
7. Mutation: Apply the mapping function to the selected m variables of parents

8. Crossover: Set remaining variables to new solutions
9. Repeat steps 2 to 8 until, stopping criterion is achieved

3.3.7 Constraint Handling via Penalization

The optimization problems defined in this study includes large number of constraints, although the test systems involve limited number of generators and buses. For real, large sized power system, the number of constraints increases dramatically. Therefore, reaching the parameter space where feasible solutions are located becomes a challenge during optimization.

Constraint handling methods can be divided into four groups, such as rejection, repair, multi-objective optimization and penalizing [53]. In rejection method, infeasible solutions are directly eliminated from the solution set. This method has several disadvantages, especially if the initial solution set is completely infeasible. Some solutions with low objective function value and low violation can carry information about the problem eliminated in rejection method and this information is not used by the optimization. In repair method, problem dependent algorithm tried to repair infeasible solution and to move it into the feasible space. Development of the problem dependent algorithm may not be easy. Also, the algorithm needs considerable time to solve infeasibility. On the other hand, it may reach better results than optimization algorithm, but there is no clear conclusion so far. As third method, reformulating the problem as a multi-objective optimization problem where the objectives are real objective function and measures of constraint violation. The last method is penalizing that is used also in this study.

Penalizing is the most used method for dealing with infeasible solutions in population-based optimization methods. Constrained optimization problem becomes unconstrained by using penalty function. A penalty function *p(x)* can be added to the original objective function *f(x)*. This is the additive form of penalization, and the new objective function becomes,

$$e(x) = f(x) + p(x) \tag{3.31}$$

If solution x is feasible, the $p(x)$ will be zero. Second form of penalization is multiplicative, that multiply the objective function $f(x)$ with the function $p(x)$. If solution x is feasible, the $p(x)$ will be one. The new objective function becomes,

$$e(x) \ = f(x).p(x) \tag{3.32}$$

In this study, additive form of penalization is used which is the popular one in most applications.

A simple idea for penalization of infeasible solutions is to adding static (constant) penalty to these infeasible solutions. This method is called static penalization and the biggest drawback of this method is large number of parameters to be selected manually. As shown in [54], performance of this method is very susceptible to the selected parameters.

To discard the selection of large set of parameter, an adaptive penalization technique is used in this thesis [55]. This technique does not need parameter tuning and it has ability to set the penalized fitness function at different phase of the optimization. The fitness evaluation function is calculated as follows,

$$e(x) = d(x) + p(x) \tag{3.33}$$

where $p(x)$ is the penalty term and $d(x)$ is the distance term of candidate solution x, respectively. The distance term is,

$$d(x) = \begin{cases} v'(x) & if \quad r_f{=}0 \\ \sqrt{f'(x)^2 + v'(x)^2} & else \end{cases} \tag{3.34}$$

where r_f represents the feasibility rate of the population. If all solutions in the population are infeasible then $r_f{=}0$ and $d(x) = v'(x)$. $f'(x)$ represents the normalized value of the objective function such that,

$$f'(x) = \frac{f(x) - f_{min}}{f_{max} - f_{min}} \tag{3.35}$$

where $f(x)$ is the objective function value of solution vector x, f_{max} and f_{min} are maximum and minimum objective function values of all solutions in the population. $v'(x)$ in (3.34) is the normalized constraint violation such that,

$$v'(x) = \frac{v(x) - v_{min}}{v_{max} - v_{min}} \quad \textbf{(3.36)}$$

where v_{max} and v_{min} are maximum and minimum total constraint violation of all solutions in the population and *v(x)* is the total constraint violation of solution vector *x* which is computed as follows,

$$v(x) = \sum_{i=1}^{m+n} \max(0, g_i(x)) \quad \textbf{(3.37)}$$

where *m* and *n* are the number of equality and inequality constraints, respectively. $g(x)$ represents both inequality constraints and equality constraints, since all equality constraints are transformed to inequality constraints.

p(x) penalty function is used to provide proper fitness value for infeasible solutions in different phase of the optimization. For instance, first phase generally describes early iterations where populations involves only infeasible solutions ($r_f=0$). In this phase, violation is more important than objective function, thus infeasible solutions with low violations are subjected to less penalization than other solutions. In second phase, when algorithm starts to find feasible solutions beside infeasible ones, thus infeasible solutions with low objective function values are subjected to less penalization than infeasible solutions with high objective function values. This technique is formulated as follows,

$$p(x) = (1 - r_f)X(x) + r_f Y(x) \quad \textbf{(3.38)}$$

$$X(x) = \begin{cases} 0 & if \quad r_f = 0 \\ f'(x) & else \end{cases} \quad \textbf{(3.39)}$$

$$Y(x) = \begin{cases} 0 & if \ \ x \ is \ feasible \\ f'(x) & else \end{cases} \quad \textbf{(3.40)}$$

Third phase can be considered and latter iterations where all population consists of feasible individuals. Then, as seen from the equations, penalization action becomes passive because $v'(x) = 0$ and $p(x) = 0$. So, fitness evaluation function $e(x)$ equals to the objective functions $f(x)$ for all individuals.

4. DYNAMIC SECURITY ASSESSMENT BY ANN

4.1 Introduction

This section represents the proposed methodology to design ANN based DSA framework. From ANN point of view, DSA can be considered as a classification or regression problem. In the classification task, classifiers can classify the security status of the system on a particular OP as secure or insecure. On the other hand, in regression task, tools can estimate a security index that gives information about the vulnerability of the system against contingencies. For both tasks, designed ANN uses supervised learning algorithms for their training.

In supervised learning [56], ANN requires a knowledge base that includes different examples of the system behavior to be learned. The initial step of an ANN design is to generate the training data that includes meaningful instances. The ANN is trained by using the training data, so the data can be successfully approximated by the trained ANN structure. More importantly, if an input string is given to a well-trained ANN, expectation from ANN is imitating the output of the real system when the same input is given to the real system. Error is the difference between the outputs of the real system and ANN. Generally, mean squared error or mean absolute error values are minimized by using gradient descent techniques for MLP, which is the ANN type used for the regression task in this study.

The basic steps of ANN based DSA are given in Figure 4.1 Initial target of the methodology is generating the training data for learning process of ANN. To generate the training data, initial tasks must be completed for power system, such as contingency selection, determining the possible OPs of the system by considering loading levels and system topologies. Then a feature selection process is applied to reduce the dimension of input pattern of the KB and mitigate the curse of dimensionality problem, without losing too much information, which may also cause unsatisfactory assessment performance. The last step is training and optimizing the structure of ANN.

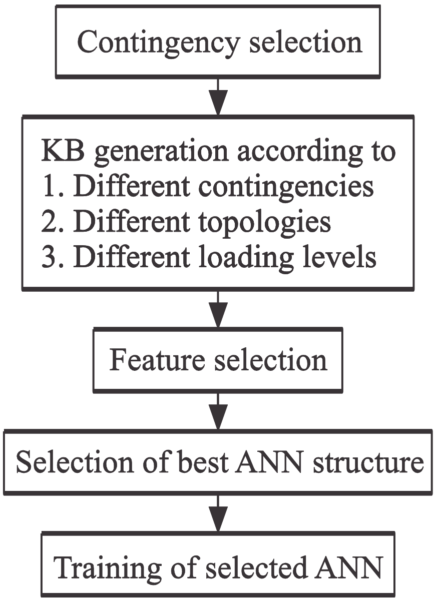


Figure 4.1 : Steps of ANN design for dynamic security assessment.

4.2 Methodology of ANN Approach

4.2.1 Contingency selection

Contingency selection has an important role on the security assessment of the power system. Large sized power systems include large number of components, which also means large number of contingencies for the system. Generally, not all of these contingencies cause overloading of transmission lines, bus voltage violations or instability problems for the current OPs of the system. During, security assessment and security enhancement procedures, considering all contingencies will significantly increases the computational burden and decrease the applicability of the methodology [3]. In this thesis, contingency selection is applied to determine the critical contingencies that have the potential to create transient instabilities that is considered as the main stability phenomena in this study. As mentioned in Section 1, contingencies could be faults, generator outages, line outages, load changes, voltage collapse or some combination of them. Faults and especially 3 phase-ground faults can be considered as more severe than other contingency types when dealing with transient instabilities. In this study, the critical contingencies considered in the test systems are 3-phase-ground faults that are cleared between 5 to 10 cycles after their occurrences by a single line tripping but causing transient instabilities based on the large disturbance angle stability index defined in (4.1).

$$\eta = \frac{360-\delta_{max}}{360+\delta_{max}} \qquad -100 < \eta < 100 \tag{4.1}$$

where δ_{max} is the maximum angle separation in degrees of any two generators at the same time in the post-fault response [57]. For a secure OP, the stability index must be positive when the system is subjected to each of the credible contingencies. A stability index based on critical clearing time (CCT), which is the maximum period to clear a fault before the system loses its stability [3], could also be used as a reliable indicator. However, the stability index in (4.1) is preferred for contingency selection procedure, since calculation of CCTs needs a significant computational effort. CCTs are used as an index in the KB generation section of the methodology.

In the first step of proposed methodology, the system is moved to stress OP by increasing the loading level. Next step includes extensive time domain simulations under possible contingencies. Each contingency is occurred individually in the system. The power flow computations, security assessment via time domain simulations and eigenvalue analysis are performed by the power system analysis software, DSATools^{TM} [58]. Alongside of the index in (4.1), separation of generators groups with respect to their angle behavior after the occurrence of contingencies is also important. For the sake of illustration, Figure 4.2 shows the time domain simulation results for the 16 generator-68 bus test system (Figure 4.3) subjected to 3 phase to ground fault on a transmission line between buses 23 and 24.

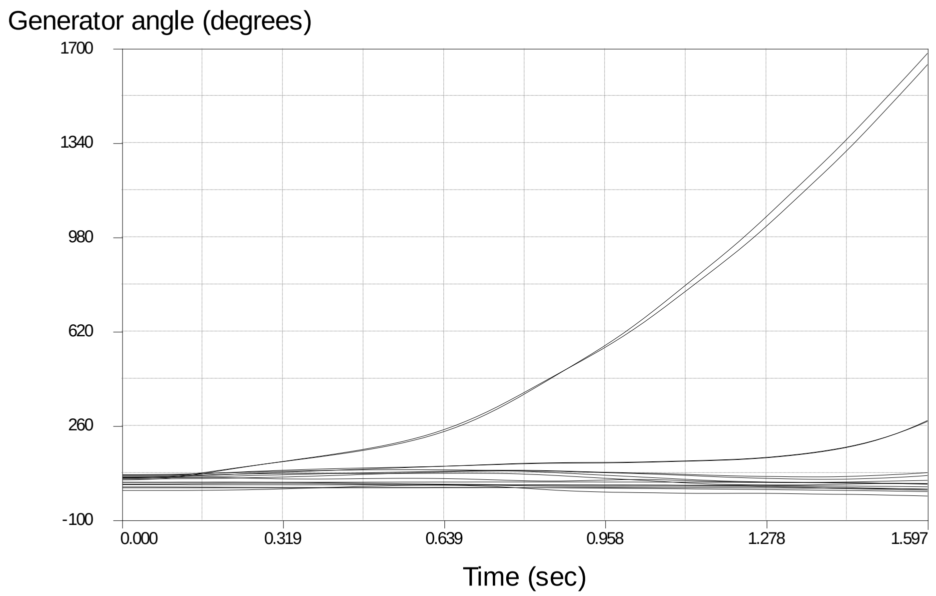


Figure 4.2 : Angular behavior of generators after the occurrence of a disturbance.

As seen from the Figure 4.2, selected contingency leads two groups of generators to accelerate and the angle separation of these generator groups start to increase dramatically. Therefore, this contingency is added to the list of critical contingencies.

In this section, the proposed methodology is applied on 16 generator-68 bus test system, which is taken from [28]. Table 4.1 lists the set of critical contingencies selected according to the criteria mentioned above.

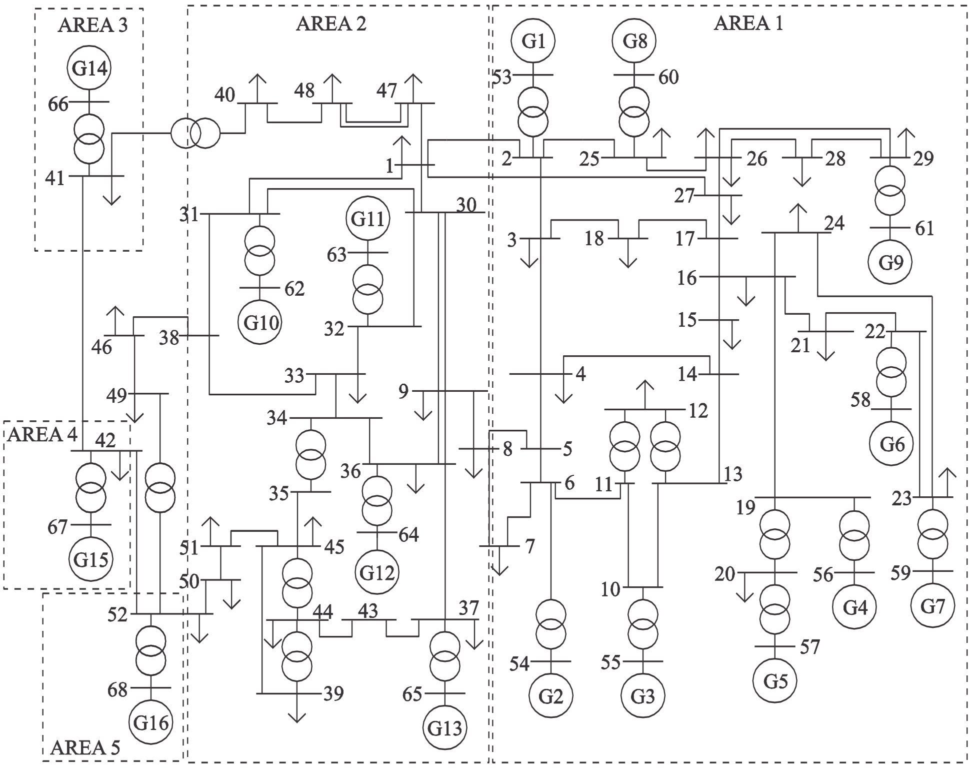


Figure 4.3 : 16 generator-68 bus test system [28].

Table 4.1 : Critical contingencies for 16-generator system.

Contingency no.	3-phase fault close to bus no.	Tripped line (between buses)
1	6	6-5
2	6	6-7
3	6	6-11
4	10	10-11
5	10	10-13
6	16	16-15
7	16	16-17
8	16	16-21
9	16	16-24
10	22	22-23
11	22	22-21
12	23	23-24

The critical contingencies, accelerating and decelerating generators with respect to these contingencies are located around two zones. These zones are inside one of the dynamically divided five areas of the test system. The critical contingency set obtained in this section significantly depends on the initially selected and stressed

OP. To study with the contingencies in the other areas of the system, the initial OP can be changed and contingencies can be scanned on new OP. This process is applied in Section 6.3 to investigate other contingencies in the system.

4.2.2 Creation of knowledge base

After the selection of critical contingencies that have the potential to create transient instabilities, a large set of OPs are created and all critical contingencies are applied to the power system operating on each OP individually. This knowledge base or training set is required for the supervised learning of ANN, but also can be used to investigate the relevant control variables that can be optimized during the optimization procedure. The security assessment tool to be designed should be sensitive to different operating conditions of the power system such as different topologies and different loading levels. Therefore, these changes are also considered when generating the training data. 45 different topological changes, which are either tripping of a line or a loss of a generator, are considered. For each topology, the OPs are computed randomly by using (4.2), such that the system's loading level is varied in the range of ±25% around a selected base case.

$$S_{L,i} = (P_{L,i}^{0} + jQ_{L,i}^{0})(1 + m(1 - 2r)) \qquad \textbf{(4.2)}$$

where $P_{L,i}^{0}$ and $Q_{L,i}^{0}$ represent the initial value of loads at *i*th bus, l indicates the loading level, *m=25%* is the allowed variation of loads and *r* is a random number generated by uniform distribution. For each OP, the power flow computations and DSA via time-domain simulations and eigenvalue analysis are performed. Generated KB involves 1500 instances. The word "feature" means a quantity that represents each instance. In this study, instances are OPs and each one is represented by totally 377 features (measurements) such as active and reactive power outputs of each generator, active and reactive power flows at each transmission line, magnitude and phase angle of the bus voltages, active and reactive power demands at all load buses, and stability index values. For the small disturbance angle stability, minimum damping value for the most critical oscillatory mode is computed by modal analysis. After the linearization of nonlinear equations of the system model, eigenvalues of the system matrix *A* are computed. If the real part of the eigenvalue is positive, the amplitude of the oscillations tends to increase and this represents instability. On the other hand, negative real eigenvalues mean asymptotic stability and damping of the oscillations. The critical eigenvalues are located close to the imaginary axis (still negative but near zero). Minimum damping ratio (MDR) of the most critical oscillatory mode is calculated as follows,

$$\xi = \frac{-\sigma}{\sqrt{\sigma^2+w^2}} \qquad \textbf{(4.3)}$$

where σ and w are the real and imaginary parts of the critical eigenvalues, respectively. For the large disturbance angle stability, CCT value for each critical contingency are computed by using time domain simulations. CCT can be defined as the maximum period to clear a fault before the system loses its stability. For the sake of illustration, CCT values of all contingencies for some selected instances (OPs) are given in Figure 4.4. To show the effects of loading level and different topologies only 100 instances are shown in the Figure 4.4. These instances represent 3 different system topologies (generator or line outage) and different loading levels. Each different colored circle represents CCT values for contingency. In each system topology, loading level increases with the instance number and this leads CCT values to decrease. On the other hand, it can be seen that, the range of CCT values for different system topologies may differ according to the importance of component that is removed from the system.

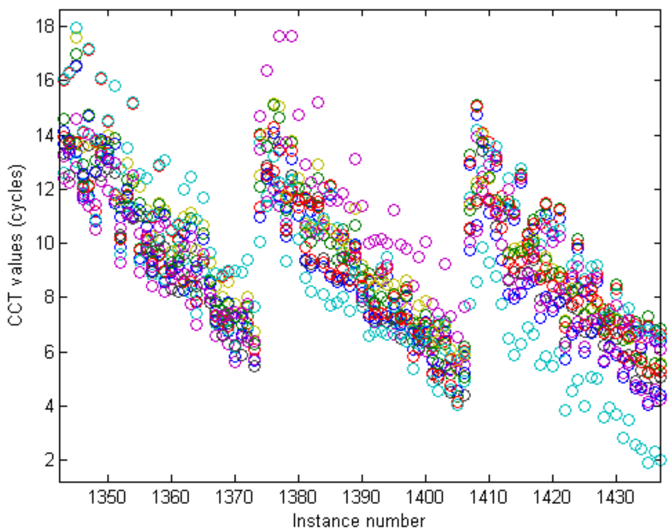


Figure 4.4 : CCT values for all contingencies and selected instances in the KB.

Measurements collected from power flow solutions can be used for small signal stability assessment but these variables cannot completely represent the dynamic behavior of the power system for the estimation of CCT. To characterize the effect of inertia of generators on angle stability, a factor called Power Generation Distribution Factors (PGDF) are determined, and calculated as follows [59],

$$PGDF_j = \frac{\sum_{i=1}^{N_j} H_i P_{gi}}{\sum_{i=1}^{N_j} H_i S_{gi}} \quad \textbf{(4.4)}$$

where H_i represent the inertia constant of ith synchronous generator. P_{gi} and S_{gi} represent the generated active power and capacity of ith generator. N_j is the number of generators in kth area. This variable also characterizes the effect of inertia of generators which is important for rotor angle stability. Results of feature selection algorithm in Section 5 demonstrate if this new defined feature is relevant or not.

4.2.3 Feature selection

In power systems, complete state information is very large. Even, the training set generated for the 16-generator test system involves more than 350 features. This high dimensional data involves features that are irrelevant to the dynamic behavior of the system under selected critical contingencies. On the other hand, there are large numbers of highly correlated features and existence of most of these features does not increase the valuable information obtained from the data. This high degree of irrelevant and redundant information will decrease the learning performance of the computational intelligence tool. Therefore, dimension of the data should be reduced and dimensionality reduction task can be classified such as “feature selection” and “feature extraction”.

In feature selection task, input information is described by using selected subset of initial big feature set, and rests of the features are eliminated. Differently, feature extraction techniques transform the big feature set into a smaller new set in a different space that holds acceptable level of relevant information on the original feature set.

In this study, ANN based DSA tool is used in both optimization of control actions and security assessment. All features can be collected from the simulation program. In this study, feature selection methodology is used to determine a subset of relevant features to describe the dynamic behavior of the system and it is assumed that these selected featured are available. To increase the actability of this assumption, ranking based feature selection is used. In feature ranking, features ranked by predetermined score. Minimum number of ranked best features that are selected for the input pattern on ANN while ensuring acceptable level of estimation accuracy.

If the DSA is considered as a classification problem, targets would be discrete variables and feature selection methods such as information gain [60], Gini index [61], distance measure [62], j-measure [63], Relief [64], ReliefF [65], MDL [66] can be used. In regression tasks where target values are continuous variables, RReliefF [67] method which is the modified Relief for regression tasks is applied for feature selection.

In this study, RReliefF method is used for feature selection process on regression tasks. RReliefF is the extension (regression) version of Relief that can estimate the quality of features in classification problems where features have strong dependencies each other. The studies on real and artificial data show that RReliefF can also estimates the quality of features in various conditions, and can be used for learning of MLP.

Main idea of Relief is estimating the quality of features with respect to how good their values separate from the instances near to each other [64]. Input of the algorithm is a vector of feature values and the class value for each instance and the output of the algorithm is W vector of estimations of the feature quality. Steps of Relief algorithm as follows [64],

1. Set all $W(f) = 0$
2. Randomly select an instance R
3. Find H (nearest hit) and M (nearest miss)
4. Calculate $W(f)$ for all features
5. Repeat steps 2 to 4 for m times

Algorithm starts with initialization of vector W. Then, for randomly selected instance R, algorithm searches nearest neighbor from same class (nearest hit, H) and nearest neighbor from other class (nearest miss, M). In the next step, quality of estimation is calculated for all features as follows,

$$W(f) = W(f) - \frac{diff(f,R,H)}{m} + \frac{diff(f,R,M)}{m} \quad \textbf{(4.5)}$$

where m is defined by user and determine the how many times $W(f)$ is updated. The diff(feature, Instance1, Instance2) function computes the difference between the values of feature for Instance1 and Instance2. For features with continuous values, the function is defined as,

$$diff(f, I_1, I_2) = \frac{|value(f,I_1) - value(f,I_2)|}{\max(\mathrm{f}) - \min(f)} \tag{4.6}$$

This function is also used to compute the distance between instances to find nearest neighbors. The sum of distance over all features is the total distance. *W(f)* estimation of the feature quality is an approximation of the following probability differences [65], such that,

$$W(f) = P(different\ value\ of\ f \mid nearest\ instance\ from\ different\ class) - P(different\ value\ of\ f \mid nearest\ instance\ from\ same\ class) \tag{4.7}$$

In regression tasks, there is no class and all predicted values are continuous. Thus, nearest hits and nearest misses cannot be found. To solve that problem, RreliefF proposes a probability that the predicted values of two instances are different [68]. This probability is computed by using the relative distance between predicted values of two instances. The sign of each contributed term is still missing to calculate *W(f)*. So, (4.7) is reformulated as follows

$$P_{diff,f} = P(different\ value\ of\ f \mid nearest\ instances) \tag{4.8}$$

$$P_{diff,c} = P(different\ prediction \mid nearest\ instances) \tag{4.9}$$

$$P_{diff,c \mid diff,f} = P(different\ prediction \mid different\ value\ of\ f\ and\ nearest\ instances) \tag{4.10}$$

and it can be evaluated by using the probability of the predicted values of two instances being different. Finally, *W(f)* is computed as follows,

$$W(f) = \frac{P_{diff,c \mid diff,f}\, P_{diff,f}}{P_{diff,c}} - \frac{(1 - P_{diff,c \mid diff,f})\, P_{diff,f}}{1 - P_{diff,c}} \tag{4.11}$$

In this study, 12 different ANNs are designed for CCT values of 12 critical contingencies. In addition, one ANN is designed for small signal stability assessment by estimating the minimum damping ratio for the most critical mode. Thus, feature selection process is repeated for 13 times and totally 377 features are ranked by considering each 13 target values of ANNs.

Due to the size of the tables, results of feature ranking and selection are given in Appendix A. Features are ranked with respect to their *W* values. When most relevant 30 features according to the transient stability of the system against 1st critical contingency are examined from Appendix A, it is seen that, most of these selected features are active and reactive power flows through the transmission lines, which are topologically closer to the location where 1st critical contingency occur (Figure 4.3). Therefore, redesigning these power flow patterns by preventive control actions can enhance the security of the system against related contingency. In addition, power generation of synchronous machines at buses 54 and 55, are selected as significant features by RReliefF algorithm. These machines are the closest generators to the contingency location, and rescheduling of the generation of these machines can directly change the mentioned power flow patterns. Therefore, this generation rescheduling action has the biggest impact on chancing security of the system for mentioned contingency. Finally, PGDF value for the area no. 1 of the system takes the 14th place between 377 features. This results show that, PGDF values based on the inertia constant of generators and their loading levels can be used as an additional indicator for transient stability of the system. Feature selection results mentioned above are similar to the other eleven critical contingencies. These expected results confirm the success of RReliefF based feature selection and suitability of generation rescheduling as a preventive control action.

According to the feature selection results for the small signal stability of the system in Appendix A, damping ratio for the most critical oscillatory mode is related with the power flow patterns mostly in area no. 2 of the system, where generators 10 to 13 are located in. Therefore, generators in other areas are also considered for generation rescheduling action to enhance the dynamic security of the system according to large disturbance angle stability.

4.2.4 Design and training of ANN

For nonlinear mapping problems, MLP of feed-forward neural network is generally used. Proposed MLP structure involves several parameters to be selected and optimized, such as size of output layer, number of hidden layers, type of activation functions used in hidden layers and output layer, training algorithms, learning algorithm for weight and bias update, size of the input layer (number of input features) and size of the hidden layer (number of hidden neurons).

Each ANN estimates CCT value of particular contingency, so the size of the output layer is 1. Hidden layers allow ANN to find complex relationship between inputs and outputs. Using hidden layer is necessary for successful mapping of highly nonlinear functions like power system dynamics, but using 2 or more hidden layers dramatically increase the complexity of ANN and can decrease the performance of ANN. In this study, using one hidden layer ensures ANN to represent the dynamic behavior of the power system.

As explained in Section 2, ANN structure is trained by the Back propagation training algorithm based on Levenberg-Marquardt optimization. Using Back propagation training algorithm requires differentiable activation functions. In addition, by considering the range of the values of possible input features, Tangent-Sigmoid transfer function is selected for the hidden neurons. In this study, the expected output values of ANNs are CCTs of contingencies and the minimum damping ratio. These values vary between 0 and 20. By considering that range, the activation function on the output layer is selected linear. As a learning algorithm, gradient descent based optimization method is used to minimize the error and update weights and bias values.

In this study, the number of input features and number of hidden neurons are the parameters to be adjusted for optimizing the ANN structure. Increasing hidden neuron number always increases the training performance of ANN, but after one point test performance of ANN stops increasing. Hidden neurons let ANN to learn training data in a more detailed way, which causes also learning noises. When overlearned ANN tries to map unseen test data which includes different instances, performance on estimating the unseen data may not be as good its training performance. This problem is called over fitting. To determine the best number of hidden neurons and input features, k-fold cross validation method is applied to investigate performance of different combinations of number of hidden neuron and input features.

The performance of different MLP structures on estimating the CCT and minimum damping ratio are evaluated by the calculation of mean absolute error (MAE). In this study, root mean square error (RMSE) is not preferred, because error values calculated for the estimations of CCT and damping ratio are smaller than 1.

$$MAE = \frac{1}{N_t}\sum_{i=1}^{N_t}|y_i^* - y_i| \qquad \textbf{(4.12)}$$

where y_i and y_i^* are the real and estimated output values respectively, and N_t is the number of instances in the test or train set.

Proposed training methodology is given in Figure 4.5. In the first phase, 20% of KB is stored as an unseen data for evaluation of testing performance. Then, the rest of the KB is prepared for the k-fold validation process in the second phase. k-fold cross validation is one of the non-exhaustive cross validation methods. The method, randomly partition the KB into *k* subsamples with equal size. One subsample is selected as the validation data, and the remaining *k−1* subsamples are used for training. This process is repeated *k* times and each time selected validation subsample is changed. The strong side of this technique is using all observations for both validation and training. Also, each observation is used for validation once [69]. During the k-fold cross validation, MAE value for each validation set of fold is stored and the average of *k* MAE values are calculated as,

$$MMAE_{h,n} = \frac{1}{k}\sum_{i=1}^{k} MAE_{i,h,n} \qquad \textbf{(4.13)}$$

where *h* is the number of hidden neuron and *n* is the number of input feature. MMAE values are calculated for various MLP structures with all combinations of *h* and *n*.

In the third phase, best number of hidden neurons for various MLP structures with different number of input feature are determined according to (4.13). Then, the best MMAE values of MLP structures with different number of input features are compared to determine the best MLP structure. The best MLP structure is trained with 80% of KB which is previously used in k-fold cross validation, where *k* is selected 10. Then test set performance of MLPs are calculated by using the unseen test set (20% of KB), which is stored in the beginning of the first phase.

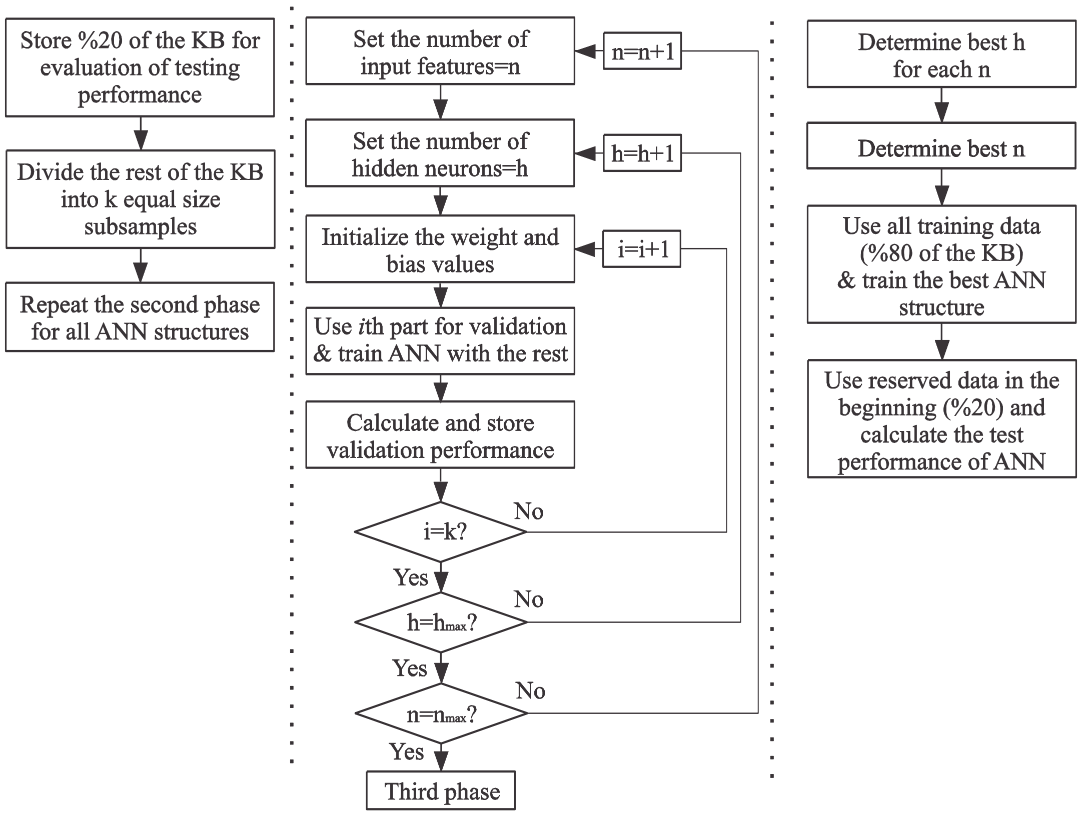


Figure 4.5 : Methodology for the design of MLP.

4.3 Results for ANN Based Dynamic Security Assessment

The results of the methodology applied for the design and training process of CCT estimator MLPs is given and discussed in this section. In the second phase shown in Figure 4.5, the number of input features are *n=6,9,12,15,18,21,27,33,39,45,51,57* and number of hidden neurons varies between 1 and 15. Increasing the number of hidden neurons may enhance the training performance but the risk of overfitting problem also increases as explained in previous section. If number of input features is increased, MLP performance may enhanced for some contingencies. The reason of stopping the number of input features at 57 is that, designed MLP is also used for online DSA application and the number of (real-time) measurements can be collected from the system is limited by the number and location of PMUs. In Figures 4.6 and 4.7, performance of MLPs designed to estimate CCT values of 12 contingencies are given. Figures show minimum $MMAE_{h,n}$ value achieved by best hidden neuron number, for each selected number of input features. Best hidden neuron numbers are indicated near each dot that represents the error value for each number of input feature.

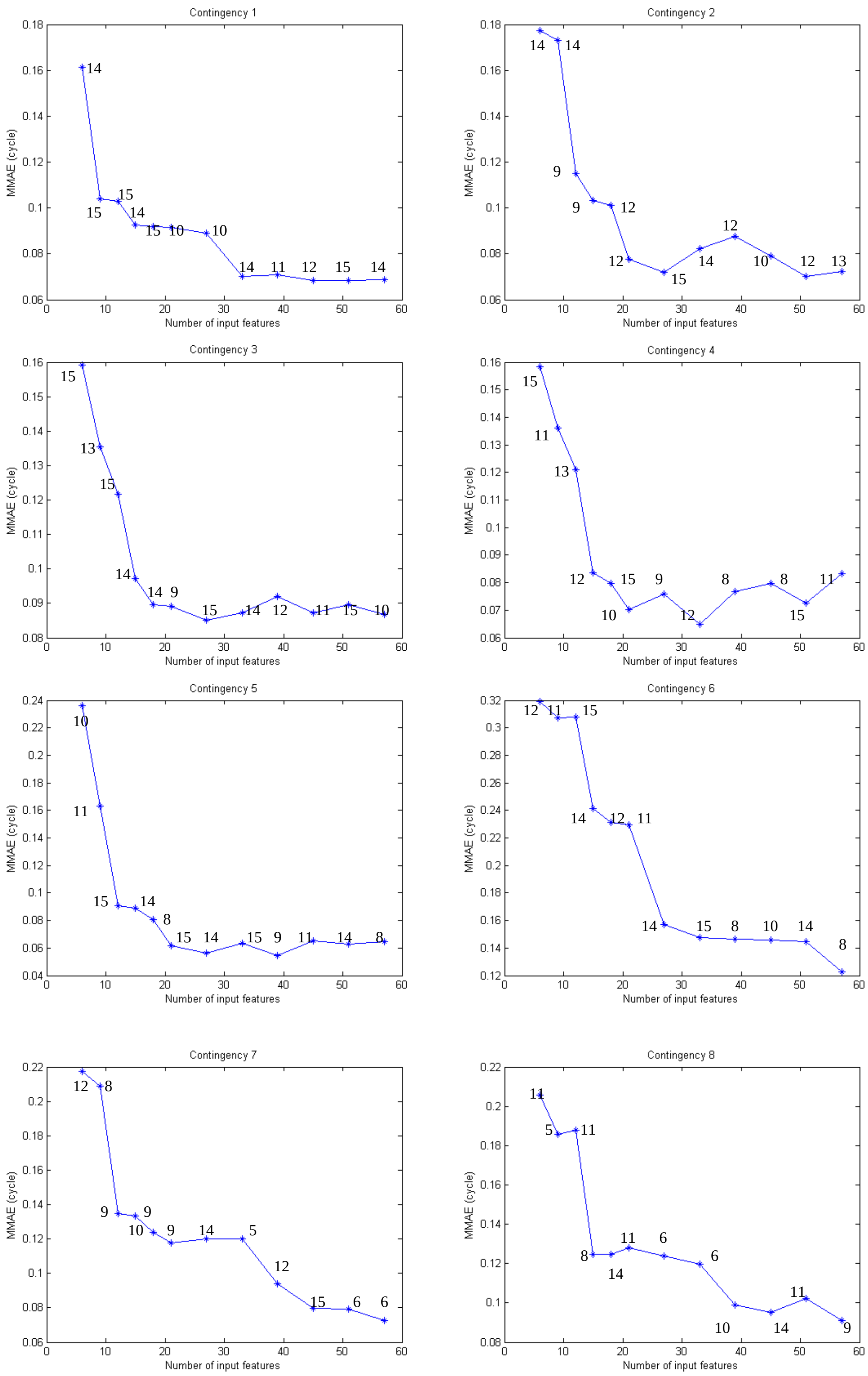


Figure 4.6 : Performance of CCT estimator MLPs (contingency 1-8) with different number of input features.

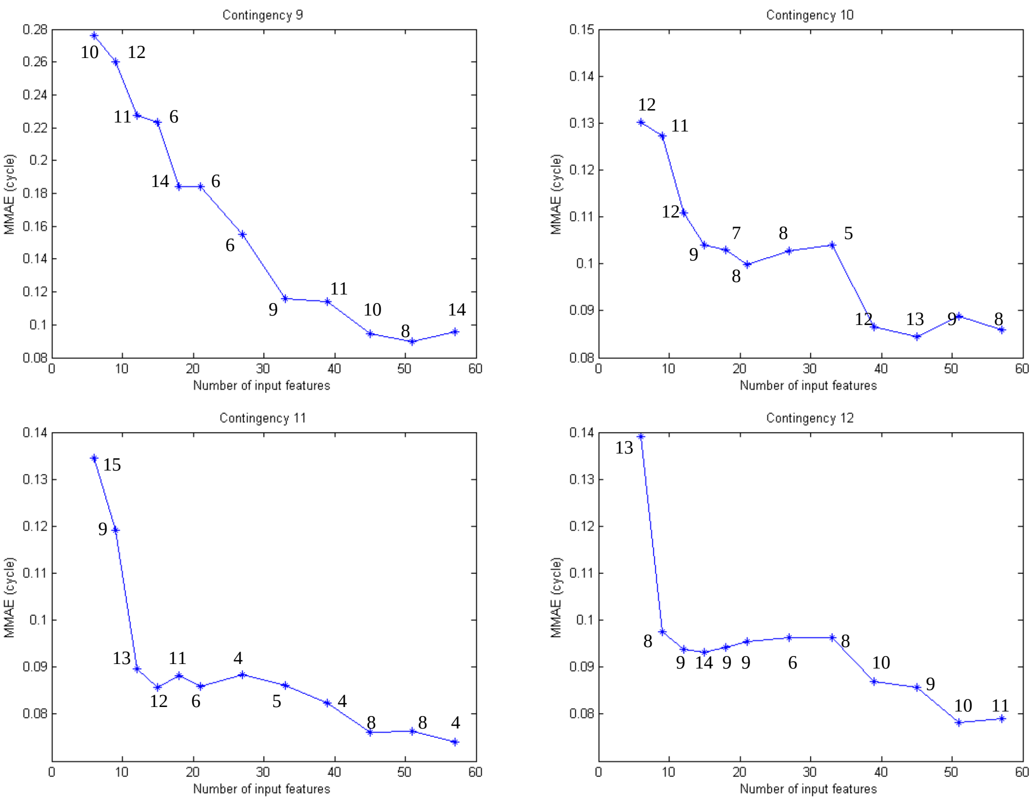


Figure 4.7 : Performance of CCT estimator MLPs (contingency 9-12) with different number of input features.

As seen from Figures 4.6 and 4.7, in most cases, there is an appreciable enhancement on MLP performance when the number of input features increases to 33. For some contingencies such as 6 to 12, performance of MLP still enhance when we continue to increase the number of features. Average validation error for best MLP structures for all contingencies is approximately 0.08 cycles. Worst performance is achieved on estimating the CCT of contingency 6, since Figure 4.6 shows that, increasing the number of input features may enhance the performance on estimating CCT value of contingency 6.

After the best MLP structures are determined, they are trained by using the same data used in k-fold cross validation (80% of KB). This time, the data is divided into two parts such as training (60% of KB) and validation (20% of KB). The remaining (unseen 20%) KB is used for testing. In second phase of the methodology, the validation set is used to find optimum MLP structure. In the third phase, the validation set is used to prevent overfitting problem.

It is clear that, the gradient-based optimization algorithms used in the training process of MLP converge to local minimum, because their performance is significantly depends on the starting point (initial weight set of MLP). To increase the testing performance of MLP, the final training process is repeated 10 times, by initializing the weight set with different values in each try. Best weight set of 10 training is stored to be use in MLP. This method, does not guarantee to achieve the global best weight set, but it ensures to use a better weight set than a set achieved just one training try.

For each contingency, the parameters of best MLP structures, performances on k-fold cross validation set and test set are given in Table 4.2. The reason of better results on test set is multiple tries on the third phase, as explained in previous paragraph. This multiple tries is not is not necessary and not applied during the k-fold cross validation, because the reason of using k-fold cross validation is comparing different MLP structures, not improving the best one. $PMAE_{test,best}$ in Table 4.2 is the mean absolute error value in percentage which is computed for best MLP structures, using test set.

$$PMAE_{test,best}(\%) = \frac{100}{N_{test}} \sum_{i=1}^{N_{test}} \frac{|y_i^* - y_i|}{y_i} \quad \textbf{(4.14)}$$

where y_i and y_i^* are the CCT values calculated by DSAToolsTM and estimated by MLP respectively. N_{test} is the number of instances in the test set.

Table 4.2 : Parameters and performance of best CCT estimator MLPs.

Contingency	n_{best}	h_{best}	$MAE_{test,best}$	$PMAE_{test,best}$
1	45	12	0.0489	0.5718
2	27	15	0.0645	0.7078
3	27	15	0.0702	0.7987
4	33	12	0.0585	0.6575
5	39	9	0.0397	0.4767
6	57	8	0.1150	1.4648
7	57	6	0.0687	0.9387
8	57	9	0.0904	1.3742
9	51	8	0.0837	1.0512
10	45	13	0.0753	0.9916
11	45	8	0.0628	1.6123
12	51	10	0.0640	0.9809

Scatter diagrams for calculated CCT values by time domain simulations and estimated CCT values by MLP are given in Figures 4.8 and 4.9.

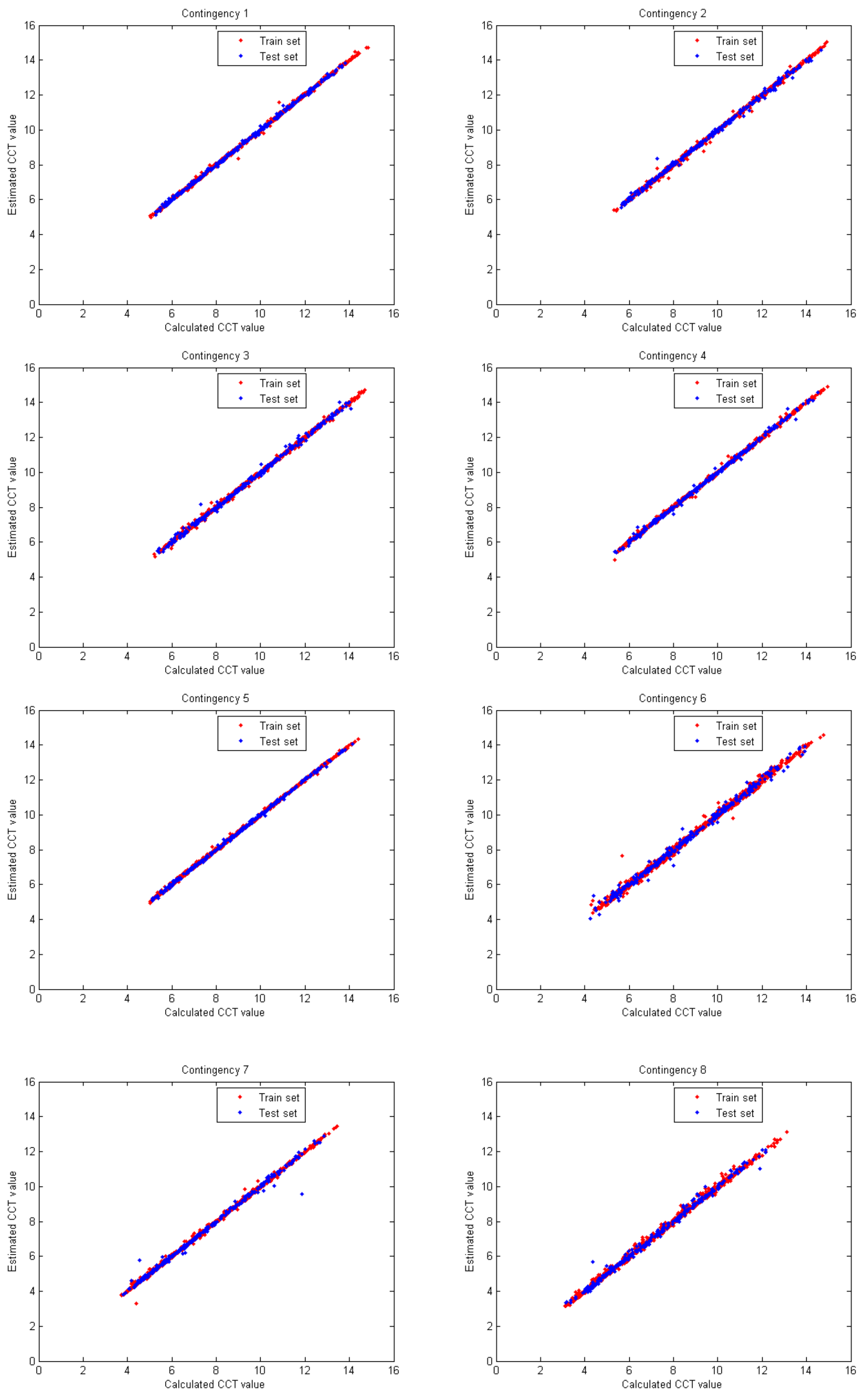


Figure 4.8 : Scatter diagrams for calculated and estimated CCT values (contingencies 1 to 8) by TDS and MLP respectively.

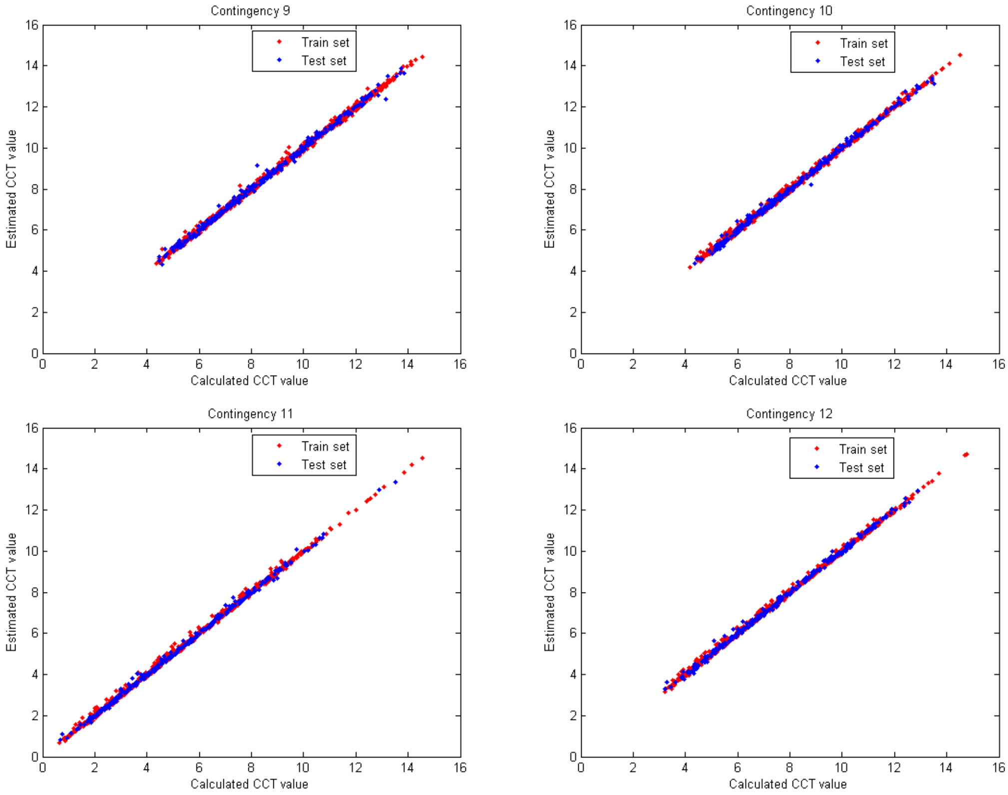


Figure 4.9 : Scatter diagrams for calculated and estimated CCT values (contingencies 9 to 12) by TDS and MLP respectively.

Same methodology is applied to design structure of MLP to estimate the minimum damping ratio for the most critical mode (small disturbance rotor angle stability). The only difference is that, number of input features changes from 6 to 57 by fixed step size 6. According to Figure 4.10, validation performance of MLP is enhanced with the increasing number of input features. For determined MLP structure, test performance of MLP and scatter diagrams are given in Table 4.3 and Figure 4.11, respectively.

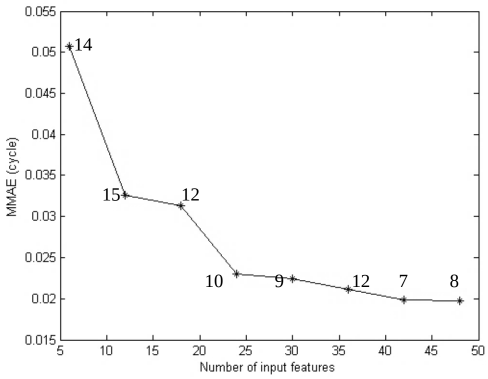


Figure 4.10 : Performance of damping ratio estimator MLP with different number of input features.

Table 4.3 : Parameters and performance of best MDR estimator MLPs.

n_{best}	h_{best}	$MAE_{test,best}$	$MAE_{test,best}$ (%)
48	8	0.021	0.5034

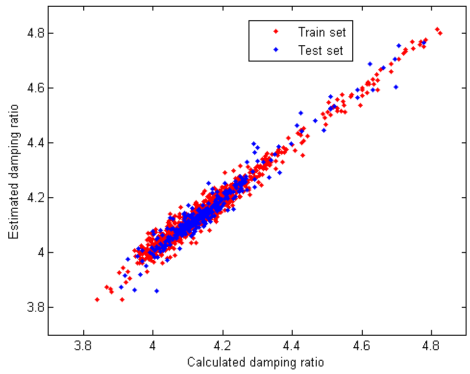


Figure 4.11 : Scatter diagram for calculated and estimated damping ratios by modal analysis and MLP respectively.

Performance of MLP on estimating CCT values and minimum damping ratio are promising. When considering all cases, average of PMAE is approximately 1%. As seen from Figures 4.6, 4.7 and 4.10, approximately 30 measurements can be enough to get satisfactory results in most of cases. Scatter diagrams in Figure 4.8, 4.9 and 4.11 shows that, train and test data have some instances, which are not well recognized by the MLP, but the number of these instances are considerably low, and most of them are away from the security threshold which is the clearing time of related circuit breaker.

The possible OPs of 16-generator power system (instances of KB) generally have large disturbance angle stability problems for defined critical contingency list, and most these OPs do not have small disturbance angle stability problem. Since small disturbance angle stability is also one of the constraints of the optimization problem, one MLP structure is designed to estimate the minimum damping ratio of most critical system mode. Results show that damping ratio estimator MLP can be used during the optimization.

5. DYNAMIC SECURITY ENHANCEMENT

5.1 Introduction

In this section, a method that combines both generation rescheduling and load curtailment approaches has been proposed as a preventive control to restore the security of the system. While restoring the security against transient instabilities, the other static security constraints related to voltage regulation, thermal and capacity limits of equipment are also considered. Within the security region constrained by both dynamic and static security limits, the power generation and consumption in the system is rescheduled such that a cost that is a function of generation and consumption rescheduling is optimized. Thus, the preventive control is designed through the formulation and solution of a security constrained optimization problem

5.2 Optimization Problem

5.2.1 Control variables

Most critical constraints of the optimization problem are based on large and small disturbance angle stability. Therefore, preferential control variables are selected to make candidate solutions to satisfy these constraints first. Angle stability of the system is sensitive to the active power flows through the transmission lines, especially tie lines between areas. In this study, the active power flows are adjusted by changing the location of injected active power to the system and also consumed active power from the system. These methods are called generation rescheduling and load curtailment, respectively.

From the generation rescheduling side, the power system can be deregulated, and market based organization can limit this control action by predetermined contracts. To increase the flexibility of changing the active power flow, load curtailment action can be applied from the consumer side, but this control action is also limited with the amount of intelligent load that can be curtailed in the system.

On the other hand, using these methods can violate some other constraints of the optimization problem, such as steady state voltage limits of each bus. For generation buses, the magnitudes of the bus voltages are controlled by AVR that adjust the reactive power generation of generators. For the other bus voltages, transformers with tap changers are used. This adds discrete control variables to optimization problem. The solution vector x for any candidate solution of this optimization problem is defined as,

$$x = \begin{bmatrix} \Delta P_G & \Delta P_L & \Delta T_{Tap} \end{bmatrix} \tag{5.1}$$

where ΔP_G and ΔP_L are change in the active power of generation and consumption of generators and loads, respectively. Within these continuous control variables, ΔT_{Tap} represents the change in tap position of transformers as discrete control variables.

Level of impact of generation shifting among different groups of generators on the system's security may differ. Therefore, system can be moved to a secure OP by rescheduling only the relevant generators. This will reduce the size of the search space, complexity of the optimization problem and also value of the cost function to be minimized. In Section 6, feature selection methods are applied to select generators relevant to the security of the system, but in this section, all 16 generators are considered to be rescheduled and results of optimization methods are discussed. In the solution vector, 15 of these generators are represented, because one of these generators (bus no. 65) is defined as dependent (slack bus). The power generation of this generator is determined by the power flow calculations.

As seen from the feature selection results in Appendix A, most features relevant to CCT value of each contingency, are collected close to the transmission lines where contingency occurs. Therefore, eight load buses close to these contingency locations are determined for curtailment process during optimization. It is assumed that, approximately 10% of total loads in these load buses are available for curtailment. Similar to selection of relevant generators, feature selection methods are applied to determine most relevant loads to be selected, in Section 6. One difference is, in Section 6, selected loads are used in load shedding control action, but in this section, these 8 loads are used for load curtailment.

Figure 5.1 shows the location of control variables and critical contingencies in the system model. Total number of continuous control variables is 23 and the number of transformer tap changers in the system is 19. Therefore, the size of the search space and the length of the solution vector of candidate solution are 42. Size of the search space affects the selection of some important parameters of the optimization methods.

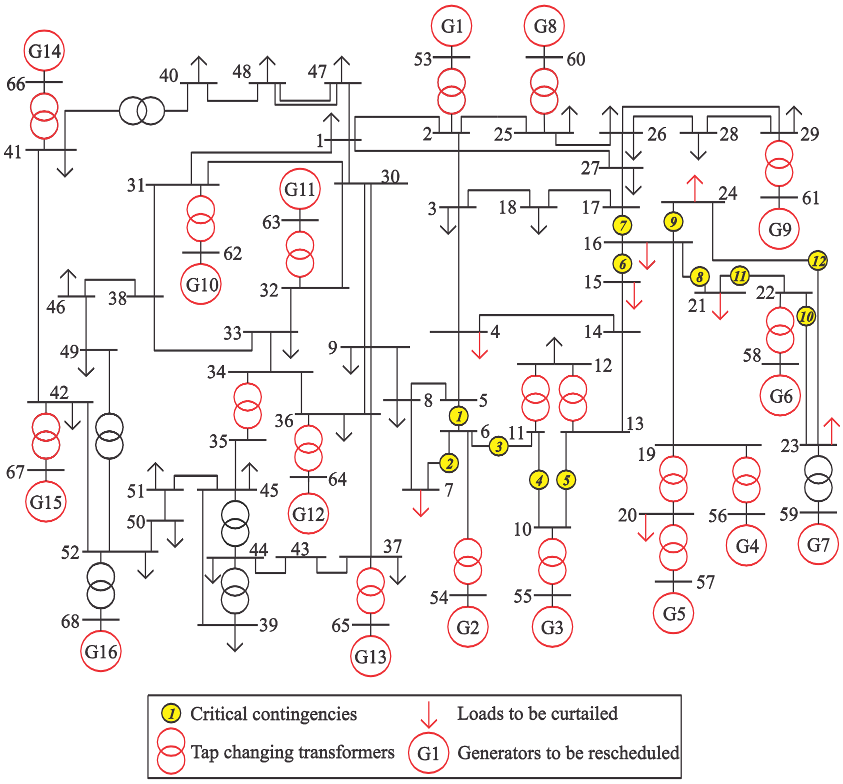


Figure 5.1 : Location of control variables and critical contingencies in the 16-generator, 68-bus system model.

5.2.2 Objective function

The objective of the optimization is adjusting the OP by increasing or decreasing the energy of participants (consumers and suppliers), for enhancing the dynamic security of the system, considering predetermined system constraints. For satisfying the security constraints, when energy of any participant is reduced, opportunity cost for reduction in consumption or generation should be paid to these participants. On the other hand, if system operator increases the energy of any suppliers, additional cost for increasing the generation should be paid to the suppliers.

The problem is formulated as cost minimization objective function. Optimization methods try to minimize the extra payment (opportunity and additional costs). It is assumed that opportunity costs and additional costs are required for participant's active power rescheduling and no cost is defined for other control variables such as transformer tap-settings and rescheduling of reactive power sources. However, the cost function can be extended with additional cost associated with other control variables. The cost function based on opportunity and additional costs for active power change can be formulated as,

$$f(x,u) = \sum_{i=1}^{N} a_i \Delta P_i^+ + b_i (\Delta P_i^+)^2 + \sum_{i=1}^{N} c_i \Delta P_i^- + d_i (\Delta P_i^-)^2 \qquad \textbf{(5.2)}$$

where *a*, *b*, *c* and *d* are the cost coefficients for change in the generation or consumption value of *N* participants in the market (Table 5.1).

Table 5.1 : Parameters of *f(x,u)* for controlled generators to and loads.

Component name	a ($/MWh)	b ($/MW^{2}h)	c ($/MWh)	d ($/MW^{2}h)	ΔP_{max} (MW)	ΔP_{min} (MW)
Gen. 1	5	0.154	5	0.3	56.429	-56.429
Gen. 2	3	0.156	2.7	0.12	118.08	-118.08
Gen. 3	2.5	0.146	2.5	0.14	151.68	-151.68
Gen. 4	3	0.132	2.1	0.13	132.1	-132.1
Gen. 5	3.9	0.158	2.9	0.21	116.08	-116.08
Gen. 6	4	0.17	3.8	0.22	165.15	-165.15
Gen. 7	2.5	0.163	4	0.29	134.25	-134.25
Gen. 8	4.3	0.144	3.5	0.23	126.09	-126.09
Gen. 9	3	0.102	2.7	0.21	183.06	-183.06
Gen. 10	4.3	0.276	2.7	0.17	112.56	-112.56
Gen. 11	2.8	0.258	2.2	0.14	217.2	-217.2
Gen. 12	3.6	0.162	2.3	0.16	285.05	-285.05
Gen. 13	4.2	0.364	4.4	0.28	422.1	-422.1
Gen. 14	4.28	0.158	3.28	0.29	404.97	-404.97
Gen. 15	4.56	0.156	2.56	0.13	237.26	-237.26
Gen. 16	3	0.15	2.5	0.15	650.84	-650.84
Load 1	11.2	0.21	9.5	0.32	0	-53.299
Load 2	10.3	0.284	7.6	0.27	0	-25.636
Load 3	12.5	0.265	9.1	0.28	0	-33.403
Load 4	9	0.215	8	0.39	0	-38.832
Load 5	12.9	0.212	7.7	0.29	0	-79.634
Load 6	13	0.289	8.5	0.26	0	-29.355
Load 7	10.8	0.224	8.3	0.28	0	-27.605
Load 8	12.1	0.253	8.8	0.31	0	-34.356

5.2.3 Constraints and penalty functions

As mentioned in Section 3.4, defined optimization problem involves large number of equality and inequality constraints. Power flow equations are the only equality constraints in this problem. Assume that $U_i e_i^{j\theta_i}$ is the complex form of the voltage value at *i*th bus. Then, active and reactive power flow equations for all buses are calculated as below,

$$P_{Gi} - P_{Li} - U_i \sum_{j=1}^{N} U_j \, Y_{ij} \cos\left(\theta_i - \theta_j - \delta_{ij}\right) = 0 \qquad \textbf{(5.3)}$$

$$Q_{Gi} - Q_{Li} - U_i \sum_{j=1}^{N} U_j \, Y_{ij} \sin\left(\theta_i - \theta_j - \delta_{ij}\right) = 0 \qquad \textbf{(5.4)}$$

where P_{Gi} and Q_{Gi} represent the active and reactive power generation at *i*th bus, respectively. P_{Li} and Q_{Li} are active and reactive power consumption at *i*th bus, respectively. Y_{ij} is the value of *i*th row and *j*th column of admittance matrix. δ_{ij} is the phase angle between the *i*th and *j*th buses where total number of buses is N. Also,

$$\sum_{i=1}^{N_G} P_{Gi} = \sum_{k=1}^{N_L} P_{Lk} + P_{Loss} \qquad \textbf{(5.5)}$$

where N_G and N_L represent the total number of generators and loads, respectively. P_{loss} is the total active power losses in overall transmission lines. If power flow equations cannot be satisfied for any individuals, biggest penalization will be applied for related individual of the population.

Steady state voltage values of each bus should be maintained with an acceptable range as follows,

$$|U_i|_{min} < |U_i| < |U_i|_{max} \qquad \textbf{(5.6)}$$

where $|U_i|_{min}$ and $|U_i|_{max}$ are lower and upper limits for *i*th bus voltages. Thermal limits can be defined as the maximum amount of electrical power flows through the transmission lines without overheating such as,

$$\left|S_{ij}\right| < \left|S_{ij}\right|_{th} \qquad \textbf{(5.7)}$$

where $\left|S_{ij}\right|$ represents the apparent power transferred between *i*th bus and *j*th bus and $\left|S_{ij}\right|_{th}$ is the thermal limit of the line between these buses. Generally, this criterion is not achieved, because angle stability constraints are more conservative than thermal limits and stability constraints limit the transferred power through the line with value lower than thermal limits. Transient stability constraint is based on CCT of each critical contingency, and the inequality constraint is defined as,

$$CT_m < CCT_m \quad \textbf{(5.8)}$$

where CCT_m is the critical clearing time for *m*th contingency, and CT_m is the clearing time of the curciut breakers located on the transmission line where the *m*th contingency occurs. Small signal stability constraint is based on damping of the most critical mode,

$$\xi_{min} < \xi \quad \textbf{(5.9)}$$

where ξ is the minimum damping ratio of the most critical mode for the current OP, and $\xi_{min}$is the minimum lower limit, which is selected %4 in this study. The penalty function for the infeasible solutions is the weighted sum of violations of inequality constraints given between (5.6) and (5.9),

$$p(x,u) = w_1 \sum_{i=1}^{68} v_{U,i} + w_2 \sum_{i=1}^{35} v_{T,i} + w_3 \sum_{i=1}^{12} v_{C,i} + w_4 v_D \quad \textbf{(5.10)}$$

where $v_{U,i}$ is the violation according to the voltage limits of *i*th bus, $v_{T,i}$ is the violation according to the thermal limit of *i*th transmission line, $v_{C,i}$ is the violation according to the transient stability limit for *i*th critical contingency and v_D is the violation according to small signal stability of the system. Weights of violations, w_1, w_2, w_3 and w_4 are not adjusted to give priority to one violation type, they are computed to equalize their effect on the penalty function, since magnitude of possible violations and number of constrained parameters are different for each inequality constraint type.

During the optimization, stability constraints for each candidate solution are estimated by offline trained ANN described in previous section. Additional constraints are also considered during the optimization. As inequality constraints, limits for the generated power by generators, limits of curtailment quantity of loads, limits for steady state bus voltages and limits for the power flows through transmission lines are taken into account. ANNs are integrated into the optimization process is as follows,

1. Initial population is created
2. Power flow solutions are computed (to read measurements)
3. Dynamic security assessment by ANN
4. Calculation of objective and penalty functions for candidate solutions

5. Calculation of fitness function for candidate solutions

6. Created of new solutions by the optimization algorithm

7. Repeat steps 2 to 6, until stopping criterion is achieved.

As explained in Section 3.4, adaptive constraint handling method is applied to reach the feasible solution space during optimization.

5.3 Results for Security Constrained Optimal Preventive Control Action

For security constrained optimal preventive control action problem is solved with 6 different optimization methods explained in Section 3. As an initial condition, one OP (27^{th} OP) of created KB to train the ANN, is selected. This OP is insecure with respect to CCT values computed for critical contingencies and clearing time (CT) values of circuit breakers given in Table 5.2.

Table 5.2 : CCT values for critical contingencies on initial OP and CT values of circuit breakers, which clear critical contingencies.

Cont.	1	2	3	4	5	6	7	8	9	10	11	12
CCT	6.97	7.33	7.01	6.87	6.59	5.81	4.93	4.06	5.64	5.53	1.91	4.37
CT	9	9	9	9	9	8	7	7	8	8	5	7

Final solutions of the optimization methods may vary because of the randomness in creating candidate solutions. To investigate the reliability of the methods, optimization process is repeated 20 times for each optimization method. Optimization tries involves approximately 8000 function evaluations for each optimization method. Results associated with the final solutions and first feasible solutions (feas1) achieved are given in Table 5.3.

Table 5.3 : Results for all optimization methods.

Method	Minimum $f_{final}(x,u)$ (\$/h)	Average $f_{final}(x,u)$ (\$/h)	Std. dev. $f_{final}(x,u)$ (\$/h)	Average Num. of $Feval_{feas1}$	Average $Time_{feas1}$ (minutes)	Average $f_{feas1}(x,u)$ (\$/h)
GA	15844.68	19797.02	2901.23	648	3.42	82947.9
DE	15840.05	17234.91	756.01	514.5	2.57	89310.4
BB-BC	17308.25	19733.03	1328.65	357	1.78	85424.4
PSO	15266.61	16861.87	1095.15	339.5	1.69	100768.5
ABC	15202.31	16689.18	912.72	734.4	3.67	85256.9
MVMO	15183.28	15920.69	526.77	1121.9	5.61	72313.1

All optimization methods start the searching process with randomly created solutions by considering upper and lower limits of control variables. Therefore, all solutions in the earlier iterations are infeasible with respect to high number of constraints. As seen from the Table 5.3, all methods have the ability to reach the feasible solutions less than 6 minutes. This time also depends on the initial condition of the power system. If the initial OP is far away from the security boundary and there are high number of constraint violations, the required time to find a feasible solution can be relatively more than the initial OP with less violations. Feasible final solutions of optimization methods also confirm the success of the proposed penalization based constraint-handling strategy.

Figure B.1 in the Appendix B, shows the evolution of penalty function value of best solutions during 20 optimization runs for all algorithms. From Table 5.3 and Figure B.1, BB-BC and PSO can be considered fastest algorithms by means of reaching feasible solutions. During, the first phase of optimization where the population involves only infeasible solutions, the main target is not minimization of the objective function. Results show that searching characteristics of BB-BC and PSO are proper to be used in the first phase of the optimization.

Last column of the Table 5.3 shows that, the average objective function values, $f_{feas1}(x,u)$ of the first feasible solutions reached during the optimization are much higher than the final solutions of the iterations. So, in this second phase, algorithms should need time to improve the objective function value of feasible solutions achieved, and also increase the number of feasible solutions in the population. First three column of Table 5.3 shows that, although BB-BC is one of the fastest algorithm with respect to its convergence speed in the first phase, the algorithm is not as successful as improving the best objective function value. This result shows that, fast convergence strategies may lead to stack into local minimum points. Relatively slower convergence strategies of other algorithms reaches objective function values lower than 16000 $/h.

Second and third columns of Table 5.3 indicate the reliability of the optimization methods. For this optimization problem, GA and BB-BC can be considered more sensitive to the randomness, when compared with the other optimization methods. Although GA can reach solutions with objective function values less than 16.000 $/h, mean and standard deviation of multiple tries are not satisfactory. Figure 5.2 shows the minimization of the best objective function values achieved in 20 runs of all optimization methods. Graphics show that the problems of GA and BB-BC are different. Multiple BB-BC runs shows similar convergence characteristic, like other reliable methods. This means that BB-BC needs to find a new strategy to improve objective function values of feasible solutions in the last section of the optimization. On the other hand, multiple GA runs may have different characteristic in each phase of the optimization. This increases the probability of sticking around local minimums during the GA optimizations. The other methods can be considered as reliable for the mentioned multi-dimensional optimization problem, which involves considerable number of nonlinear constraints, also continuous and discrete control variables.

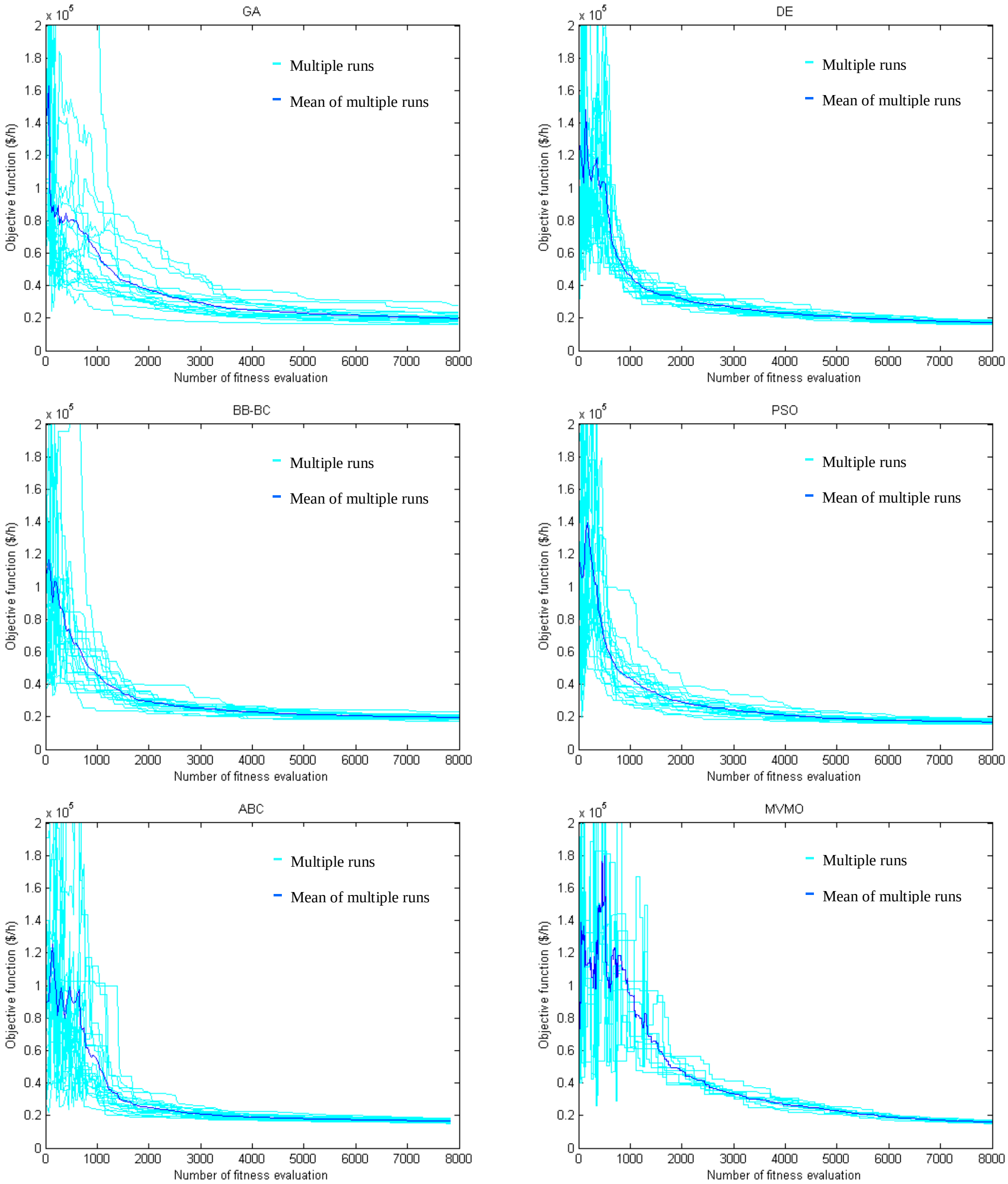


Figure 5.2 : Minimization of the best objective function values achieved in 20 trials of all optimization methods.

As mentioned before, in the earlier iterations, priority is given to feasibility instead of objective function value. This is the reason of fluctuation on the objective function values of best individuals, in the earlier iterations. As seen from the Figure 5.2, when iterations go forward and feasibility problem is solved, objective function values of best solutions start to decrease. This strategy can also be seen from Figure B.2 in the Appendix B, that shows the changes on the costly parameters of best solutions during, best runs of all optimization methods. Costly parameters of solutions mean that parameters which directly affect the objective function of the solution, such as active power change in the generation (ΔP_G) and load (ΔP_L) buses. From Figure B.2, the magnitude of the deviation of any participant's active power ($|\Delta P_G|$,$|\Delta P_L|$) increase or decrease to satisfy the constraints of the optimization problem. Then, $|\Delta P_G|$ and $|\Delta P_L|$ values tend to move close to the zero, until causing violations.

Figure 5.3 and Figure 5.4 show the final value of ΔP_G and ΔP_L for the best solutions achieved by each optimization method after multiple runs. When the generation rescheduling sections of the best preventive control strategies (ΔP_G) are analyzed by considering the system topology in Figure 5.1, it has been observed that final solution of the optimization decrease the active power generation of synchronous generators (no. 2, 3, 6, 7) which significantly affect the active power flows through the transmission lines where critical contingencies occurs. In addition, curtailment of selected loads around the locations of critical contingencies helps generation rescheduling to relax these important transmission lines and increase the CCT values. As mentioned before, curtailment action is limited with the amount of intelligent loads in selected load buses. So, the difference between high generation decrease on generators 2, 3, 6 and 7 cannot be balanced only by limited curtailment action and synchronous generators in the west and north side of the power system model increases their generations, as seen from Figure 5.3. Another result from Figure 5.3 and 5.4, is the correlation between the parameters of best solutions of different optimization methods. This relation can be easily observed on the ΔP_G parameters, which are more effective than ΔP_L parameters, on satisfying the security constraints.

Discrete ΔT_{Tap} parameters of the solution is not investigated in here, since their main effect is on changing reactive power flow and satisfying steady state voltage constraints for the solution in each phase of the optimization. Therefore, ΔT_{Tap}

parameters of solutions can get any value between predetermined limits during the optimization and do not change the objective function value of the solutions.

When the optimization methods use randomly generated initial populations, they require approximately 40 minutes for 8000 iterations. If ANNs are not utilized, optimizations take 18 hours, and this time can increase for larger systems. Since optimizations need 8000 iterations, results show that optimization methods can quickly reach feasible solutions with the help of constraint handling methods. As seen from Figure B.2, variables of best solutions swing before the search algorithm reaches feasible area. Then, first feasible solutions start to converge to an optimum point which is relatively closer to the first feasible solutions, if compared with the current insecure OP of the system. Therefore, if system operator needs to apply a fast control action to prevent the system against critical contingencies, feasible solutions achieved by the algorithms just in a few minutes (Table 5.3) can be used. When the optimization is completed, system operator can move the system to the final OP which is not far away from the temporal OP (first feasible solution).

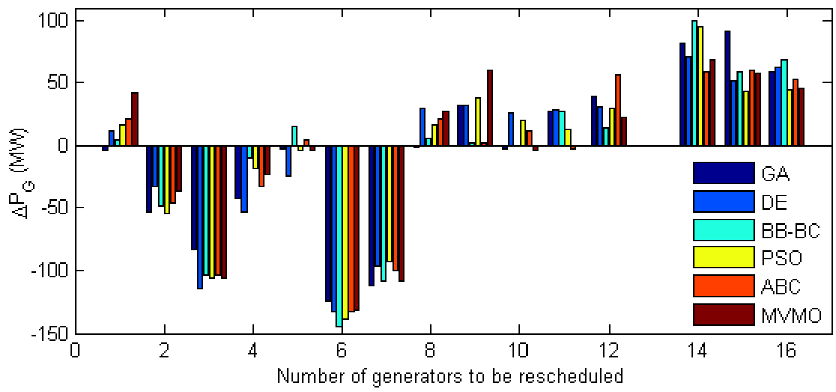


Figure 5.3 : Generation rescheduling section of the best solutions achieved by each optimization method.

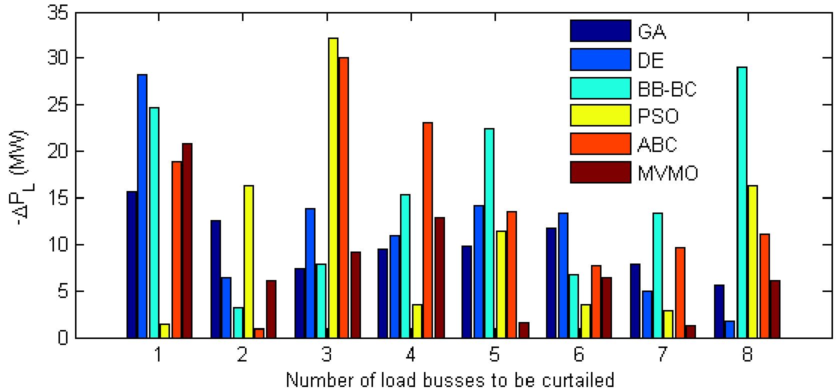


Figure 5.4 : Load curtailment section of the best solutions achieved by each optimization method.

Results given so far, are based on preventive control action applied on a test system operating in an insecure OP (OP_{27}), which is chosen from the KB. Same methodology is applied to various selected insecure OPs with different topologies and loading levels (Table 5.4). As seen from loading level values, the system is stressed to create insecure operating conditions for selected 12 contingencies. In addition, some important lines are removed from the system. For all OPs, CCTs values of each critical contingency is lower than the stability limits. Then, each optimization method runs (5 times) to enhance the dynamic security of the system operating in these OPs. Table 5.5 shows the, average of cost function values found by each optimization method after 5 optimization runs. Since, designed ANNs for DSA is capable to recognize topological changes and various loading levels, the same ANNs can be used for the optimizations related with all insecure current OPs. Final solutions of all optimization methods move the system to a secure OP. Most of the results are similar to the tables and figures given above for the first case (OP_{27}). According to the results of Table 5.5, for various insecure OPs, the only difference is the total cost required to move the system to a secure OP.

Table 5.4 : Topological changes and loading levels for selected OPs.

OP number in KB	Line outage between buses	Loading level (%)
27	-	111
228	4-14	115
329	8-9	120
425	17-27	112

Table 5.5 : Optimization results for different system conditions.

	Average $f_{final}(x,u)$ (\$/h)			
Method	OP_{27}	OP_{228}	OP_{329}	OP_{425}
GA	19797.02	26798.77	41517.48	26931.87
DE	17234.91	24525.63	24331.59	20748.36
BB-BC	19733.03	26336.66	28567.89	22004.34
PSO	16861.87	25490.49	27205.68	20828.03
ABC	16689.18	24495.04	26729.76	20086.17
MVMO	15920.69	22993.44	29376.33	20668.55

6. RESULTS FOR VARIOUS TEST SYSTEMS

6.1 Introduction

During my doctoral studies, proposed methodology has been modified and it has been applied to various available test systems. Sections 4 and 5 represent the results of the present form of the methodology applied to 16-generator, 68-bus test system. This section represents the results of the past methodologies applied to 17-generator,163-bus Iowa and 50-generator, 145-bus IEEE tests systems [70], in addition to 16-generator, 68-bus test system.

In the methodology explained in Sections 4 and 5, DSA is considered as a regression problem. Nonlinear relationship between CCT values of each contingency and relevant system features is identified by MLPs. Beside online security assessment, these neural network structures are also used to determine the security status of the candidate solutions during optimization of preventive control action, generation rescheduling.

In previous methodologies, DSA is also considered as a two-class classification problem where the classes for the system security are secure and insecure. This problem is solved by using a modified Probabilistic Neural Network (PNN) which is specially designed for classification problems. During the GA optimization for optimal generation rescheduling, PNN classify new children of the population (candidate solutions) as secure or insecure.

Although ANN structures increase the speed of the optimization, it is obvious that there is a trade-off between speed and accuracy of identifying the security boundary. In this section, 100% accurate but time consuming time domain simulations are also used during optimization to compare various optimization methods to optimize both preventive and corrective control actions. Details about these studies can be found in [12, 72].

6.2 PNN and ANFIS Integrated Optimal Preventive Control Action

This section represents, DSA and generation rescheduling methodology utilizing GAs which are integrated with PNNs and ANFISs for the preventive control action against transient instabilities.

PNNs are employed in a feasible manner to calculate the security regions accurately during the assessment and control. The security constrained generation rescheduling is implemented through a GA, which optimizes the total fuel cost or generation shifting during the preventive control. The steady-state solutions of the variables required for the GA are smoothly performed by the use of an ANFIS. The methodology is demonstrated on the 17-generator, 163-bus Iowa power system and on the IEEE 50-generator, 145-bus test system.

The methodology includes a number of elaborate steps towards generation rescheduling as a preventive control against transient instabilities. These steps can be listed as,

1. Contingency analysis and creation of a KB

2. Training and developing of a PNN as a security assessment tool

3. Training and developing of ANFIS as a power flow solution tool

4. Application of GA based optimization to enhance power system security

6.2.1 Contingency analysis and creation of knowledge base

Method starts with a contingency analysis to be performed for determining the critical contingencies that have the potential to create transient instabilities in the power system. This step includes extensive time-domain simulations under possible contingencies and differentiating the critical contingencies from the others.

The critical contingencies considered in the test systems are 3-phase-ground faults that are cleared 5 cycles after their occurrences by a single line tripping but causing transient instabilities based on the stability index defined in (4.1). In Table 6.1, a list of considered critical contingencies for the 17-generator and 50-generator systems is given.

Table 6.1 : Critical contingencies for 17-generator and 50-generator systems.

17-generator system			50-generator system		
Contingency no.	3-phase fault close to bus no.	Tripped line between buses	Contingency no.	3-phase fault close to bus no.	Tripped line between buses
1	26	26-25	1	128	128-119
2	26	26-75	2	128	128-129
3	26	26-74	3	129	129-128
4	26	26-149	4	94	94-60
5	75	75-26	5	60	60-94
6	75	75-128	6	117	117-102
7	75	75-9	7	117	102-117
8	128	128-75			

Followed by the contingency analysis, a group of generators is selected for generation rescheduling as a preventive control against the critical contingencies. For each critical contingency, the generators that are most effective in shaping the system's transient stability can be found through sensitivity analysis. Although, this approach may reduce the dimension of the space in which we apply the security assessment and control, and thus, reduce the computational burden, in this methodology, it is assumed that a group of generators that are available for rescheduling such that some of the generators in the group are very effective in the system's transient stability against the contingencies whereas the others are not. The reason of this approach is to test the efficiency of the proposed assessment and control method in a more general case in which the classification and decision are to be done when some of the variables are not very critical for the security status of the system. For both power systems, five generators are assumed to be available for generation rescheduling and the security regions are computed in the space of generations at the buses given in Table 6.2.

Table 6.2 : Generators considered in DSA and preventive control.

17-generator system				50-generator system			
Generator no.	Bus no.	Min. output (MW)	Max. output (MW)	Generator no.	Bus no.	Min. output (MW)	Max. output (MW)
1	6	1007	1107	1	94	100	250
2	73	357	1007	2	102	1400	1500
3	76	1107	1557	3	128	8750	8850
4	131	707	807	4	137	2350	2500
5	130	133	1172	5	145	21932	22137

In this method, the security assessment and control are conducted in the parameter space of outputs of some selected generators. Creation of a direct KB which contains a wide range of OPs, and the security status of the system at each of these points is substantial. A synthetic data, KB, is generated through power flow calculations and time-domain simulations for training and testing processes of PNN. During the creation of KB, OPs are defined and distinguished by the real power generations at the five selected buses which can be rescheduled during the operation of the power system. To create an initial KB, all independent generation values for each OP are produced as we uniformly grid the hypercube,

$$H = \prod_{i=1}^{r-1} \left[\underline{P_{Gi}} \overline{P_{Gi}} \right] \qquad \textbf{(6.1)}$$

where there are *(r-1)=4* independent generators considered in the DSA, $\underline{P_{Gi}}$ and $\overline{P_{Gi}}$ are the minimum and the maximum limits of the *i*th generator, respectively. For each OP, the dependent power generation, P_{G5} , is determined by the power flow solution at the current loading condition. For the 17-generator system, the initial KB is formed by 140 OPs as we grid the hypercube with a spacing of 100 MW, whereas the initial KB for the 50-generator system is formed by 144 OPs with a grid spacing of 50 MW. For performance evaluation of the proposed PNNs, test sets with higher resolutions are generated. For the 17-generator system, the grid spacing is selected as 25 MW resulting a test set consists of 12825 OPs and for the 50-generator system, the grid spacing is selected as 12.5 MW resulting a test set consists of 13689 OPs.

For each OP of KB, the power flow computation and the identification of security status via time-domain simulations are performed by DSATools™ [58]. The OPs in the KB identified by the generations at which the system preserves its stability against all credible contingencies without violating generation capabilities of the generators are labeled as secure. In this work, the transient stability criterion is considered to be the only dynamic security criterion, and the angle stability of the system is quantified by the stability index η defined in (4.1).

6.2.2 Security assessment by PNN

In the DSA process, we propose the employment of a PNN that classifies the security status of the power system as it determines if the current or a projected OP is secure for all of the credible contingencies. Hence, depending on the PNN's classification, proper preventive control actions can be taken if necessary.

Two important factors in the design of a PNN have been elaborated in this work: classification performance of the PNN and computational feasibility during the implementation. While the classification performance of a PNN significantly depends on the network structure and the parameters of the Gaussian activation functions, computational feasibility is greatly affected by the size of the TS, which has to be generated through power flow and time-domain simulations. Moreover, execution speed of the PNN is significantly related with the size of the pattern layer of the PNN, which is also directly dependent on the size of the TS. In Figure 6.1, an algorithm is proposed for generating the proper training sets, which enhance the classification performance of the PNNs, whereas the algorithm keeps the computational requirements at a limited level.

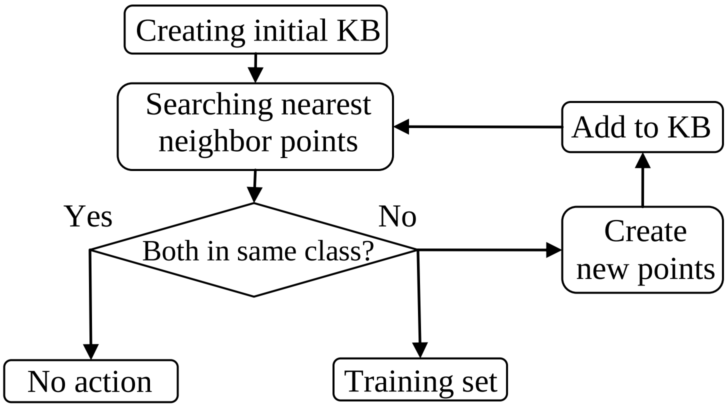


Figure 6.1 : Flowchart of training set selection algorithm.

The proposed algorithm starts with the generation of an initial KB, which includes a collection of OPs and their securities in the parameter space of interest. The algorithm then iterates the following two consecutive steps until a satisfactory classification performance is ensured: searching the pairs of neighboring OPs belonging opposite classes for training, and generation of new OPs for the next iteration.

In the former step, the pairs of nearest neighbor OPs are collected as we measure the level of neighborhood by the Euclidian distance between the points in the KB. If the points in a pair belong to different classes, they are considered to be located near the security boundary, and these points are selected for the TS of the PNN. Suppose the KB at the *k*th iteration of the algorithm, KB_k, is composed of two distinct sets: the set of secure OPs, S_k , and the set of insecure OPs, I_k , i.e. $KB_k = S_k \cup I_k$. Then, the set of pairs, each of which includes two OPs with opposing security statuses and that are close to the boundary,

$$SB_k = \{(OP_i, OP_j) \in S_k \times I_k : \|OP_i - OP_j\| = min\|OP_i - OP_r\|\}$$

$$OP_i \in S_k, OP_j \in I_k \qquad \textbf{(6.2)}$$

$$i = 1, 2 \dots N(S_k), j = 1, 2 \dots N(I_k) \; r = 1, 2 \dots N(S_k), i \neq r$$

where the size of a set is denoted by *N(.)*. Hence, the TS at the *k*th iteration,

$$TS_k = \{OP: OP \; \in SB_k^l, SB_k^l \in SB_k, l = 1,2, \dots, N\ (SB_k)\} \qquad \textbf{(6.3)}$$

The selection of the TS formed only by the neighboring OPs of different classes results in a high classification performance of PNN, because the accuracy in classification of an input vector (OP) near the actual boundary is directly dependent on its distance to the points of the TS.

In the latter step, the selected pairs of points in the previous step are used for creating new OPs which are to be added to the KB for the next iteration of the algorithm. For each selected pair, a new OP which is the midpoint between the points in the pair is generated.

$$KB_{k+1} = KB \cup \left\{OP: OP = \frac{1}{2(OP_i + OP_j)}, (OP_i, OP_j) \in SB_k\right\}, k = 1,2 \dots \qquad \textbf{(6.4)}$$

Thus, since the new pairs of OPs get closer to the actual security boundary, the classification performance of PNN increases with the number of iterations.

During the generation of the new OPs and the TS of PNN, owing to the proposed approach, since the number of new points to be created is kept limited, the computational burden due to power flow and time-domain simulations as well as the execution time of the PNN remains feasible.

Closeness of an OP to the security boundary can be associated with the number of its nearest neighbors placed on the other side of the boundary. Therefore, in this work, the pattern neuron associated with an OP is weighted based on the closeness of the OP to the security boundary. The weight of each neuron in class *c* can be selected as

$$w_{c,s} = \alpha / s \qquad \textbf{(6.5)}$$

where α is the number of nearest neighbors of the related point with the opposite security state, and s is the number of pattern neurons belonging to class c.
Since the DSA in this work can be considered as a two class classification task, two types of misclassification of PNN may occur: false alarm when a secure OP is classified as insecure, missed alarm when an insecure OP is classified as secure.

When the missed alarm rate is considered to be more critical, a relatively small weight can be assigned for the output of the neuron belonging to secure class in the summation layer. The missed alarm rate decrease, but the false alarm rate increases, thus, the classification performance of PNN does not change significantly.

Classification performance of a PNN is also greatly affected by the spread values of the Gaussian activation functions. Small spread values produce sharp shaped functions, which can cause an over-fitting problem, on the other hand, large spread values flatten details. In any of the two cases, the misclassification rate of PNN increases as they lead to false or missed alarms in the security assessment. Assigning different spread parameters for activation functions belonging to different classes in the pattern layer increases the flexibility of PNN's structure. The use of single and multi-spread PNN structures in the DSA in power systems is studied in [72]. In this work, we only utilize the single-spread PNNs due to their simplicity.

By the proposed approach, the centers of activation functions in the pattern layer of PNN coincide with the points in the TS. Starting with an initial KB, the KB is updated in each iteration as described in Figure 6.1. Table 6.3 shows the sizes of the TS and the KB in each iteration for the two test systems.

Table 6.3 : Size of the TS and KB at each iteration.

17-generator system			50-generator system		
Iteration	TS size	KB size	Iteration	TS size	KB size
1	71	140	1	84	144
2	119	221	2	116	211
3	162	302	3	123	278

The size of the TS as well as the number of activation functions in the pattern layer increases with the number of iterations. However, by the proposed approach, the total TS size is kept limited in order to bind the PNN's size and its execution time. As the number of iterations increases, OPs in the TS become denser around the security boundary. Hence, the developed PNN detects the security status of any current OP more accurately as the iterations progress. Table 6.4 shows the maximum PNN performances in each iteration for the calculated optimum spread values. Results show that classification performances of the PNN structures increase with the number of iterations, whereas the sizes of the pattern layers of the PNNs remain small.

Table 6.4 : Performances of PNNs.

	17-generator test system				50-generator test system			
It.	Spread	Overall success (%)	Missed alarm (%)	False alarm (%)	Spread	Overall success (%)	Missed alarm (%)	False alarm (%)
1	69	95.82	2.91	1.27	35	83.55	8.18	8.27
2	64	96.15	3.46	0.39	33	92.49	4.54	2.97
3	60	96.58	3.06	0.36	12	95.48	1.68	2.84

For each iteration, PNN classification performances with respect to changing values of spread parameters are given in Figure 6.2. A high classification performance requires a proper spread parameter, which is dependent on the distances between the nearest neighbors in the TS. A proper selection of the spread parameter that takes the developed TS into account ensures the enhancement of the classification performance as the iterations go forward. According to Figure 6.2, even if the optimum spread parameters in Table 6.4 are not assigned, the classification performance increases with the number of iterations as long as a fixed spread parameter from a reasonable range is selected.

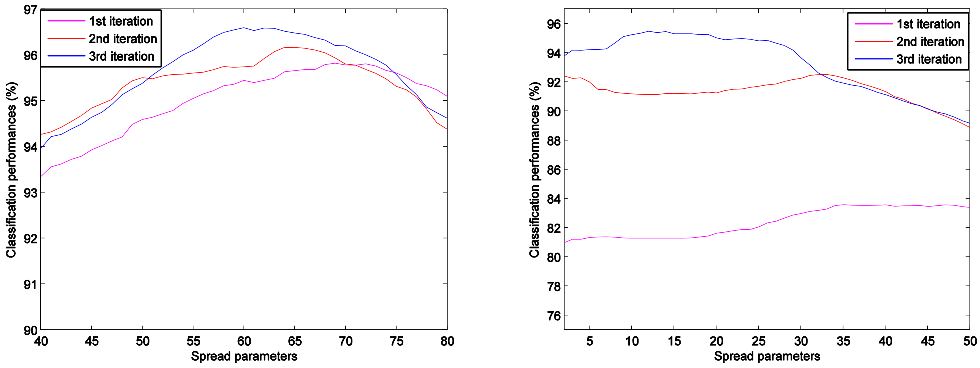


Figure 6.2 : PNN performances with respect to changing values of spread parameters a) 17-generator system b) 50-generator system.

Missed alarms are more critical than false alarms during the DSA, because no preventive control action would be considered for the current insecure OP in case of a missed alarm. Missed alarms are also critical during the preventive control, since the system can be dragged to an insecure OP by the control action. In order to decrease the missed alarm rate, the output of summation neuron belonging to secure class is reduced by 5% in the PNN structure. As seen from Table 6.4 and Table 6.5, this modification decreases the missed alarm rate and increases the false alarm rate, while the overall classification performance remains satisfactory.

Table 6.5 : Performances of PNNs accounting for missed alarm priority.

	17-generator system				50-generator system			
It.	Spread	Overall success (%)	Missed alarm (%)	False alarm (%)	Spread	Overall success (%)	Missed alarm (%)	False alarm (%)
1	75	95.75	2.61	1.62	59	84.16	4.79	10.92
2	73	96.57	2.31	1.10	37	91.89	3.06	5.04
3	78	97.15	0.16	2.68	12	95.48	1.44	3.08

6.2.3 Power flow solutions by ANFIS

To calculate the fitness values of the new children, the output of the dependent generator that is rescheduled is to be determined. Therefore, a steady-state solution for each new OP has to be calculated via power flow computation, which is a time consuming task that can slow down the optimization algorithm dramatically. As an alternative, which relieves most of the computational burden due to this problem, an ANFIS model that estimates the dependent generator's output is proposed. The process of forming a new population in GA is summarized in Figure 6.3.

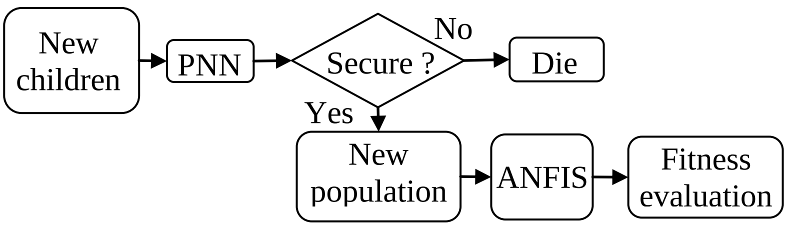


Figure 6.3 : Flowchart of forming a new population in GA.

The ANFIS is trained by a set of OPs (steady-state solutions) which have previously calculated through power flow computations and included in the KB generated for security assessment. The independent generator outputs of the OPs are the inputs to the ANFIS, and the dependent generator outputs are selected to be the target values.

The number of MFs is directly related with the size of the ANFIS structure, and it also affects the computational burden and execution time. While using a single MF for each input node can decrease the accuracy of ANFIS, using a large number of

MFs, and, therefore, using excessively large numbers of rules and parameters require more computation without significantly enhancing the overall performance of ANFIS. The ANFIS, which computes the values of dependent generator outputs for the new children (OPs) instead of running a power flow program, has the parameters given in Table 6.6.

Table 6.6 : Parameters of ANFIS.

Number of inputs	4 ($P_{G1...4}$)
Number of outputs	1 (P_{G5})
Number of MFs	8
MF type	Generalized Bell
Number of rules	16
Number of consequent param.	80
Training epoch number	5
Training error goal	0.0001
Initial step size	0.001
Step size decrease rate	0.9
Step size increase rate	1.1

In order to assess the performance of the ANFIS, the relative error E in computing the steady-state solutions of OPs in either training or test set is defined as

$$E = \frac{\sum_{i=1}^{n} \left| P_{G5,i} - \hat{P}_{G5,i} \right|}{\sum_{i=1}^{n} P_{G5,i}} \qquad \textbf{(6.6)}$$

where n is number of OPs, $P_{G5,i}$ and $\hat{P}_{G5,i}$ are the actual and estimated outputs of the dependent generator at the ith OP, respectively.

The final KB in Table 6.4, which has been utilized during the PNN's training is randomly divided into two as training and test sets for the calculation of relative errors of ANFIS. The relative errors in the training and test sets are given in Table 6.7. The results show that the proposed ANFIS has a satisfactory performance in estimating steady-state solutions.

Table 6.7 : Estimation performance of ANFIS.

	E_{Train}	E_{Test}	Training set size	Test set size
17-generator system	3.12 x 10^{-4}	3.20 x 10^{-3}	202	100
50-generator system	1.49 x 10^{-4}	4.59 x 10^{-4}	186	92

6.2.4 GA based optimal generation rescheduling

A dynamic security constrained generation rescheduling method is proposed as a preventive control technique against transient instabilities when the current OP is classified to be insecure by the PNN. The method involves shifting the generations among a group of available generators such that the system is drawn to an OP in the secure region in which the system preserves its stability even if a critical contingency occurs.

While the power system is moved to a new OP at which the system's security is regained, the proposed method also involves an optimization procedure that offers a minimum generation shifting or a minimum total fuel cost for the preventive control action. The security constrained generation rescheduling can be expressed as

$$\textit{minimize } f(x, u), \textit{ subject to}$$
$$g(x, u)=0$$
$$h(x, u) \leq 0$$

where u represents the control variables, which are the active power generations to be rescheduled, and x represents the dependent variables of the system due to power flow solutions and time-domain simulations. The power flow equations are represented by the equality $g(x,u) = 0$ whereas the dynamic security constraints are represented by the inequality $h(x,u) < 0$. Two objective functions are considered in this work: the total amount of generation shifting during the preventive control action,

$$f_1(u) = \sqrt{\sum_{i=1}^{r}(P_{Gi}^0 - P_{Gi})^2} \quad \textbf{(6.7)}$$

and the total fuel cost at the target OP,

$$f_2(u) = \sum_{i=1}^{r} f_{Gi} = \sum_{i=1}^{r} a_i\, P_{Gi}^2 + b_i P_{Gi} + c_i \quad \textbf{(6.8)}$$

where r is the number of generators to be rescheduled, P_{Gi} is the active power output of ith generator, P_{Gi}^0 is the active power output of ith generator for the current insecure point. a_i, b_i and c_i are the parameters for the fuel cost function of ith generator, f_{Gi}. The total generation shifting f_1 is expressed in MW, and the total fuel cost f_2 is expressed in *\$/hr*. The parameters of the fuel cost function in (6.7) for generators to be rescheduled are given in Table 6.8.

Table 6.8 : Parameters of fuel cost function.

17-generator system				50-generator system			
Gen. no.	a_i ($/MW^{2}h)	b_i ($/MWh)	c_i ($/h)	Gen. no.	a_i ($/MW^{2}h)	b_i ($/MWh)	c_i ($/h)
1	0.15	20	2000	1	0.1	25	1500
2	0.15	40	2000	2	0.1	20	1500
3	0.08	15	1400	3	0.01	8	1400
4	0.2	50	2000	4	0.09	25	1500
5	0.25	15	1500	5	0.01	10	2000

In this work, generation rescheduling is considered as a security constrained optimization problem. An optimization technique that starts from an initial point and searches the global optimal point in a multidimensional parameter space can be a time consuming task. If the initial point is not selected properly, the optimization algorithm may require a substantial amount of computation time for convergence or it might get stuck at local optimums. Due to aforementioned disadvantages, usage of GAs for the solution to generation rescheduling in large power systems is promising.

In the GA structure of the constrained optimization problem of interest, each individual is represented by an OP defined by the active power outputs of *r* generators to be rescheduled. Since the rescheduling problem is solved under a constant loading condition of the system, the outputs of the *(r-1)* independent generators will define each OP uniquely at which the output of the dependent generator is calculated via power flow equations.

Fitness of individuals depends on the selected objective functions. Depending on the objective function, if an individual is very close to the current OP or has little fuel cost, the fitness value as well as the selection probability of this individual is high.

OPs are expressed as individuals in a population, and each point is presented by a chromosome. For direct calculations, real coded representation is used instead of binary code representation. Therefore, any chromosome *I*, which contains *(r-1)* independent generator outputs as its genes, is represented by

$$I = \left[P_{G1}\ P_{G2}\ \dots\ P_{G(r-1)}\right] \qquad \textbf{(6.9)}$$

Generally, initial population is formed by randomly selected secure OPs from a KB. For both objective functions, since the optimum solutions normally lay on the security boundary, the initial population can be formed by the OPs that are close to the boundary, which were previously used in the PNN training. Hence, the search space and computation time for the optimization can be decreased judiciously.

Individuals can be selected through various selection operators such as roulette wheel, rank and tournament selection. The winners are selected as parents to produce children (new OPs) via a crossover operator.

One or multi-point crossover methods, which are the mostly used crossover methods, produce the OPs that already belong to the KB. In this work, to increase gene variety and to produce different OPs, weighted (arithmetic) crossover method is applied.

Security condition of the new OPs has to be determined before adding them to the population. If an insecure new child is detected, this child will not be placed into the population. The classification of the new OPs is simply performed by the trained PNN which was used for the security assessment of the current OP. In order to form the new population, the individuals with lowest fitness values are replaced by the newly generated secure children.

To calculate the fitness values of the new children, the output of the dependent generator that is rescheduled is to be determined. Therefore, a steady-state solution for each new OP has to be calculated via power flow computation, which is a time consuming task that can slow down the optimization algorithm dramatically. As an alternative which relieves most of the computational burden due to this problem, an ANFIS model that estimates the dependent generator's output is proposed.

The ANFIS is trained by a set of OPs (steady-state solutions) which have previously calculated through power flow computations and included in the KB generated for security assessment. The independent generator outputs of the OPs are the inputs to the ANFIS, and the dependent generator outputs are selected to be the target values.

The number of MFs is directly related with the size of the ANFIS structure, and it also affects the computational burden and execution time. While using a single MF for each input node can decrease the accuracy of ANFIS, using a large number of MFs, and, therefore, using excessively large numbers of rules and parameters require more computation without significantly enhancing the overall performance of ANFIS.

After replacing the OPs with lowest fitness values by the newly generated secure OPs, a mutation operator is applied to prevent the algorithm getting stuck into local optimum solutions. If an excessively large mutation probability is selected, the algorithm needs more time to converge, and the time required for the optimization increases.

The selection of the stopping criterion is also critical for the proposed method. Due to the randomness in the operators used in the algorithm, an arbitrary number of iterations may not always give an optimum solution. The deviation in the average objective function value of the evolving population can be utilized in the stopping criterion, to determine if the algorithm still needs to run for a better solution.

Security constrained generation rescheduling method that is described in Section 3.3 is implemented to the two test systems as the objective functions f_1 in (6.7) and f_2 in (6.8) with the parameters given in Table 6.8 are minimized.

In the beginning of the optimization procedure based on GA, the chromosomes of the initial population involving the independent generator outputs are randomly selected from the set of secure OPs in the final (3^{rd}) iteration of KB creation (Table 6.5). While a small sized population may not scan the whole parameter space, a larger sized population requires more time for fitness evaluation in one GA iteration. In this work, the population size is chosen as 60 by considering the parameter limits and the chromosome length.

The tournament method is chosen as a selection operator. Large tournament sizes may increase the chance of individuals with low fitness values and they may also slow down the algorithm's convergence. For the selected population size of 60, the tournament size is selected as 8. According to the weighted (arithmetic) crossover method, for each pair of parents, new children c_a and c_b can be calculated as,

$$c_a = P_a(w) + P_b(1 - w) \tag{6.10}$$

$$c_b = P_a(1 - w) + P_b(w) \tag{6.11}$$

where P_a and P_b represent the parents in the pair and the weight w is selected as 0.65. Followed by the crossover operation, the individuals with the lowest fitness values in the population are replaced by the new children that are identified as secure by the PNN. The ANFIS, which computes the values of dependent generator outputs for the new children (OPs) instead of running a power flow program.

To prevent the algorithm getting stuck into local optimum solutions, the mutation probability is set to be %10. If the mutation operator is applied in a generation, the steady-state solutions for the mutated chromosomes are calculated by the previously developed ANFIS. Additionally, the stopping criterion for the GA is selected as

$$\alpha = \frac{mean(J_{x-150}) - mean(J_x)}{mean(J_{x-150})} < 0.01, \quad x > 150 \qquad \textbf{(6.12)}$$

where $mean(J_x)$ and $mean(J_{x-150})$ are the average objective function values of the populations at the *x*th and the *(x-150)*th generation, respectively.

The proposed generation rescheduling method is applied to the two test systems that are initially operating at insecure OPs at which the securities of the systems are successfully determined by the developed PNNs.

The two objectives for the preventive control, which are the minimization of total fuel cost and generation shifting, have been considered for the test systems. The optimum solutions to these problems will normally lie on the security boundary. During the execution of GA, as the individuals (OPs) of the evolving population approach the security boundary, newly generated OPs are more likely to be insecure despite their high fitness values. In this case, the individuals of the population and average objective function value of population do not change significantly, as more iterations are performed. Figure 6.4 shows the average objective function value of each population during the execution of GA for minimum generation shifting.

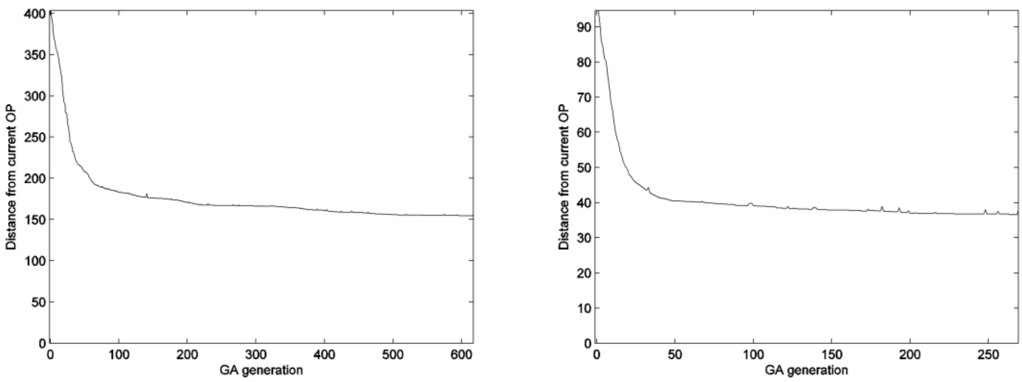


Figure 6.4 : The average objective function values of population within each generation a) for 17-generator system b) for 50-generator system.

Although the developed PNN has a good performance in differentiating the insecure OPs as well as reducing the missed alarm rates, there may be rare cases where the fittest individuals are insecure. In order to guarantee the security of the optimum rescheduling, time-domain simulations can be directly performed on the individuals of the final generation starting with the fittest individual.

For both of the test systems, Table 6.9 lists the initial and rescheduled OPs by the proposed method and the costs associated with the preventive controls applied. OP^*_{shift} and OP^*_{cost} are the optimum solutions for the minimum generation shifting and minimum total fuel cost, respectively.

Table 6.9 : Initial insecure OPs and GA optimized secure OPs.

17-generator system						
	P_{G1} (MW)	P_{G2} (MW)	P_{G3} (MW)	P_{G4} (MW)	P_{G5} (MW)	*f(u)*
Initial OP	1007	732	1432	757	515	$ 0.710 M/h
OP^*_{shift}	1069	671	1333	791	576	148.97 MW
OP^*_{cost}	1088	688	1318	707	640	$ 0.715 M/h

50-generator system						
	P_{G1} (MW)	P_{G2} (MW)	P_{G3} (MW)	P_{G4} (MW)	P_{G5} (MW)	*f(u)*
Initial OP	250	1400	8750	2350	22083	$ 6.73 M/h
OP^*_{shift}	218	1400	8755	2380	22078	44.24 MW
OP^*_{cost}	150	1400	8800	2350	22106	$ 6.75 M/h

In Figure 6.5 and Figure 6.6, the projections of the initial and rescheduled OPs in 3-dimensional parameter spaces are illustrated. As seen from these figures, optimal points tend to locate near security boundary. Therefore, success of classification of OPs near security boundary is substantial for the optimization. This result confirms the necessity of enrichment of training set around security boundary to train PNN.

For the sake of illustration, an example from the case studies explored in this work, the 17-generator system operating at the initial insecure OP and rescheduled point OP^*_{shift} in Table 6.9, is considered. TDS results for the relative generator angles of the system subjected to the critical contingency no. 2 (Table 6.1) are shown in Figures 6.7 and 6.8, respectively.

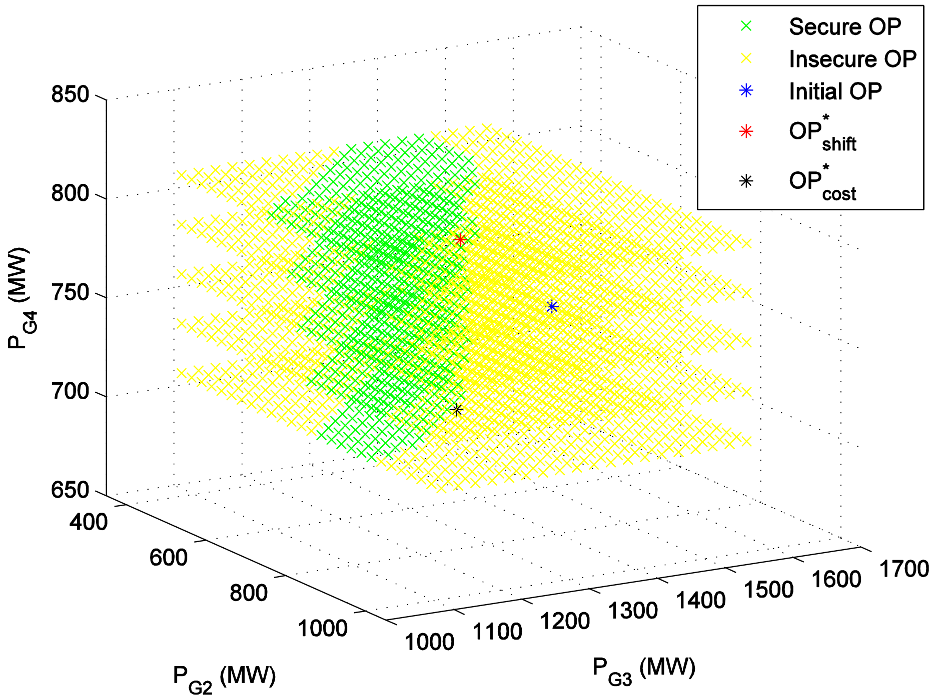


Figure 6.5 : OPs used in the test data and optimized OPs for the 17-generator test system projected into 3-dimensional space (P_1=1007 MW).

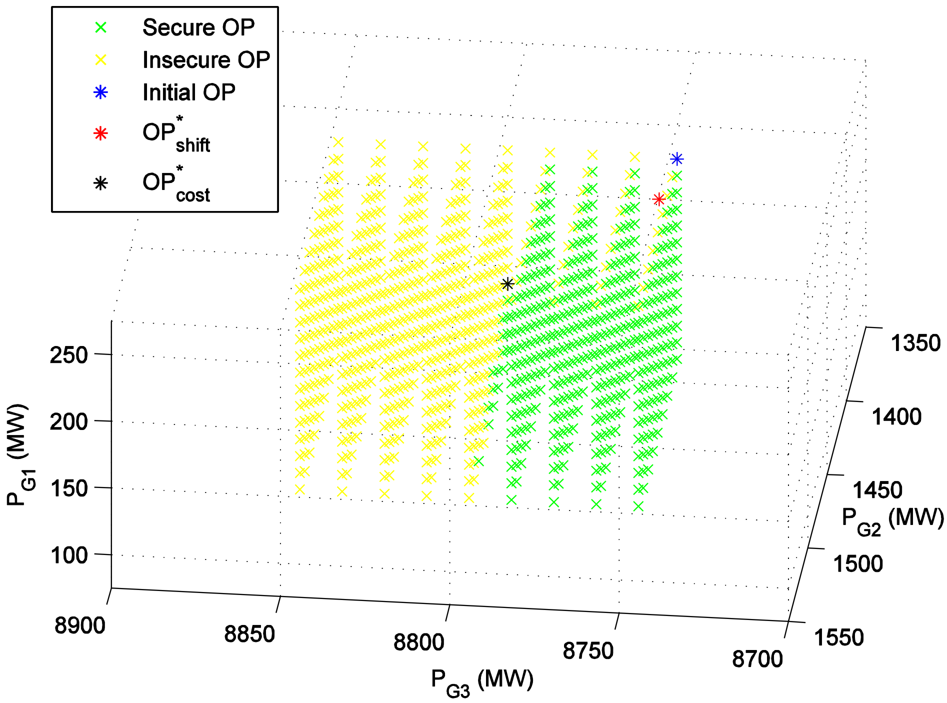


Figure 6.6 : OPs used in the test data and optimized OPs for the 50-generator test system projected into 3-dimensional space (P_4=2400 MW).

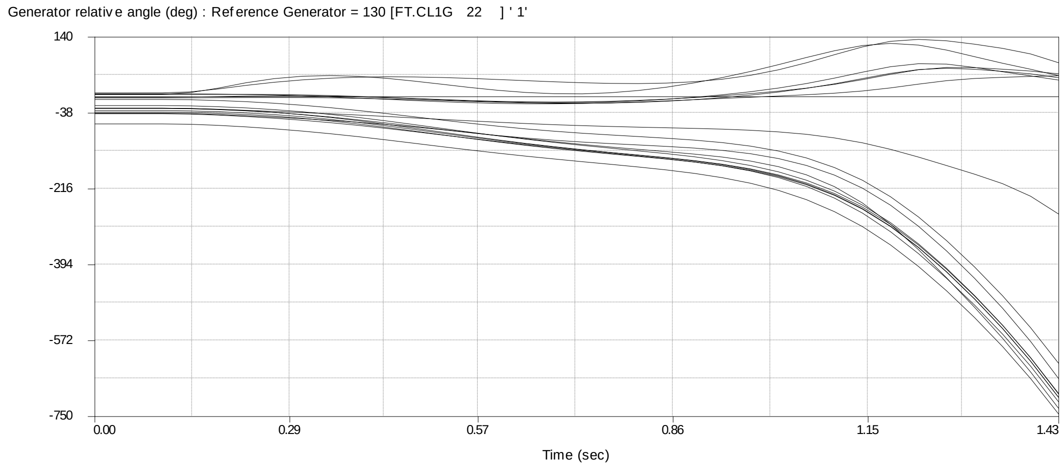


Figure 6.7 : The relative generator angles of the 17-generator system operating at initial, insecure OP.

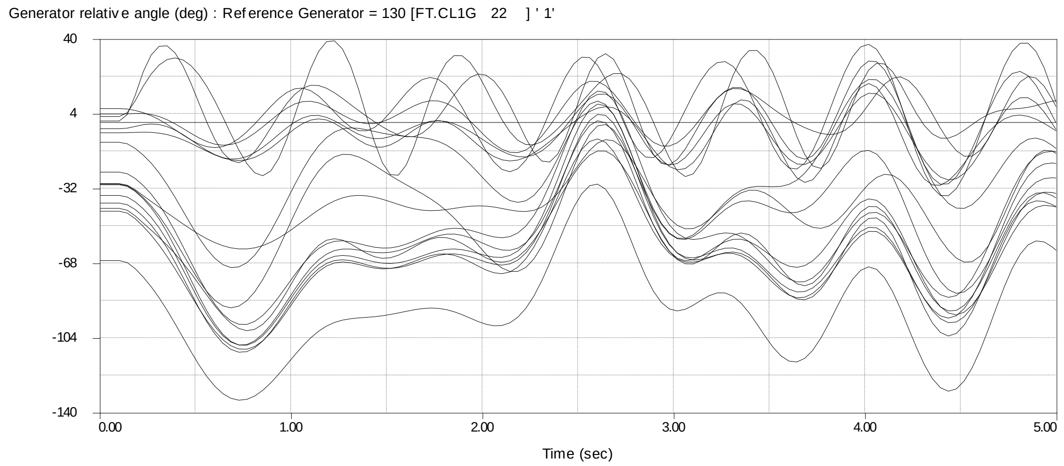


Figure 6.8 : The relative generator angles of the 17-generator system operating at secure OP^{*}_{shift}.

During the course of the implementation, the computational burden can be divided into the following tasks: generation of KB by power flow and time-domain computations, training and execution of ANFIS, execution of the PNN, and execution the GA. Table 6.10 includes the computational time requirements for the 17-generator system in case of using a single modern workstation with AMD Phenom^{TM} 9950 Quad-Core CPU 2.20 GHz. Most of the computation requirement is due to the KB generation, which can be almost equally shared by multiple computers running in parallel, if the computation time is desired to be reduced.

Table 6.10 : Computation requirements.

Creation of KB (302 OPs)		ANFIS		PNN	GA*	
PFC	TDS	Training (201 OPs)	Execution (1 OP)	Execution (1 OP)	Execution for f_1	Execution for f_2
5 min 45 s	12 min 49 s	0.174 s	3.9 x 10^{-5} s	3.4 x 10^{-4} s	5.91 s	1.49 s

* Cooperating with ANFIS and PNN.

6.3 TDS Integrated Optimal Preventive and Corrective Control Actions

In the previous subsection, the proposed ANN structures speed up the GA optimization by estimating the security constraint violations of candidate solutions, instead of using time domain simulations. As a results of that study, accuracy of ANN and its speed advantage shows that, they are suitable for security assessment during optimization.

The next study focuses on implementation of other population based optimization methods such as BB-BC, PSO, DE and conventional direct method. Therefore, in this study, time consuming but 100% accurate time domain simulations are used during optimizations.

Differently from previous study, this subsection also handles optimization of a corrective control action, such as load shedding, which is planned to be applied after the occurrence of a contingency, which cannot be cleared by optimum preventive control action. Both preventive and corrective control related optimization problems consider static and dynamic security constraints.

In this study, to reduce the size of the search spaces and the computational burden, decision trees and correlation coefficients are used as feature selection tools, which determine the most effective generators and loads for shaping the system's transient stability. Differently from previous study, the new methodology is applied to 16 generator-68 bus test system.

Flowchart of the methodology is given in Figure 6.9. The methodology includes similar steps with previously explained methodologies. In the first step, critical contingencies are determined as explained in previous studies. In the second step, two KBs are created for preventive and corrective control actions respectively. In previous studies, KBs are used to train the ANNs, now KBs are used to determine relevant control variables (generators and load), which will be used in optimization of control actions. After the creation of knowledgebase and selection of relevant control variables, various population based optimization methods and a conventional optimization method are applied to both preventive and corrective control actions, respectively.

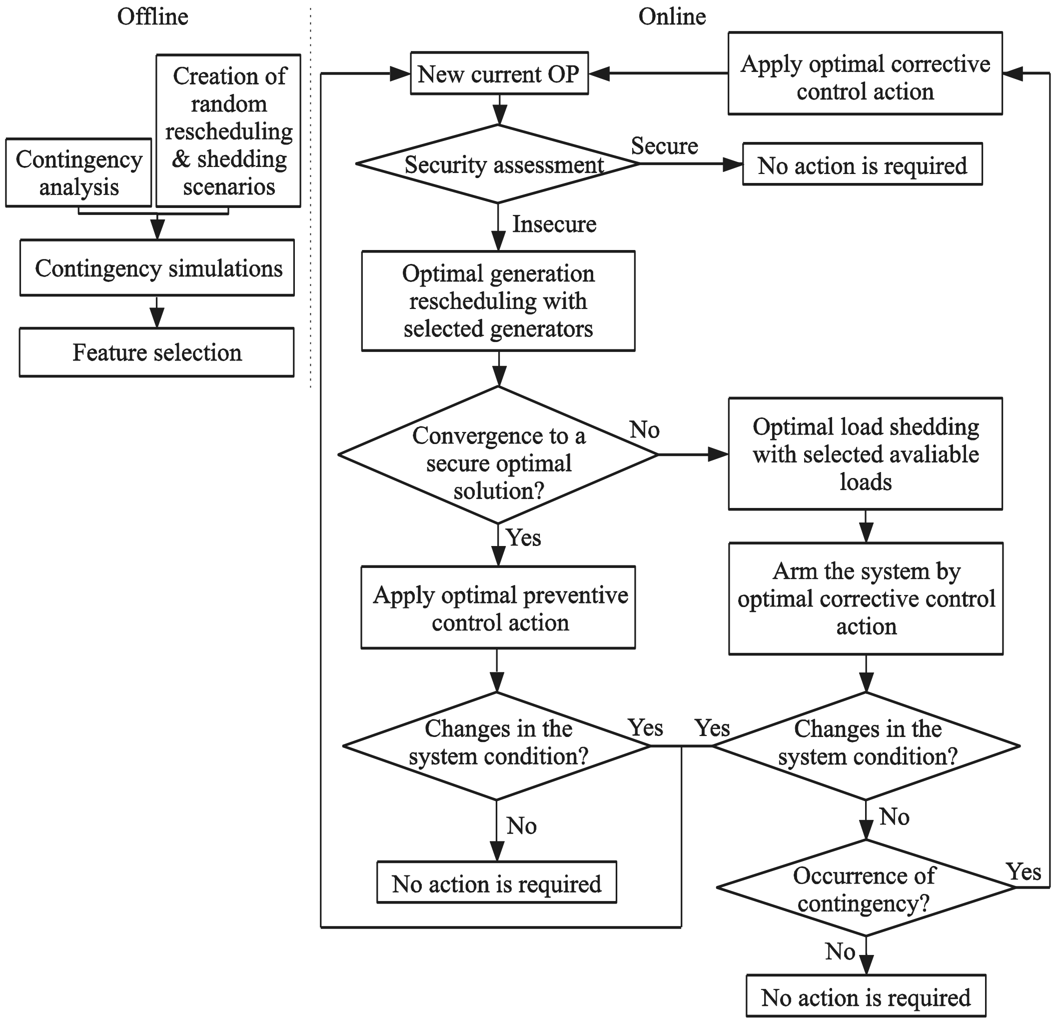


Figure 6.9 : Proposed DSE methodology.

6.3.1 Contingency analysis and creation of knowledge base

Initially, the critical contingencies that have the potential to create transient instabilities are determined by a contingency analysis. As previously explained, extensive time-domain simulations under the credible contingencies are run. The critical contingencies, which are 3-phase-ground faults cleared 5 cycles after their occurrences by a single line tripping but causing transient instabilities, are listed in Table 6.11. Methodology in Section 5 is applied to the same test system, but critical contingency set is different. The 16 generator-68 bus test system is divided into 5 area. Contingency set in Section 5, focuses on the dynamic behavior of generators in the first area (first 9 generators). The initial OP and its power flow solution are modified in that way. Methodology in Section 6 also focuses on the dynamic behavior of generators in the other areas (Generators 10 to 16). It can be seen from the Table 6.11, only the first contingency is related with area 1. Other contingencies are occurred on the tie lines between the areas from 2 to 5.

Table 6.11 : Critical contingencies for 16-generator system.

Contingency no.	3-phase fault close to bus no.	Tripped line (between buses)
1	22	22-21
2	40	40-48
3	51	51-45
4	52	52-50
5	50	50-51
6	40	40-41

The critical contingencies of the test system requiring preventive or corrective control actions are located in the neighborhood of the lines between the buses 52-50, 40-41 and 22-21. The transient stability of the system is strongly related to the real power flows through these lines. These power flows are relatively more sensitive to the real power injections at the buses 58, 59, 65, 66, 67 and 68 to which generators having large inertia constants are connected.

To construct a DT for determining the generators to be rescheduled, LS is generated. LS consist of 5000 randomly created rescheduling schemes where all generators in the system with their output limits are considered. To make a fair comparison between generators in feature selection process, random values of each generator output are generated as they have a uniform distribution with the same variance. The security of the system at each OP and for each critical contingency is determined based on the transient stability index calculated.

6.3.2 Selection of relevant generators and loads

For any critical contingency, the level of impact of generation shifting among different groups of generators on the system's security could differ. Selection of the most contributive generators reduces the dimension of the search space and, thus, increases the performance in security assessment and optimization of control actions. In this paper, both DTs and correlation matrices are utilized to determine the generators that play an important role in shaping the transient stability of the system.

In the DT approach, the LS consist of a range of OPs, each of which is obtained by a possible generation rescheduling, and their corresponding security statuses. Each randomly generated OP is represented by a vector of active power outputs of all generators in the system. If the angle stability is preserved for all critical contingencies at a particular OP, the OP is considered to be secure; otherwise it belongs to the insecure class.

After developing an orthogonal tree through Classification and Regression Trees (CART) methodology, the most contributive generators that significantly change the security of the system are determined by means of calculation of variable importance. All generator outputs are potential splitters for the tree structure constructed by a node-splitting criterion based on improving the purity of the child nodes. Various impurity functions can be defined for calculation of purity [73]. If the proportions of J classes in a node is given by the vector $p = (p_1, \ldots, p_J)$, the entropy based impurity function $I(p)$ of that node can be defined as

$$I(p) = -\sum_{i=1}^{J} p_i \, log p_i \qquad \textbf{(6.13)}$$

Then, the split improvement of the split of a node, leading to a left and a right child node, is calculated as

$$\theta = I(p) - P_L I(p_L) - P_R I(p_R) \qquad \textbf{(6.14)}$$

where p_L and p_R are the proportions of the classes in the left and right child nodes, respectively. P_L is the proportion of the population of left child node sent by the split and $P_R = 1\text{-}P_L$. For the calculation of variable importance, all main splitters as well as surrogates, which mimic or predict the split of the primary variable, along with the resulting improvements are listed and this list is aggregated by variable accumulating improvements. Each improvement value can be scaled according to the largest value in the list.

In this study, beside DTs, the selection of the most contributive generators is also based on correlation coefficients. The degree of linear dependence between two random variables can be measured by correlation [74]. A positive large correlation between two random variables indicates a strong inclination for both variables to increase or decrease together, whereas a negative large correlation shows a strong relation between variables in opposite directions. In this work, for each critical contingency, the sample correlation coefficient between each generator output and the stability index in (4.1) is calculated by using the same OPs generated in the DT approach with the stability indices previously computed. Let G_k be the output of kth generator, S_m is the stability index for mth contingency. The correlation coefficient between the G_k and S_m,

$$r_{km} = \frac{\sum_{i=1}^{n}(G_{k,i}-\bar{G}_k)(S_{m,i}-\bar{S}_m)}{\sqrt{\sum_{i=1}^{n}(G_{k,i}-\bar{G}_k)^2 \sum_{i=1}^{n}(S_{m,i}-\bar{S}_m)^2}}, \quad -1 \le r_{km} \le 1 \qquad \textbf{(6.15)}$$

where n is the size of the sample, $S_{m,i}$ is the stability index of the ith OP under mth contingency and the, $G_{k,i}$ is the output of kth generator of the ith OP, $\overline{S}_m$ and $\overline{G}_k$ are the sample means. During the selection of contributive generators, the absolute values of correlation coefficients are taken into account, because the output of each generator to be rescheduled is assumed to be either increased or decreased for enhancing the stability index.

By using the software CART [75], for each critical contingency, an optimum tree is developed with the splitting criterion defined by the entropy based impurity function, and thus, the significant generators are determined. For each critical contingency, the DT based variable importance associated with each generator output is scaled to 100 and given in Figure 6.10.

The learning set generated for the DT is also used to calculate the correlation coefficients. For each critical contingency, the correlation coefficients between the stability index values and the generator outputs are given in Figure 6.11. Based on the two approaches, the generators that are found to be significant are selected as the generators to be rescheduled. Their output limits and the parameters of fuel cost functions are given in Table 6.12.

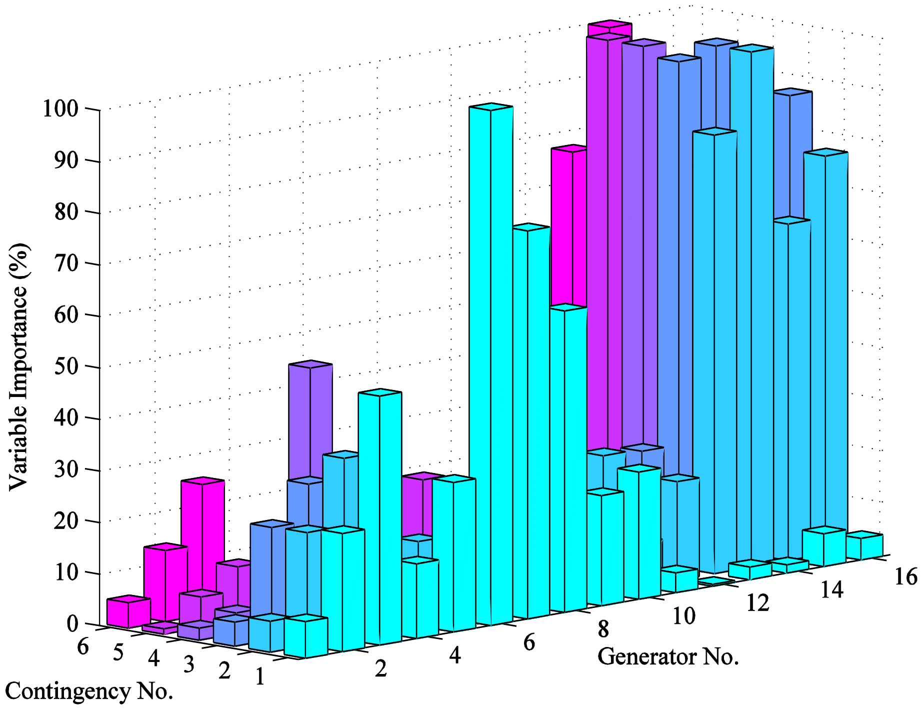


Figure 6.10 : DT based variable importance of generators for each contingency.

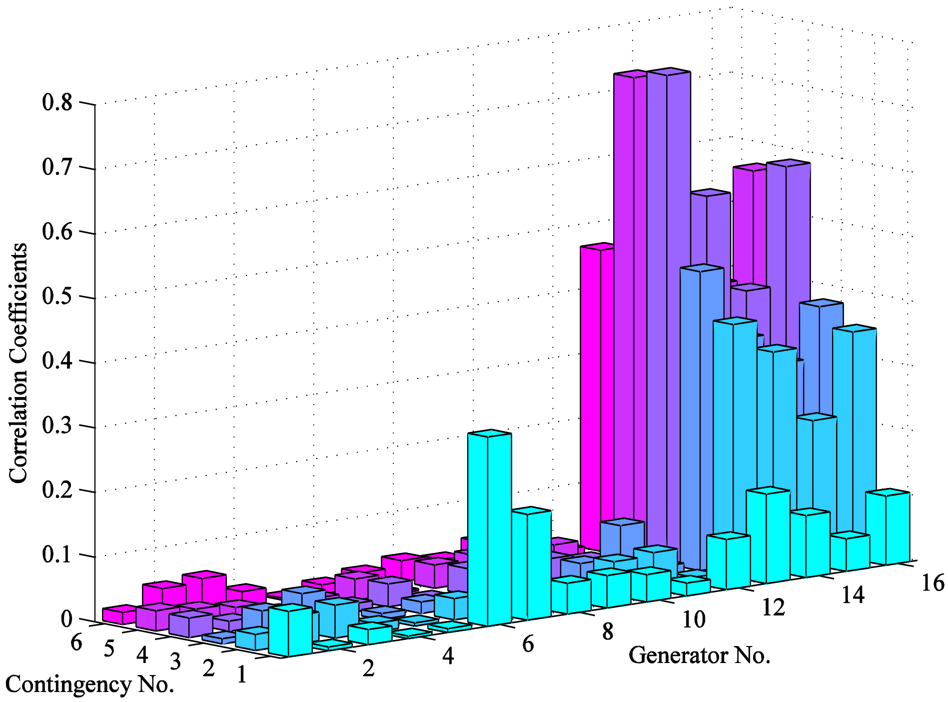


Figure 6.11 : Correlation between the stability index and the generator outputs.

Table 6.12 : Limits and fuel cost function parameters of selected generators.

Generator no.	6	7	13	14	15	16
P_{Gmax} (MW)	1400	1700	12000	5000	4000	5500
a_i ($/MW^{2}h)	0.1	0.11	0.02	0.1	0.04	0.01
b_i ($/MWh)	17	21	9	23	11	9
c_i ($/h)	1500	1500	1300	1600	1900	1800

The procedures applied for the selection of the most contributive loads are similar to the methods proposed in generation rescheduling. In the DT approach, the LS consist of the possible load shedding schemes and the post-contingency security statuses of the system against a single critical contingency. Each randomly generated load shedding scheme is represented by a vector of amounts of load shedding within their possible limits. If the angle stability of the system subjected to the contingency is restored followed by a particular load shedding, the scheme is considered to be secure. Alternatively, the sample correlation coefficients are also utilized for the selection of significant loads to be shed. Unlike the approach in generation rescheduling, only the positive values of correlation coefficients are taken into account, since only the load shedding schemes enhancing the stability index be reasonable.

Among the critical contingencies analyzed, for demonstration purposes, contingency no. 1 is selected to be the contingency against which the load shedding scheme can be thought as a corrective control. Considering the time delays for communication and relay operations, the load shedding is assumed to be executed 5 cycles after the occurrence of the fault. The loads playing a significant role in shaping the transient stability are determined through the two approaches using DT and correlation coefficients. DT based variable importance values (scaled to 0.5) associated with the loads and correlation coefficients between the stability index and each load are given in Figure 6.12.

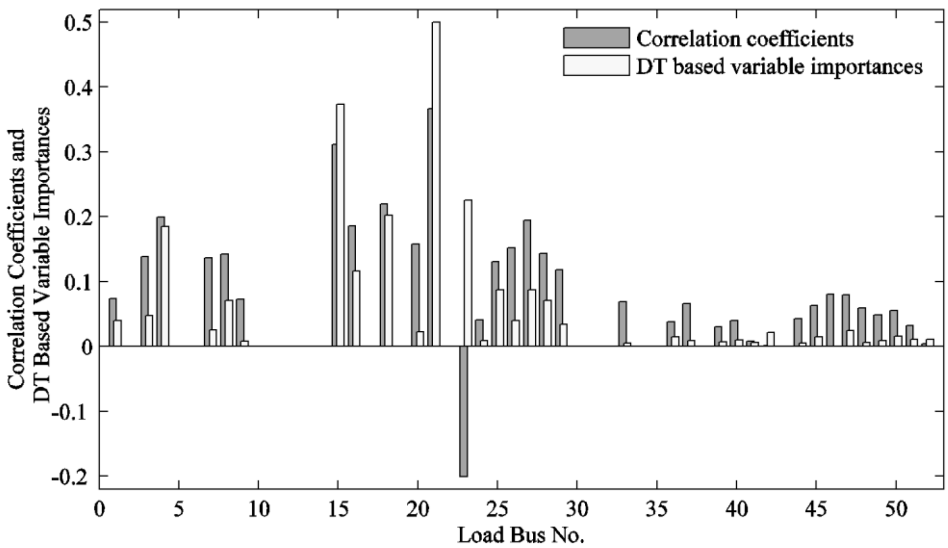


Figure 6.12 : Correlation coefficients and DT based variable importance values of loads.

In both methods, similar loads have high level of impact on regaining the system stability after the occurrence of contingency no. 1. Although, both methods show that the load at bus no. 23 is relevant, a negative high correlation indicates that an increase in load would result in an increase in the stability index. Therefore, the load at that bus is not selected. In contrast to the results found by the DT, the direction of the load shedding effect on the stability index is utilized and distinguished by the correlation coefficients. The selected loads to be shed, their limits and weights are given in Table 6.13.

Table 6.13 : Limits and weights of loads to be shed.

Load no.	Load Bus no.	Initial value (MW)	Weight	Shedding Limit (MW)
1	4	500	0.52	112
2	15	320	0.71	80
3	16	329	0.53	120
4	18	158	0.54	124
5	21	174	0.87	104
6	27	281	0.51	116

The results of the two feature selection methods using correlation coefficients and DTs conform to this anticipation. Moreover, for both of the feature selection methods used in generation rescheduling, the generators playing a significant role in shaping the system security are found to be the same. The use of correlation coefficients turns out to be advantageous in the load shedding method, since the direction of the load shedding effect on the stability index can be distinguished by the correlation coefficients. On the other hand, the DT approach, which ignores this effect, could be misleading when shedding of any load decreases the stability index significantly. The results related to Figure 6.12, exemplify the occurrence of such concern.

6.3.3 Optimization of preventive control action

Security constrained generation rescheduling method is proposed as a preventive control technique against transient instabilities when the current OP is insecure. Generations are shifted among controllable generators, and the power system moves to a secure OP so that the stability of the system is preserved despite the occurrence of a critical contingency. In this procedure, an optimization method that searches the minimum cost for the applied rescheduling strategy is considered. The security constrained generation rescheduling problem can be stated as, *minimize f (x, u) subject to g(x, u)=0 and h(x, u) ≤ 0*

where u represents the active power outputs of generators to be rescheduled (control variables), and the dependent variables of the system due to power flow solutions and time-domain simulations are represented by x. The equality $g(x, u) = 0$ represents the power flow equations and the inequality $h(x, u) \leq 0$ represents the operational constraints involving generation limits and the security criteria.

In the optimization methods used, each candidate solution represents an OP (rescheduling strategy) which is defined by the active power outputs of the $r-1$ independent generators to be rescheduled. The active power output of dependent generator of each solution is determined by a power flow computation. During the optimization processes, the total fuel cost to be minimized,

$$f_{fuel}(x,u) = \sum_{i=1}^{r} f_{Gi} = \sum_{i=1}^{r} a_i\, P_{Gi}^2 + b_i P_{Gi} + c_i \qquad \textbf{(6.16)}$$

where P_{Gi} is the active power output of the ith generator, a_i, b_i, and c_i are the parameters for its fuel cost function. The total fuel cost f is expressed in *\$/h*.

When generation rescheduling is solely dependent on the total fuel cost, the system can be moved to an optimum OP where the selected contingencies for the initial OP are no longer critical, but new critical contingencies may emerge at the new OP. To partially prevent the emergence of new contingencies, a measure of total generation shifting,

$$f_{shift}(x,u) = \|P_G - P_G^0\| = \gamma \sqrt{\sum_{i=1}^{r} \left(P_{Gi} - P_{Gi}^0\right)^2} \qquad \textbf{(6.17)}$$

can also be integrated to the cost function to be minimized. Here, P_G^0 is the vector of generator outputs at the initial OP and γ is a scaling factor assumed in the norm of generation shifting. Then a multi-objective cost function can be defined as

$$f_{mix}(x,u) = \alpha f_{fuel}(x,u) + (1-\alpha) f_{shift}(x,u) \qquad \textbf{(6.18)}$$

where, the weights of the fuel cost and generation shifting are specified by α. Naturally, large values of α results in optimum OPs with low fuel costs, whereas smaller values of α results in optimum OPs that are closer to the initial OP around which the probability of emergence of new critical contingencies is smaller.

To examine the efficiency of optimization methods, solutions with the low cost function values are removed from the initial population and the ability of the methods to avoid being trapped in local optimum points is tested. Since the final solutions of the optimization methods may vary due to the inherent randomness in creating candidate solutions, a number of trials for each method are performed for comparison. The optimization results based on 20 trials for generation rescheduling optimization, and their best solutions are given in Table 6.14 and Figure 6.13. Minimization of $f_{fuel}(x,u)$ during the trials with the best performances of the proposed methods are given in Figure 6.14.

Table 6.14 : Optimization results for generation rescheduling.

Cost function $f_{fuel}(x,u)$ (\$/h)						
	BB-BC$_{120}$	BB-BC	GA	PSO	DE	ASM
Best $f(x,u)$	903587	904614	907580	902189	901960	958060
Mean $f(x,u)$	905788	914583	939639	903712	902595	1047502
Worst $f(x,u)$	909149	921323	965951	907445	904137	1188201
Cost function $f_{mix}(x,u)$						
	BB-BC$_{120}$	BB-BC	GA	PSO	DE	ASM
Best $f(x,u)$	944248	952100	1082300	936170	935385	945411
Mean $f(x,u)$	966091	1006100	1185400	950602	941727	1067076
Worst $f(x,u)$	991920	1060200	1206500	967360	951477	1183701

All population based methods run with population consisting of 30 solutions and maximum 60 iterations. As the best solutions are compared, while the BB-BC method outperforms ASM and GA, the results of PSO and DE are found to be better. However, as seen from the Figure 6.14, the results of BB-BC method can be improved if the iteration goes forward, because the parameters of BB-BC is selected for preventing premature convergence. Therefore, the BB-BC method runs again for 120 iterations and the results are given in the columns of BB-BC$_{120}$ in Table 6.14. A new critical contingency emerges when the system is operated at the optimum points based on fuel cost minimization (α=1): a three phase fault at bus 42 cleared after 5 cycles. On the other hand, when the system is operated at the optimum solution minimizing $f_{mix}(x,u)$ in (6.18), with α=0.4 and γ=764, no additional critical contingency is found. Although the optimization based on the cost function $f_{mix}(x,u)$ can be preferred despite the higher fuel cost implied by its optimum, the approach does not always guarantee the prevention of new contingency emergence which significantly depends on the initial OP. Based on the results of optimization for the fuel cost function, performance of population based optimization methods are better than the ASM method. Although the best solution of ASM for the mixed cost function is comparable with the other methods applied, this solution is attained due to a randomly generated initial point close to the optimum in contrast to the cases for its mean and worst solutions. Results of generation rescheduling optimization show that the performance of BB-BC is slightly less favorable than the performances of PSO and DE but better than those of GA and ASM.

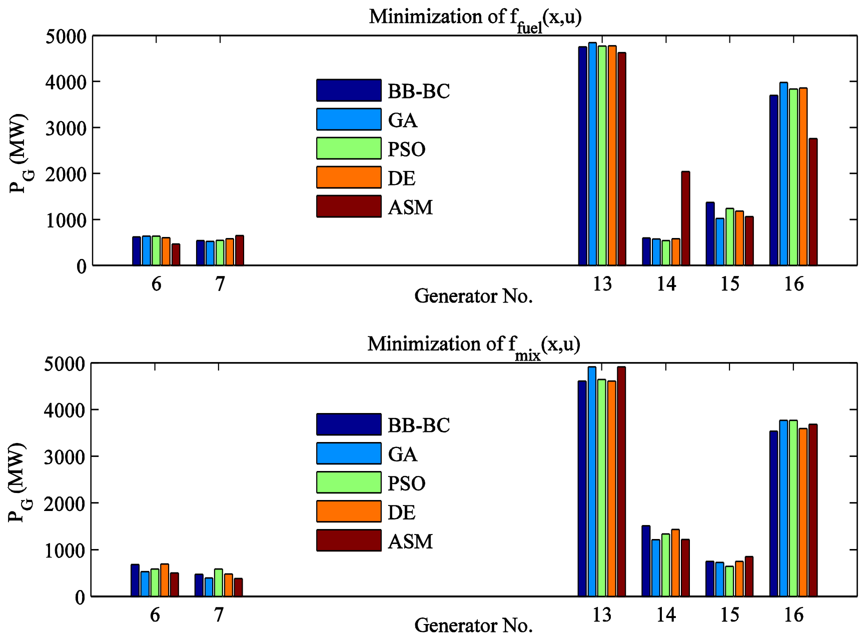


Figure 6.13 : Best solutions of 20 rescheduling trials of the BB-BC, GA, PSO, DE methods and ASM.

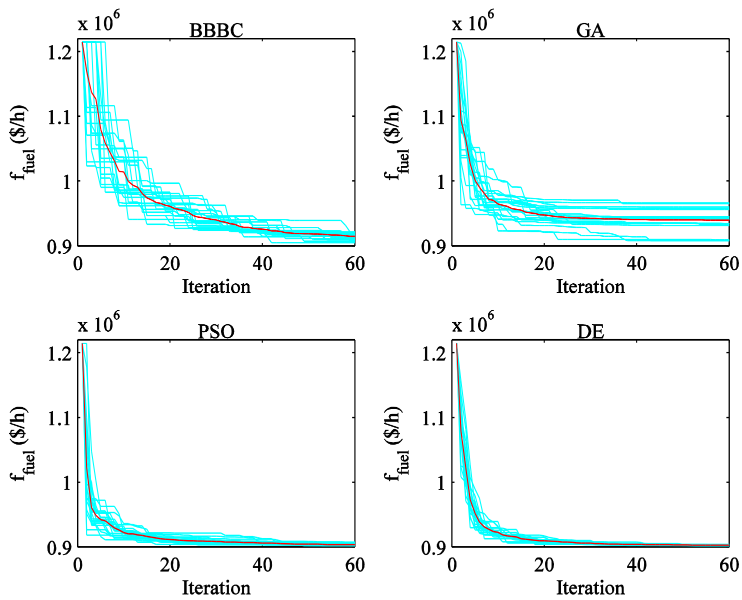


Figure 6.14 : Minimization of cost function f_{fuel} *(x,u)* in 20 trials of the BB-BC, GA, PSO and DE methods.

6.3.4 Optimization of corrective control action

In this study, a security constrained load shedding method is presented as a corrective control action against transient instabilities. After an occurrence of a particular critical contingency, a selected amount of load is shed to regain system stability. The method is applied through an optimization process that searches minimum amount of load to be shed while satisfying the constraints. The optimization problem can be expressed as in (6.19). The objective function is considered as the weighted sum of load shedding,

$$f_{load}(x,u) = \sum_i^{N_L} w_i x_i = \sum_i^{N_L} w_i P_{LSi} = \sum_i^{N_L} w_i \left(P_{Li}^{old} - P_{Li}^{new}\right) \qquad \textbf{(6.19)}$$

where N_L is the number of loads to be shed, ${P_{Li}}^{new}$, ${P_{Li}}^{old}$ are the active power consumptions for the *i*th load bus before and after the load shedding, respectively. The weight w_i is determined based on the priority of the load to be shed. For this optimization problem, now, the control variables are the active power consumptions to be decreased and the operational constraints, $h(x,\ u) \leq 0$ include the stability criteria and shedding limits.

The optimal load shedding problem is solved for a single contingency and each candidate solution is defined by a vector consisting of the selected loads to be shed. Since load shedding is to be performed by switching operations, the control variables, each of which is a load shedding scenario, are discrete.

The optimization results based on 20 trials for load shedding optimization, and their best solutions are given in Table 6.15 and Figure 6.15. For the load shedding, as a discrete optimization, each selected load to be shed is assumed a discrete variable with a fixed step size of 4 MW. As the best cost function values of the optima are compared, the BB-BC method is found to be outperforming all other methods. Although the loads at bus no. 15 and 21 have significantly larger weights than the other loads, larger amounts of loads at these buses are to be shed for the best result of BB-BC optimization. This result is consistent with the outcomes of DT and the correlation coefficients, since these loads are found to be the two most effective loads to be shed against the contingency no. 1.

Table 6.15 : Optimization results for load shedding.

Cost function $f_{load}(x,u)$					
	BB-BC	GA	PSO	DE	ASM
Best *f(x,u)*	244.76	246.80	245.56	245.04	249.28
Mean *f(x,u)*	245.68	248.70	246.65	245.65	252.72
Worst *f(x,u)*	246.44	250.28	248.16	246.52	256.48

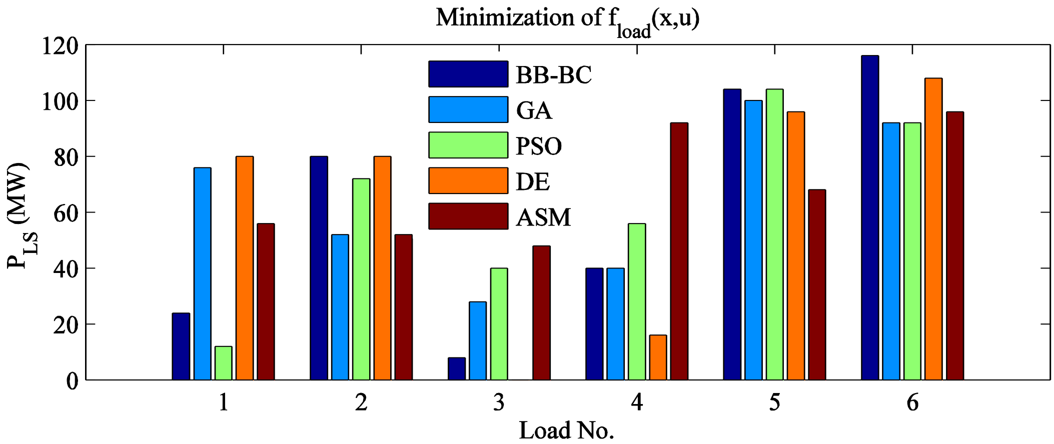


Figure 6.15 : Best solutions of 20 shedding trials of the BB-BC, GA, PSO, DE methods and ASM.

For the load shedding which involves discrete optimization, the population based methods have better results than the ASM method, whereas the BB-BC method shows the best performance among the others that are experimented in this study.

The optimization methods require approximately 3 minutes for the load shedding and about 20 minutes for the generation rescheduling in a modern PC with Intel® Core™ i5-650 processor. For the sake of illustration, time-domain simulations with the load shedding scheme are given in Figure 6.16, where the system's stability is preserved after the corrective action implied by the best solution of the BB-BC method and the frequency of the system is maintained by the speed governors.

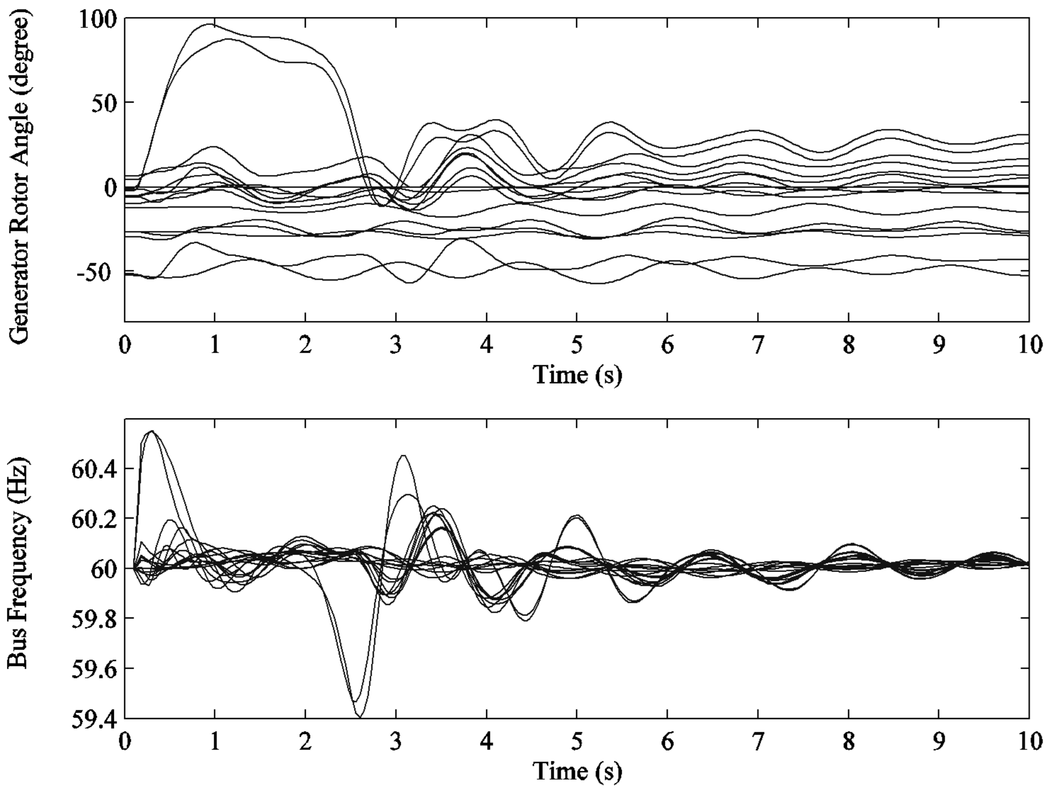


Figure 6.16 : Relative generator angles and bus frequencies when the optimal load shedding is applied.

6.3.5 Optimization under uncertainty

While the optimization methods perform well in the problems considered, their robustness to the uncertainties in the loading conditions are also investigated. To study how well the solutions found by the optimization methods work when the loading conditions are slightly different than the assumed ones, a series of experiments are performed as some uncertainties are added to the deterministic loading condition which was assumed previously.

For the generation rescheduling problem, which optimizes f_{fuel}, a set of three loads which are effective in shaping the transient stability related to all of the critical contingencies has been selected: The loads at the buses no. 40, 42, and 52. A range of uncertainties having a uniform distribution are added the deterministic loading condition as follows:

$$P_{Li} = P_{Li}^{o} + \mathcal{U}(-\varepsilon P_{Li}^{o}, \varepsilon P_{Li}^{o}), \;\; i = 40, 42, 52 \qquad \textbf{(6.20)}$$

where $\mathcal{U}$ represents a uniform distribution, with zero mean, defined on the interval $[-\varepsilon P_{Li}^{o}, \varepsilon P_{Li}^{o}]$, ε is the degree of uncertainty on the real power demand P_{Li}^{o} at bus i.

For a range of degrees of uncertainty between 0%, which is the deterministic case, and 10%, the optimization methods are run and the optimal solutions have been found for 20 different sets of randomly generated load demands (6.20) at each degree of uncertainty. A measure of closeness of the cost of any optimal solution x^* to the cost of optimal solution x^0 for the deterministic loading condition is defined as

$$\kappa(x^*) = \frac{f_{fuel}(x^*) - f_{fuel}(x^0)}{f_{fuel}(x^0)} \times 100 \qquad \textbf{(6.21)}$$

Using the defined measure κ, the boxplot of the data obtained is given in Figure 6.17. The results show that the closeness κ of the optimal costs obtained under uncertainties up to $\varepsilon = 10\%$ lies below 4% for all population-based methods except GA, for which κ may exceed 7%. On the other hand, the closeness κ of the optimal costs obtained by the ASM method takes considerably high values.

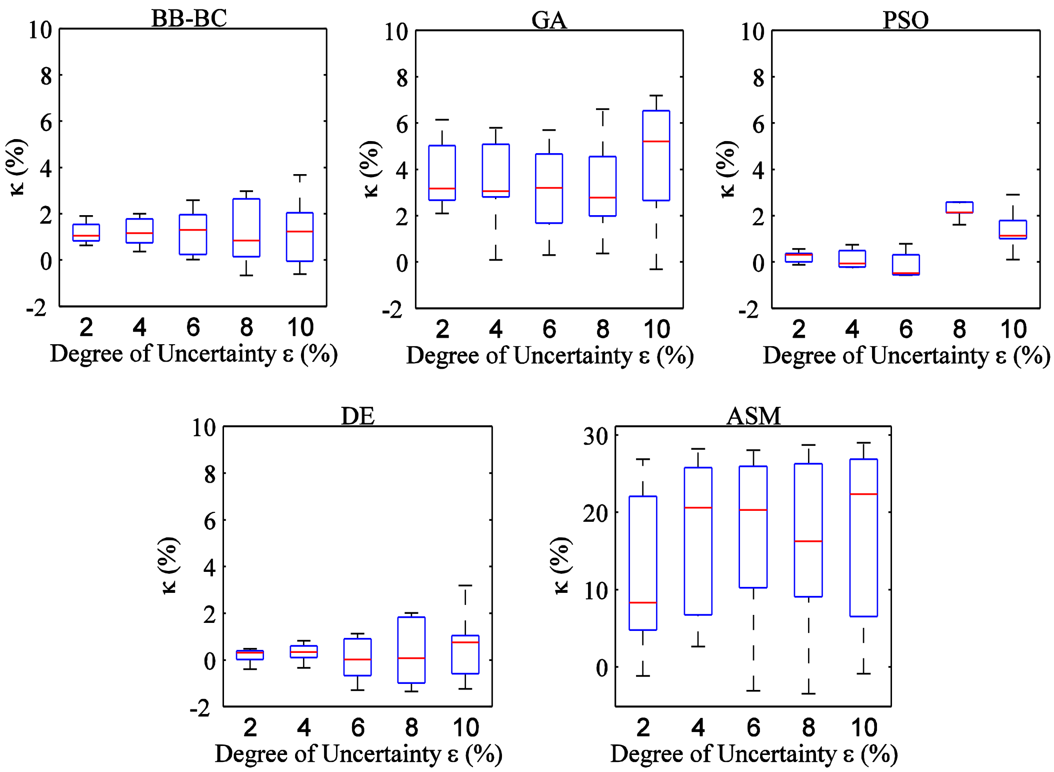


Figure 6.17 : The robustness of the optimization methods under uncertainty.

The results show that the population based methods perform well under the uncertainties of loading conditions, whereas the results of ASM are as expected since the method's performance significantly depends on the initial candidate solutions selected. As the distributions of the optimal costs produced by all methods are investigated, using the population based methods, PSO, DE and BB-BC, are found to be advantageous when an uncertainty in the loading conditions is present.

It is evident that the optimal solution found in the deterministic case could be violating some of the static or dynamic security constraints when the loading conditions are uncertain. However, depending on the degree of uncertainty, as slightly more conservative security constraints are assumed, the population based methods including the BB-BC method can provide quite reliable optimal solutions under uncertainty at which all the security constraints are fully satisfied.

7. DISCUSSIONS, CONCLUSION AND FUTURE WORK

7.1 Discussions and Conclusion

In this study, an efficient methodology is designed to assess and enhance the dynamic security of power systems. Determining suitable and cost effective control actions to enhance the dynamic security is considered as constrained optimization problem. To solve these complex optimization problems, population based optimization methods are proposed. In addition, ANN based dynamic security assessment tools are integrated into the optimization process for estimating the violations of security based constraints faster than the TDS based assessment approach.

7.1.1 Feature selection

Even, small sized test systems investigated in this study, the number of features collected from the system and control variables to be optimized is considerably large. This complexity requires using feature selection process in various steps of DSA and dynamic security enhancement.

In Section 4, RreliefF algorithm selects relevant features to security indexes and these features are used in ANN based regression tasks. Even though selected 20 of 377 features would use by ANNs, the DSA results are satisfactory. This proves the success of feature selection in model based DSA and also increases the importance in online monitoring task where the measurable features are limited.

When feature selection results for each contingency are analyzed, it can be seen that, active power flows through the transmission lines, active power generation, voltage magnitude and voltage angle of buses close the lines where critical contingencies occur, have a large influence on the dynamic security of the system. These expected results confirm the feature selection process.

In section 6.2, feature selection process determines most relevant control variables to enhance the dynamic security of the system against critical contingencies. The critical contingencies of the test system requiring preventive or corrective control actions are located in the neighborhood of the lines between the buses 52-50, 40-41 and 22-21. The transient stability of the system is strongly related to the real power flows through these lines. These power flows are relatively more sensitive to the real power injections at the buses 58, 59 and 65-68 to which generators having large inertia constants are connected. The results of the two feature selection methods using correlation coefficients and DTs conform to this anticipation. Moreover, for both of the feature selection methods used in generation rescheduling, the generators playing a significant role in shaping the system security are found to be the same. The use of correlation coefficients turns out to be advantageous in the load shedding method, since the direction of the load shedding effect on the stability index can be distinguished by the correlation coefficients. On the other hand, the DT approach, which ignores this effect, could be misleading when shedding of any load decreases the stability index significantly. The results related to Figure 6.12, exemplify the occurrence of such concern.

7.1.2 Dynamic security assessment by ANN

In Section 4, DSA is considered as a regression task, and ANN based methodology is proposed for estimation of CCT and minimum damping values. Since there are studies that propose one ANN structure to estimate CCT values for all critical contingencies, these structures show good performance on a small test system. Real power systems involve large sized contingency and topology sets. Thus, one CCT estimator ANN structure may not be able to show desirable regression performance. To deal with that risk, contingencies can be divided into groups such that, each group involves similar contingencies with respect to relevant system behavior in case of their occurrence. On the other hand, one ANN can be designed for each contingency. Although, increasing the number of ANNs designed for DSA may increase the offline computation burden, this process decrease the risk of misdetection of any insecure OP during both online monitoring and optimization of control actions.

According to the low error values achieved in Section 4, MLP results are found to be satisfactory for DSA. On the other hand, the objective function to be minimized during the optimization is designed by economic considerations that are contrary to the system security. Thus, optimization methods try to push the limits of the security constraints to find more economic candidate solutions. In the meantime, the distance between the security boundary and new candidate solutions can be too short such that, even ANNs with low errors, can estimate the CCT values for candidate solutions on the wrong side of the security boundary. To deal with that problem, ANNs should be trained in a conservative way and the final solution of the optimization must be confirmed by TDS that are more accurate than ANNs.

Proposed PNNs in Section 6.1, is found to be promising in DSA. Their accuracy in determining the system's security depends significantly on the training sets as well as their spread parameters. The developed algorithm guarantees an enhancement on the PNN performance if a spread parameter from a proper range is selected. Additionally, large training sets are not feasible, especially for large power systems due to the time-domain and power flow computations required. The proposed TS selection algorithm provides a high execution speed and accuracy in classifying the security of the system as well as it keeps the computational burden limited for large power systems. Although the results show that the developed PNNs have satisfactory overall classification performances, missed alarms may cause security problems during the assessment and the rescheduling processes. The methodology also enables us to decrease the missed alarm rate without decreasing the overall classification performance of the PNN.

Although ANFIS successfully estimates the active power generation at the slack bus for each OP in Section 6.1, ANFIS is not applicable for large power systems applications, due to the size limitations of the input layer of its rule-based structure.

7.1.3 Security constrained optimal control actions

In Section 5, proposed preventive control action is a mixture of generation rescheduling and load curtailment. Although, integration of ANNs speeds up the optimization process, optimization methods need considerable number of iterations to reach optimum solution. Optimization time can be considered suitable, since it is a preventive control action. On the other hand, with the help of constraint handling methods, population based optimization methods can find feasible solutions with relatively higher costs than optimum solutions in just a few minutes, despite of large number of equality and inequality constraints. As a first and fast step of preventive control action, OP of the system can be moved to a one feasible solution that is found in the earlier steps of the optimization. Therefore, this action can prevent the loss of synchronism in case of occurrence of any critical contingency. Then the system can be moved to the final OP, when the optimizations are completed.

This study shows the ability of applied population based optimization methods to enhance the security of the system and satisfy all system constraints, under economic considerations characterized in the objective function. Convergence characteristics, reliability, best solutions and their costs may differ for each optimization methods, but final solutions of optimizations successfully enhance the dynamic security of the system with an acceptable additional cost. In addition, current insecure OP of the system is changed according to the system topology and loading level. When, proposed methodology is applied to various insecure current OPs, optimization methods still can enhance the security of the system. As it is expected, total cost to move the current insecure OP to a new OP where all system constraints are satisfied, differs according to the operating conditions of current insecure OP.

Except MVMO, each optimization method is slightly modified to suit optimization problem mentioned in this study, and they show similar performance. Comparison of proposed optimization methods according to their best solutions and generalization may not be very meaningful. As it is seen in literature, each method can be highly modified, and results according to these modified variants can disproof generalization according to the results of another study. On the other hand, when the structure of optimization methods are investigated, it can be seen that there are similarities between the selection, mutation and crossover operators of different methods, such as DE, ABC, PSO, MVMO and GA. Since BB-BC may differ from other methods according to its searching strategy, it also shows similar performance with other algorithms.

Based on the optimization results in Section 6, for the fuel cost function, performance of population based optimization methods are better than the conventional active set method (ASM). Although the best solution of ASM for the mixed cost function is comparable with the other methods applied, this solution is attained due to a randomly generated initial point close to the optimum in contrast to the cases for its mean and worst solutions. Results of generation rescheduling optimization show that the performance of BB-BC is slightly less favorable than the performances of PSO and DE but better than those of GA and ASM.

For the load shedding which involves discrete optimization, the population-based methods have better results than the ASM method, whereas the BB-BC method shows the best performance among the others that are experimented in this study.

The results also show that the population-based methods perform well under the uncertainties of loading conditions, whereas the results of ASM are as expected since the performance of the method significantly depends on the initial candidate solutions selected. As the distributions of the optimal costs produced by all methods are investigated, using the population-based methods, PSO, DE and BB-BC, are found to be advantageous when an uncertainty in the loading conditions is present.

It is evident that the optimal solution found in the deterministic case could be violating some of the static or dynamic security constraints when the loading conditions are uncertain. However, depending on the degree of uncertainty, as slightly more conservative security constraints are assumed, the population based methods including the BB-BC method can provide quite reliable optimal solutions under uncertainty at which all the security constraints are fully satisfied.

7.2 Future Work

Power system stability and security will maintain its importance, since power transmission through electric power systems go on being more complex for system operators with the increasing penetration of renewable sources, increasing uncertainty of their generation because of their nature and enforcements of energy markets. The aim of this study is developing a framework that involves security assessment and security enhancement tools based on collaboration of artificial intelligent methods and metaheuristic optimization methods.

Although metaheuristic optimization methods show promising results of complex, multidimensional optimization problems of power systems, they generally requires considerable number of function evaluation. These approaches are computationally intensive, although computational effort for a single function evolution can be reduced as it is done in this study. In addition, if parameters of these methods are not carefully adjusted, they cannot guarantee optimality. Despite of high popularity of metaheuristic optimization methods and increasing number of variants of them in every day, these methods should be the alternative step for solving an optimization problem when problem cannot be described well mathematically. It can be worth spending effort to find potential convex relaxations and approximations which may profit sub-optimality (or even better), high speed, less computation effort and efficient results.

Same considerations are also valid for using artificial neural networks, but as mentioned before, structure and operation of power systems is going to be more complex in the future. This may decrease the implementation of methods have a solid mathematical basis and let artificial intelligent methods to continue their popularity. Since, power system become more complex, the size of the data that handled also increases. This may also affects the performance of artificial intelligent methods according to the curse of dimensionality. New features, which are the combination of a set of features, or relationship between some features can be determined by data mining approaches, to deal with mentioned problem.

In this study, MLP is selected as regression tool, and PNN is selected as classification tool for DSA. This study can be extended by comparing various tools for enhancing the accuracy of DSA and security enhancement process.

This study focuses on generation rescheduling, load curtailment and load shedding control actions for enhancing the dynamic security of the system considering small and large disturbance angle stability. This study can be extended by applying other preventive and corrective control actions and investing their cost to enhance the security of the system. In addition, assessment and enhancement of other types of stability issues should be considered as a future study.

In this study, the dynamic security enhancement task is handled by a deterministic approach, which has given high security levels in last decades. This approach considers that risk of each security scenarios is equal. Today's power systems involve participants with different characteristics, targets and behaviors, and then using deterministic approaches may not be reasonable. Probabilistic nature of power system incidents and conditions should be considered. Future studies should go in the direction of risk based security assessment. The approach investigates the probability of unstable condition of the system, and requires intensive computation effort. This drawback can be passed with the help of artificial intelligence methods and recent powerful microprocessors.

REFERENCES

[1] **Makarov, Y.V. & Du, P** et al. (2012). PMU-Based Wide-Area Security Assessment: Concept, Method, and Implementation, *IEEE Transactions on Smart Grid, 3* (3), 1325-1332.

[2] **Andersson, G. & Donalek P.**, et al. (2005). Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance. *IEEE Transactions on Power Systems, 20* (4), 1922-1928.

[3] **Fouad, A.A. & Vittal**, **V.** (1991). *Power System Transient Stability Analysis Using the Transient Energy Function Method*. NJ.: Prentice Hall.

[4] **Anderson, M.P. & Bose, A.** (1983). A Probabilistic Approach to Power System Stability Analysis Power Engineering Review, *IEEE Transactions Power Systems, 3* (8), 25-26.

[5] **Pao, Y. H. & Sobajic**, **D. J.** (1992). Combined use of unsupervised and supervised learning for dynamic security assessment, *IEEE Transactions Power Systems, 7* (2), 878-884.

[6] **Bettiol, A. L., Souza, A., Todesco, J. L. & Tesch Jr, J. R.** (2003). Estimation of Critical Clearing Times Using Neural Networks, *IEEE PowerTech Conference*, Bologna, Italy, June 23-26.

[7] **El-Keib, A. A. & Ma, X.** (1995). Application of Artifical Neural Networks in Voltage Stability Assessment, *IEEE Transactions on Power Systems, 10* (4), 1890-1896.

[8] **Arya, L. D. & Titare, L. S.,** et al. (2007). Probabilistic assessment and preventive control of voltage security margins using artificial neural network, *Electrical Power and Energy Systems, 29*, 99–105.

[9] **Genc, V. M. I., Diao, R. & Vittal, V.,** et al. (2010). Decision Tree-Based Preventive and Corrective Control Applications for Dynamic Security Enhancement in Power Systems, *IEEE Transactions Power Systems, 25* (3), 1611-1619.

[10] **Voumvoulakis, E. M., Gavoyiannis, A. E.,** et al. (2006). Decision Trees for Dynamic Security Assessment and Load Shedding Scheme, *IEEE PES General Meeting*, Montreal, Quebec, Canada, June 18-22.

[11] **Moulin, L. S., da Silva, A. P. A.,** et al. (2004). Support Vector Machines for Transient Stability Analysis of Large-Scale Power Systems, *IEEE Transactions Power Systems 19* (2), 818-825.

[12] **Kucuktezcan, C. F. & Genc, V. M. I.** (2012). A new dynamic security enhancement method via genetic algorithms integrated with neural network based tools, *Electric Power Systems Research 83* (1), 1-8.

[13] **Tessema, B. & Yen, G. G.** (2009). An Adaptive Penalty Formulation for Constrained Evolutionary Optimization, *IEEE Transactions on Systems, Man, and Cybernetics, 39* (3), 565-578.

[14] **Gardner, M. W. & Dorling, S. R.** (1998). Artificial neural networks (the multilayerperceptron)—a review of applications in the atmospheric sciences, *Atmospheric Environment, 32*, 2627-2636.

[15] **Specht**, **D. F.** (1990). Probabilistic neural networks, *Neural Networks, 3*, 109–118.

[16] **Goldberg, D. E.** (1989). *Genetic Algorithms in Search, Optimization and Machine Learning*. Boston, MA.: Addison-Wesley.

[17] **Storn, R. & Price**, **K.** (1997). Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces, *Journal of Global Optimization, 11*, 341–359.

[18] **Kennedy, J. & Eberhart**, **R. C.** (1995). Particle swarm optimization, *IEEE International Conf. on Neural Networks IV*, (pp.1942–1948) Piscataway, NJ.

[19] **Karaboga, D. & Akay, B.** (2009). A Comparative Study of Artificial Bee Colony Algorithm, *Applied Mathematics and Computation, 214*, 108-132.

[20] **Erol, O. K. & Eksin**, **I.** (2006). A new optimization method: big bang-big crunch, *Advances in Engineering Software, 37*, 106-111.

[21] **Erlich, I., Venayagamoorthy G. K., & Nakawiro**, **W.** (2010). A mean-variance optimization algorithm, *in Proc. IEEE World Congress on Computational Intelligence*, Barcelona, Spain, July 18-23.

[22] **IEEE/CIGRE Joint task force on stability terms and definitions**. (2004). Definition and Classification of Power System Stability, *IEEE Transactions on Power Systems, 19* (2), 1387–1401.

[23] **Dy Liacco**, **T. E.** (1968). Control of Power Systems via the Multi-Level Concept, *Case Western Reserve Univ., Systems Res. Center, Rep*. 68-19.

[24] **Kundur, P.** (1994). *Power System Stability and Control.* NY.: McGraw-Hill.

[25] **Taylor, C. W.** (1994). *Power System Voltage Stability*. NY.: McGraw-Hill.

[26] **CIGRE Task Force** (1999). *Analysis and Modeling Needs of Power Systems Under Major Frequency Disturbances*. (Report no.: 38.02.14).

[27] **Chow, Q. B., Kundur, P.,** et al. (1989). Improving nuclear generating station response for electrical grid islanding, *IEEE Transactions on Energy Conversion, 4*, 406–413.

[28] **Rogers, G.** (2000). *Power System Oscillations*, Boston, Kluwer Academic Publishers.

[29] **Browne, T. J., & Vittal, V.,** et al. (2008). A comparative Assessment of Two Techniques for Modal Identification from Power System Measurements, *IEEE Transactions on Power Systems*, *23* (3), 1408 – 1415.

[30] **Sanchez-Gasca, J. J. & Chow, J. H.** (1999). Performance Comparison of Three Identification Methods for the Analysis of Electromechanical Oscillations, *IEEE Transactions on Power Systems, 14* (3), 995 – 1002.

[31] **Wehenkel, L. & Pavella, M**. (2004). Preventive vs. emergency control of power systems, *IEEE PES Power Systems Conference and Exposition*, New York, USA, October 10-13.

[32] **Pavella, M., Ernst D. & Ruiz-Vega, D.** (2000). *Transient Stability of Power Systems: A Unified Approach to Assessment and Control*, Boston: Kluwer Academic Publishers.

[33] **Kehler, J. H.** (2001). Procuring load curtailment for grid security in Alberta *IEEE Power Engineering Society Winter Meeting*, Columbus, Ohio, USA, January 28 – February 1.

[34] **Rosenblatt, F.** (1962). *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms*. Washington, D.C.: Spartan Books.

[35] **Specht, D. F.** (1990). Probabilistic Neural Networks, *Neural Networks, 3*, 109-118.

[36] **Park, J.** (1991). Universal Approximation Using Radial-Basis-Function Networks, *Neural Computation, 3*, 246-257.

[37] **Specht, D. F.** (1991). A General Regression Neural Network, *IEEE Transactions on Neural Networks, 2*, 568-576.

[38] **Kohonen, T.** (1997). *The self-organizing map.* Berlin: Springer.

[39] **Kohonen, T.** (1995). *Learning vector quantization, in: The Handbook of Brain Theory and Neural Networks.* pp: 537–540. MA.: MIT Press.

[40] **Dayhoff, J. E.** (1990). *Neural Network Architecture: an Introduction*. NY.: Van Nostrand Reinhold Co.

[41] **Haykin, S.** (1998). *Neural Networks - A Comprehensive Foundation*. Upper Saddle River, NJ.: Prentice – Hall.

[42] **Hopfield, J. J.** (1982). Neural networks and physical systems with emergent collective computational abilities, *Proceedings of the National Academy of Sciences of the USA, 79*, 2554-2558.

[43] **Jaeger, H.** (2001). *The Echo State Approach to Analyzing and Training Recurrent Neural Networks*, GMD Report 148 - German National Research Institute for Computer Science.

[44] **Elman, J. L.** (1990). Finding Structure in Time, *Cognitive Science, 14*, 179-211.

[45] **Carpenter, G. A., Grossberg, S. & Reynolds, J. H.** (1995). A fuzzy ARTMAP nonparametric probability estimator for nonstationary pattern recognition problems, *IEEE Transactions on Neural Networks, 6* (6), 1330-1336.

[46] **Gopalsamy, K.** (1994). Delay-independent stability in bidirectional associative memory networks, *IEEE Transactions on Neural Networks, 5*, 998-1002.

[47] **Bishop, C. M.** (1996). *Neural Networks for Pattern Recognition*. Oxford: Clarendon Press.

[48] **Micheli-Tzanakou, E.** (1999). *Supervised and Unsupervised Pattern recognition: Feature Extraction and Computational Intelligence.* Florida: CRC Press.

[49] **Battiti, R.** (1992). First and second-order methods for learning: Between steepest descent and Newton's method, *Neural Computing, 4*, 141–166.

[50] **Jang, J. S. R.** (1993). ANFIS: Adaptive-Network-Based Fuzzy Inference System, *IEEE Transactions on Systems and Cybernetics*, *23* (3), 665-685.

[51] **Bonabeau, E., Dorigo, M., & Theraulaz, G.** (1999). *Swarm intelligence: From Natural to Artificial Systems*. NY.: Oxford University Press.

[52] **Rueda, J. L. & Erlich, I.** (2013). Hybrid Mean-Variance Mapping Optimization for Solving the IEEE-CEC 2013 Competition Problems, *IEEE Congress on Evolutionary Computation,* Cancún, México, June 20-23.

[53] **Michalewicz, Z.** (1995). A Survey of Constraint Handling Techniques in Evolutionary Computation Methods, *The 4th Annual Conference on Evolutionary Programming*, (pp.135-155), San Diego, CA., USA, March 1-4.

[54] **Michalewicz, Z.**, (1996). Genetic algorithms, numerical optimization and constraints, T*he 6th international conference on genetic algorithms*, (pp.151-158).

[55] **Tessema, B., Yen, G. G**. (2006). A self adaptive penalty function based algorithm for constrained optimization, *IEEE Congr. Evolut. Comput*. (pp.246-253), Vancouver, BC., Canada.

[56] **Caruana, R. & Nicules-Mizil, A.** (2006). An empirical comparison of supervisedlearning algorithms, *in Proceedings of the 23rd international conference on Machine learning*, (pp.161-168), New York, NY, USA, June 25-29.

[57] **TSAT User Manual**, Powertech Labs, Inc., Surrey, BC, Canada.

[58] **DSATools™**, (Version 14) [Computer software]. Surrey, BC, Canada.

[59] **Hoballah, A. & Erlich, I.** (2010). A Framework for Enhancement of Power System Dynamic Behavior, *IEEE PES General Meeting*, Minneapolis, MN, USA, July 25-29.

[60] **Hunt, E. B., Martin, J. & Stone, P. J**. (1966). *Experiments in Induction*. NY.: Academic Press.

[61] **Breiman, L. & Friedman, J.** et al. (1984). *Classification and Regression Trees*. Belmont, CA: Wadsworth Inc.

[62] **Mantaras, R. L.** (1989). ID3 revisited: A distance based criterion for attribute selection. *Int. Symp. Methodologies for Intelligent Systems*. Charlotte, North Carolina, USA, October.

[63] **Smyth, P., & Goodman, R. M.** (1990). *Rule induction using information theory*. MA.: MIT Press.

[64] **Kira, K. & Rendell, L. A.** (1992). A practical approach to feature selection, *in Proceedings of International Conference on Machine Learning*, (pp.249–256).

[65] **Kononenko, I.** (1994). Estimating attributes: Analysis and extensions of Relief. *in Proceedings of the European conference on machine learning on Machine Learning*, (pp.171–182), Catania, Italy, April 6-8.

[66] **Kononenko, I.** (1995). On biases in estimating multi-valued attributes. *In Proceedings of the International Joint Conference on Artificial Intelligence*, (pp.1034–1040), Montreal, Quebec, Canada, August 20-25.

[67] **Robnik, S. M. & Kononenko, I.** (1997). An adaptation of relief for attribute estimation in regression, *in Proceedings of the Fourteenth International Conference on Machine Learning*, (pp.296–304), Nashville, TN, USA.

[68] **Robnik, S. M. & Kononenko, I.** (2003). Theoretical and Empirical Analysis of ReliefF and RReliefF, *Machine Learning, 53*, 23–69.

[69] **Seymour, G.** (1993). *Predictive Inference*. NY.: Chapman and Hall.

[70] **University of Washington, IEEE test case archive**. Retrieved 14.07.2011, from: http://www.ee.washington.edu/research/pstca/

[71] **Kucuktezcan C. F. & Genc**, **V. M. I.** (2015). Preventive and Corrective Control Applications in Power Systems via Big Bang-Big Crunch Optimization, *International Journal of Electrical Power & Energy Systems, 67*, 114-124.

[72] **Kucuktezan, C. F. & Genc, V. M. I.** (2010). Dynamic Security Assessment of a Power System Based on Probabilistic Neural Networks, *IEEE ISGT Europe*, Gothenburg, Sweden.

[73] **CART for Windows V5.0**—User's Guide, Salford Systems, San Diego, CA.

[74] **Gibbons, J. D.** (2003). *Nonparametric Statistical Inference*. NY.: M. Dekker.

[75] **Salford Systems, CART Software**, (2012). Retrieved 18.08.2012, available from http://www.salfordsystems.com

APPENDICES

APPENDIX A: Results of feature selection process for 13 MLP structures
APPENDIX B: Detailed results of optimization of preventive control action

APPENDIX A: Results of feature selection process for 13 MLP structures

Table A.1 : Estimations of the feature quality for each contingency.

	Contingency 1		Contingency 2		Contingency 3	
Ranking	W	Feature name	W	Feature name	W	Feature name
1	0.03605419	Pg54_2	0.0350113	Pg54_2	0.02730899	Pg54_2
2	0.03278029	Pli5_6_111	0.0316308	Pli5_6_111	0.01979087	Pli4_5_109
3	0.0223759	Qg54_18	0.0205791	Qg54_18	0.01909328	Pli5_6_111
4	0.0180085	Pli7_8_115	0.0198592	Pli5_8_112	0.01860755	Pli13_14_120
5	0.0176387	Pli6_7_113	0.018623	Pli7_8_115	0.01853154	Pli10_13_119
6	0.01709861	Pli5_8_112	0.0184568	Pli6_7_113	0.01644363	Qg54_18
7	0.01536413	Vm54_290	0.0142101	Vm54_290	0.01437477	Pg55_3
8	0.01316262	Pli3_4_107	0.0123796	Pli4_5_109	0.01246925	Pli6_11_114
9	0.01311562	Pli10_13_119	0.0121457	Qli5_6_178	0.01234964	Pli10_11_118
10	0.0130604	Pli13_14_120	0.0116611	Pli10_13_119	0.01028552	Pli4_14_110
11	0.01280676	Pli4_5_109	0.0115775	Va54_358	0.01025237	Pli3_4_107
12	0.01274605	Va54_358	0.0115315	Pli13_14_120	0.01009276	Va54_358
13	0.01135714	Pg55_3	0.0115134	Pg55_3	0.01004452	Pgdf_1_373
14	0.01075334	Pgdf_1_373	0.0114379	Pli3_4_107	0.0098692	Vm54_290
15	0.00982833	Vm6_242	0.0112637	Qli7_8_182	0.00902194	Vm41_277
16	0.00969986	Qli10_11_185	0.0107704	Pgdf_1_373	0.00893077	Qg55_19
17	0.00943107	Vm8_244	0.0107124	Qli6_7_180	0.0082679	Qli8_9_183
18	0.00933423	Qg55_19	0.0097758	Vm7_243	0.00818175	Vm7_243
19	0.0091917	Vm10_246	0.0095481	Vm8_244	0.0081353	Vm10_246
20	0.00910679	Vm7_243	0.0091884	Vm41_277	0.00798127	Vm6_242
21	0.00906651	Qli7_8_182	0.0091756	Qli5_8_179	0.00784297	Vm8_244
22	0.00891049	Vm5_241	0.0091125	Vm6_242	0.00768976	Qli10_11_185
23	0.00870577	Qli8_9_183	0.0090492	Pli8_9_116	0.00751307	Qg65_29
24	0.00850121	Qli6_11_181	0.0089997	Qli8_9_183	0.00714184	Qli14_15_188
25	0.00821434	Qli5_6_178	0.0089325	Qg55_19	0.00711049	Pli8_9_116
26	0.00811455	Pli8_9_116	0.0087556	Qli10_11_185	0.00700568	Vm4_240
27	0.00785535	Pli14_15_121	0.0087395	Vm10_246	0.00672339	Vm5_241
28	0.00767474	Vm41_277	0.0077926	Qli6_11_181	0.00659062	Qli4_5_176
29	0.00733112	Vm11_247	0.0071081	Vm5_241	0.00656755	Vm14_250
30	0.00672066	Pli6_11_114	0.0067962	Qg65_29	0.00640597	Qli3_4_174
31	0.00670245	Pli10_11_118	0.0067549	Vm11_247	0.00614562	Qli6_11_181
32	0.00665658	Vm14_250	0.0066708	Vm14_250	0.00597265	Vm21_257
33	0.00664814	Vm13_249	0.0065762	Vm21_257	0.00571403	Vm23_259
34	0.0066343	Vm4_240	0.0062763	Vm4_240	0.00563858	Vm11_247
35	0.00611122	Vm21_257	0.0062653	Pli10_11_118	0.00532509	Pli14_15_121
36	0.00593805	Qg65_29	0.00622	Pli6_11_114	0.00524979	Vm13_249
37	0.00588215	Pli15_16_122	0.0061204	Vm13_249	0.00477816	Vm12_248
38	0.00565577	Qli14_15_188	0.0061019	Pli14_15_121	0.0047546	Qli15_16_189
39	0.00556492	Vm12_248	0.0054269	Vm12_248	0.00474004	Va55_359
40	0.00553425	Qli5_8_179	0.005176	Vm23_259	0.0046935	Qli7_8_182
41	0.00545611	Qli6_7_180	0.0051171	Vm16_252	0.00468637	Vm16_252
42	0.00538798	Va55_359	0.0049737	Pg56_4	0.00465288	Qli5_6_178
43	0.0052405	Vm23_259	0.0048131	Va55_359	0.0044974	Vm15_251
44	0.00513273	Qli3_4_174	0.0046936	Vm15_251	0.00402326	Plo49_64
45	0.00512625	Qli4_5_176	0.0046003	Pli15_16_122	0.00388132	Qli2_3_172
46	0.00502375	Vm15_251	0.004531	Qli3_4_174	0.00371962	Pg56_4
47	0.00490026	Pg56_4	0.004269	Plo49_64	0.00370757	Pli6_7_113
48	0.00479343	Qli15_16_189	0.0042576	Pg53_1	0.00361157	Va6_310
49	0.00477175	Vm16_252	0.0041784	Vm56_292	0.00359056	Plo44_59
50	0.00465899	Va7_311	0.0041277	Qli4_5_176	0.00356518	Qlo44_94
51	0.00435391	Va6_310	0.0039874	Qg53_17	0.00354898	Pli15_16_122
52	0.00430771	Pg60_8	0.0039824	Qli15_16_189	0.00353542	Plo45_60
53	0.00427349	Vm56_292	0.0038281	Pg60_8	0.00351151	Qli6_7_180
54	0.00397666	Va11_315	0.0037688	Va6_310	0.00348417	Qli5_8_179

Table A.1 (continued) : Estimations of the feature quality for each contingency.

	Contingency 4		Contingency 5		Contingency 6	
Ranking	W	Feature name	W	Feature name	W	Feature name
1	0.04900955	Pg55_3	0.0438873	Pg55_3	0.0226221	Pli21_22_129
2	0.01215511	Qg55_19	0.0203399	Pli10_13_119	0.0223305	Qli8_9_183
3	0.01183531	Pli10_13_119	0.019264	Pli13_14_120	0.0215341	Pli23_24_131
4	0.01081332	Pli10_11_118	0.0135331	Pli10_11_118	0.0209933	Pg58_6
5	0.01047068	Pli13_14_120	0.0127846	Pli6_11_114	0.0206767	Pli16_21_125
6	0.0095848	Pli6_11_114	0.012144	Qg55_19	0.0203352	Qg58_22
7	0.0087419	Vm41_277	0.0111314	Pli4_5_109	0.017376	Vm23_259
8	0.00826837	Qg65_29	0.0106571	Qli8_9_183	0.0156348	Vm21_257
9	0.0078903	Pgdf_1_373	0.0102623	Qli14_15_188	0.0150812	Qg59_23
10	0.00730177	Qli8_9_183	0.0100119	Pli5_6_111	0.0141392	Pli16_24_126
11	0.00652337	Vm10_246	0.0085325	Pli4_14_110	0.0138716	Qli7_8_182
12	0.00645894	Vm6_242	0.0076014	Pgdf_1_373	0.0136773	Pli23_59_132
13	0.00587202	Qg54_18	0.0075738	Qg54_18	0.013677	Pg59_7
14	0.00567161	Vm8_244	0.0072736	Qg65_29	0.0133902	Pg56_4
15	0.00548871	Va55_359	0.0071089	Vm10_246	0.0133142	Vm15_251
16	0.00511268	Vm7_243	0.0069488	Vm6_242	0.0132405	Pgdf_1_373
17	0.00483142	Vm23_259	0.0067029	Vm8_244	0.0131391	Vm22_258
18	0.00472576	Vm12_248	0.0066281	Qli3_4_174	0.0130669	Qli5_8_179
19	0.00468067	Vm5_241	0.0066037	Vm41_277	0.0119506	Vm16_252
20	0.00464426	Pli5_6_111	0.0065624	Qli7_8_182	0.0117697	Vm58_294
21	0.00464144	Vm11_247	0.0064254	Qli15_16_189	0.0117259	Qli23_24_198
22	0.00458497	Vm14_250	0.0063591	Vm7_243	0.0116808	Qli16_21_192
23	0.00441639	Qli15_16_189	0.0062152	Qli4_5_176	0.0114335	Pli16_17_123
24	0.00431995	Vm13_249	0.0059456	Qli6_11_181	0.0110439	Vm41_277
25	0.00421688	Vm4_240	0.0057964	Vm4_240	0.0110039	Vm10_246
26	0.00403169	Qli6_11_181	0.0056477	Vm14_250	0.0108816	Pli16_19_124
27	0.00400796	Plo49_64	0.0054916	Vm5_241	0.0107944	Vm8_244
28	0.00399877	Qli7_8_182	0.0054656	Qli5_8_179	0.0106544	Vm5_241
29	0.0039232	Qli38_46_217	0.0054338	Va55_359	0.0104012	Vm24_260
30	0.00382872	Qli3_4_174	0.0051172	Vm12_248	0.0102981	Qg56_20
31	0.00372791	Qli14_15_188	0.0049907	Pg54_2	0.0102495	Vm12_248
32	0.00368727	Vm21_257	0.004893	Vm11_247	0.0101135	Qli14_15_188
33	0.00368349	Vm15_251	0.0048721	Qli10_11_185	0.0098759	Vm4_240
34	0.00360173	Plo21_44	0.0048458	Vm13_249	0.009797	Pli22_23_130
35	0.00332711	Vm16_252	0.0043946	Pli3_4_107	0.0096781	Qli23_59_199
36	0.00329505	Qli46_49_218	0.0042073	Vm23_259	0.0096328	Vm7_243
37	0.0032619	Plo45_60	0.0039411	Qli6_7_180	0.0091372	Qg54_18
38	0.00324971	Qli5_8_179	0.0036062	Va54_358	0.0090398	Qli22_23_197
39	0.003147	Qlo20_78	0.0035097	Plo49_64	0.0088377	Vm6_242
40	0.00312959	Pg68_16	0.0034736	Pli8_9_116	0.0088276	Va58_362
41	0.00310263	Qlo23_80	0.0033214	Vm15_251	0.0087977	Qli6_7_180
42	0.003095	Plo27_49	0.0031985	Qlo51_101	0.008672	Qg55_19
43	0.00304184	Plo37_54	0.0031422	Plo21_44	0.0086714	Vm56_292
44	0.00302592	Pgdf_5_377	0.003126	Plo45_60	0.0086655	Va59_363
45	0.00293528	Vm46_282	0.0031123	Qlo20_78	0.0084551	Vm13_249
46	0.00292659	Plo47_62	0.0030968	Qli38_46_217	0.0084077	Qli6_11_181
47	0.00292311	Pg54_2	0.0028655	Plo44_59	0.0080732	Vm11_247
48	0.00291107	Pgdf_2_374	0.0028629	Vm21_257	0.0080047	Vm19_255
49	0.0028829	Qlo51_101	0.00282	Plo27_49	0.0079784	Vm40_276
50	0.00287107	Pli3_4_107	0.0027908	Plo41_57	0.0079502	Vm14_250
51	0.0028534	Plo41_57	0.0027526	Plo47_62	0.0078986	Qli41_40_235
52	0.00281164	Qlo18_77	0.0027104	Qli5_6_178	0.0078443	Pg53_1
53	0.00279497	Plo33_52	0.0026762	Qlo23_80	0.0078436	Qg53_17
54	0.00278999	Plo44_59	0.0025839	Plo33_52	0.0075429	Qli2_3_172
55	0.00278968	Qlo25_82	0.0025744	Plo37_54	0.0073852	Qli10_11_185
56	0.00278682	Qlo36_88	0.0025626	Vm16_252	0.0073257	Qli4_5_176
57	0.00278459	Qlo16_76	0.0025326	Pli14_15_121	0.0072754	Qli21_22_196

Table A.1 (continued) : Estimations of the feature quality for each contingency.

	Contingency 7		Contingency 8		Contingency 9	
Ranking	W	Feature name	W	Feature name	W	Feature name
1	0.02518429	Pli21_22_129	0.0363171	Pli16_21_125	0.0253305	Pli21_22_129
2	0.02401638	Pli23_24_131	0.0357162	Pli21_22_129	0.0241754	Pli23_24_131
3	0.02396745	Pg58_6	0.0355273	Pli23_24_131	0.0231069	Pg58_6
4	0.02378138	Pli16_21_125	0.0332136	Pg58_6	0.0229295	Pli16_21_125
5	0.02199981	Qg58_22	0.0280618	Qg58_22	0.0209295	Qg58_22
6	0.01909615	Pg56_4	0.0256291	Pli16_24_126	0.0183279	Vm23_259
7	0.01784751	Vm23_259	0.0214081	Qli16_21_192	0.016309	Qg59_23
8	0.01608686	Pli16_24_126	0.02063	Vm58_294	0.0160137	Pli23_59_132
9	0.01601342	Qg59_23	0.0203255	Pli23_59_132	0.0160109	Pg59_7
10	0.0157823	Vm21_257	0.0203198	Pg59_7	0.0154422	Vm21_257
11	0.01561441	Pli16_19_124	0.0202976	Qg59_23	0.0154113	Pli16_24_126
12	0.01512934	Pli23_59_132	0.020119	Vm23_259	0.0137118	Pgdf_1_373
13	0.01512527	Pg59_7	0.0182749	Pg56_4	0.0133877	Qli16_21_192
14	0.01440537	Vm58_294	0.0175483	Pli16_19_124	0.0125068	Vm58_294
15	0.01399995	Vm56_292	0.0169159	Pli22_23_130	0.0124689	Vm22_258
16	0.01356864	Pgdf_1_373	0.0161867	Vm21_257	0.0122403	Vm15_251
17	0.01327973	Vm22_258	0.0157465	Qli22_23_197	0.0121662	Pg56_4
18	0.01292283	Qg56_20	0.0152956	Vm22_258	0.0109261	Vm16_252
19	0.01244175	Qli16_21_192	0.0152839	Vm56_292	0.0107862	Pli22_23_130
20	0.01242694	Pli16_17_123	0.0140562	Qli23_24_198	0.0096987	Qg65_29
21	0.01223744	Vm15_251	0.0137105	Qli23_59_199	0.0096505	Qli23_24_198
22	0.01164465	Pli22_23_130	0.0120313	Qg56_20	0.0095963	Vm24_260
23	0.01130217	Vm16_252	0.0116363	Pgdf_1_373	0.0095375	Qg56_20
24	0.01114267	Qli23_24_198	0.0114985	Vm19_255	0.0095179	Pli16_19_124
25	0.01077413	Qli22_23_197	0.0110652	Va58_362	0.00942	Qli22_23_197
26	0.01047403	Qli23_59_199	0.010919	Vm15_251	0.0093947	Qli8_9_183
27	0.01040815	Vm19_255	0.0105067	Va59_363	0.0093103	Qli23_59_199
28	0.00992752	Va58_362	0.0101294	Vm16_252	0.0091231	Vm41_277
29	0.00979513	Vm24_260	0.0098859	Qli21_22_196	0.0089653	Va58_362
30	0.00967931	Pli15_16_122	0.0088309	Vm24_260	0.0089219	Va59_363
31	0.00966908	Va59_363	0.0087792	Pli16_17_123	0.0085892	Pli16_17_123
32	0.00961029	Qg57_21	0.0086311	Qg57_21	0.008379	Vm56_292
33	0.0089443	Qg65_29	0.0083202	Vm59_295	0.0082098	Vm10_246
34	0.00888407	Vm41_277	0.0082183	Qg65_29	0.0081786	Vm19_255
35	0.00846895	Va56_360	0.0079248	Vm20_256	0.0078888	Vm12_248
36	0.00801882	Vm10_246	0.0078788	Va22_326	0.0072929	Qg57_21
37	0.00770769	Va22_326	0.0073423	Vm41_277	0.0072283	Vm5_241
38	0.00749637	Qli21_22_196	0.0073373	Va23_327	0.0071573	Vm4_240
39	0.00744146	Vm12_248	0.0071593	Pli15_16_122	0.0070059	Pli15_16_122
40	0.00743095	Vm20_256	0.006261	Va56_360	0.0067927	Va22_326
41	0.00730237	Va23_327	0.0062465	Vm10_246	0.0064755	Qli21_22_196
42	0.00715432	Va57_361	0.0057165	Vm12_248	0.0064738	Qg53_17
43	0.00675858	Pli14_15_121	0.0053664	Pg57_5	0.0064044	Va23_327
44	0.00673538	Vm4_240	0.0053636	Qli14_15_188	0.006196	Vm20_256
45	0.0066008	Pg57_5	0.0053442	Vm17_253	0.006194	Vm40_276
46	0.00649032	Va19_323	0.0053175	Plo8_37	0.0061633	Pg53_1
47	0.00640961	Va20_324	0.0051621	Va21_325	0.0060836	Qli41_40_235
48	0.00635789	Vm5_241	0.0051234	Vm57_293	0.0060785	Vm8_244
49	0.0063506	Plo8_37	0.0051054	Vm4_240	0.0060784	Vm17_253
50	0.00595751	Vm17_253	0.0050184	Va57_361	0.0060681	Qg55_19
51	0.00589041	Qli14_15_188	0.0048937	Qli16_19_191	0.0059435	Va67_371
52	0.00579956	Va21_325	0.0047826	Vm5_241	0.0059386	Va42_346
53	0.00570326	Vm59_295	0.0045543	Qli16_24_193	0.0058776	Plo8_37
54	0.00559737	Qli8_9_183	0.0044896	Plo4_35	0.0058712	Vm7_243
55	0.00549655	Vm14_250	0.0044863	Va20_324	0.0058251	Va56_360
56	0.00545541	Qg54_18	0.0044221	Va19_323	0.0058115	Vm59_295
57	0.00541103	Qg55_19	0.0042753	Vm18_254	0.0057847	Qg54_18

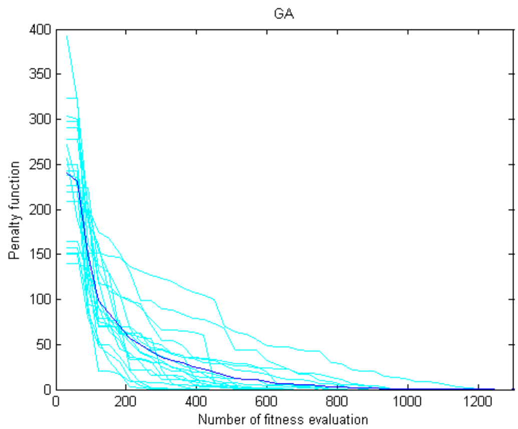
Table A.1 (continued) : Estimations of the feature quality for each contingency.

	Contingency 10		Contingency 11		Contingency 12	
Ranking	W	Feature name	W	Feature name	W	Feature name
1	0.05124663	Pg58_6	0.0627123	Pli21_22_129	0.060396821	Pli23_24_131
2	0.03971124	Pli21_22_129	0.0623822	Pli16_21_125	0.053229037	Pli23_59_132
3	0.03848305	Pli16_21_125	0.0612383	Pli23_24_131	0.053197953	Pg59_7
4	0.03672211	Qg58_22	0.0605618	Pg58_6	0.050451234	Pli16_24_126
5	0.03193506	Vm58_294	0.0519807	Pli16_24_126	0.049372621	Pli21_22_129
6	0.03184365	Pli23_24_131	0.0484379	Qg58_22	0.049205542	Pli16_21_125
7	0.02570824	Pli22_23_130	0.0452465	Vm58_294	0.038085773	Pli16_19_124
8	0.02428656	Qli16_21_192	0.0447816	Pli16_19_124	0.035915417	Pg56_4
9	0.02372828	Qli22_23_197	0.042875	Pg56_4	0.034491718	Qg59_23
10	0.02367195	Pli16_24_126	0.0420206	Pli23_59_132	0.031111893	Pli22_23_130
11	0.02182543	Vm23_259	0.0419988	Pg59_7	0.030943832	Qli16_21_192
12	0.02067678	Qg59_23	0.0408258	Pli22_23_130	0.030746098	Vm56_292
13	0.02046546	Qli23_59_199	0.0383088	Vm56_292	0.027055853	Pg58_6
14	0.0202332	Vm22_258	0.0376017	Qg59_23	0.024673403	Qg58_22
15	0.02016412	Pg56_4	0.0371379	Qli16_21_192	0.024314618	Vm59_295
16	0.01944312	Pli16_19_124	0.036543	Qli22_23_197	0.021721702	Qli23_24_198
17	0.01848278	Pli23_59_132	0.0302066	Qli23_59_199	0.021107685	Vm19_255
18	0.01846764	Pg59_7	0.0278374	Qli23_24_198	0.020835996	Qg56_20
19	0.01697696	Vm21_257	0.0275218	Vm22_258	0.020230389	Vm23_259
20	0.01695484	Vm56_292	0.0274104	Vm23_259	0.017634459	Va59_363
21	0.01505993	Qli21_22_196	0.0244784	Qg56_20	0.016813201	Qli22_23_197
22	0.01426896	Qli23_24_198	0.0227978	Vm59_295	0.016633677	Vm58_294
23	0.01207123	Qg56_20	0.022585	Vm19_255	0.016256985	Qg57_21
24	0.01185141	Va58_362	0.0219973	Qli21_22_196	0.016146871	Qli23_59_199
25	0.01161428	Pgdf_1_373	0.0200968	Vm21_257	0.015901582	Vm21_257
26	0.01153082	Vm19_255	0.0165275	Qg57_21	0.015788867	Vm20_256
27	0.00991659	Vm16_252	0.0160586	Va58_362	0.014097386	Vm22_258
28	0.00990375	Vm15_251	0.0153709	Va59_363	0.012062771	Vm57_293
29	0.00934826	Vm59_295	0.014931	Vm20_256	0.011838114	Pg57_5
30	0.00846259	Qg65_29	0.011561	Vm16_252	0.011630512	Vm16_252
31	0.00786134	Va59_363	0.0114086	Pgdf_1_373	0.011134076	Vm15_251
32	0.00783583	Qg57_21	0.0111598	Vm57_293	0.01068027	Qli16_24_193
33	0.00780949	Vm24_260	0.0111507	Qli16_19_191	0.010449442	Vm24_260
34	0.00726594	Vm20_256	0.0111313	Va56_360	0.010282078	Va56_360
35	0.00725766	Va22_326	0.0110173	Pg57_5	0.010150099	Qli21_22_196
36	0.00700421	Qli16_19_191	0.010903	Vm15_251	0.010078393	Pgdf_1_373
37	0.00688457	Vm41_277	0.0104339	Va22_326	0.01002611	Qli16_19_191
38	0.00614568	Pli16_17_123	0.009714	Vm24_260	0.009953159	Va58_362
39	0.00594718	Vm10_246	0.0094599	Va23_327	0.008726429	Pli16_17_123
40	0.00590387	Va23_327	0.0089253	Pli16_17_123	0.008413643	Va23_327
41	0.00575188	Va56_360	0.00826	Va57_361	0.00825628	Va57_361
42	0.00517926	Pli15_16_122	0.0082294	Qli16_24_193	0.007650279	Va22_326
43	0.0050276	Plo8_37	0.0073482	Va20_324	0.007327493	Qg65_29
44	0.00500633	Vm17_253	0.0066203	Pli15_16_122	0.007185853	Va20_324
45	0.00487415	Vm12_248	0.0066167	Va19_323	0.00684069	Qli14_15_188
46	0.0047577	Vm4_240	0.0063922	Qli14_15_188	0.006396521	Va19_323
47	0.00464213	Plo4_35	0.0059977	Qg65_29	0.006378251	Pli15_16_122
48	0.0044329	Va21_325	0.0059292	Va21_325	0.005834305	Vm12_248
49	0.00429802	Qlo26_83	0.0055806	Vm10_246	0.005576746	Vm41_277
50	0.00423951	Vm8_244	0.0049931	Vm17_253	0.005387347	Vm17_253
51	0.00418289	Pg57_5	0.0045881	Vm12_248	0.005364393	Vm10_246
52	0.00415155	Vm7_243	0.0044376	Plo28_50	0.005217412	Vm18_254
53	0.00414504	Qli8_9_183	0.004306	Vm18_254	0.004953631	Pg60_8
54	0.00414073	Va57_361	0.0042929	Plo4_35	0.00491683	Vm4_240
55	0.00410783	Vm13_249	0.0042907	Vm4_240	0.004603238	Plo4_35
56	0.00410357	Plo29_51	0.0042692	Qlo20_78	0.00449649	Qlo1_68
57	0.0040548	Vm57_293	0.0042115	Plo8_37	0.004443831	Vm5_241

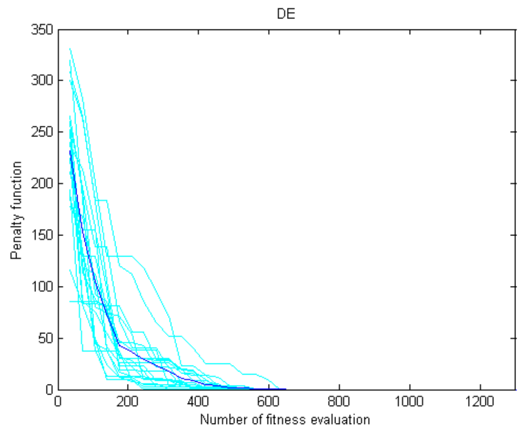
Table A.2 : Estimations of the feature quality for most critical oscillatory mode.

SSS		
Ranking	W	Feature name
1	0.0600778	Qli45_51_229
2	0.0599539	Qli35_45_223
3	0.059448	Qli50_51_231
4	0.0517651	Qli37_43_224
5	0.0510309	Qli50_52_230
6	0.0500866	Vm50_286
7	0.0456682	Vm51_287
8	0.0449973	Qli43_44_225
9	0.0416686	Vm45_281
10	0.0402957	Qli44_45_226
11	0.0379486	Qli52_42_233
12	0.0359215	Qli39_44_227
13	0.0342658	Pli52_42_166
14	0.0342008	Qli39_45_228
15	0.0338042	Qli34_36_209
16	0.0319136	Pli50_51_164
17	0.0301587	Pli50_52_163
18	0.0299656	Vm35_271
19	0.0296902	Pli45_51_162
20	0.028964	Vm39_275
21	0.0285903	Qli8_9_183
22	0.0283886	Qli33_34_210
23	0.0274829	Vm52_288
24	0.0274126	Pli48_40_155
25	0.0271413	Pli47_48_154
26	0.0271413	Pli47_48_153
27	0.0262613	Pli41_40_168
28	0.0259003	Pli1_47_152
29	0.0242401	Qg68_32
30	0.0239611	Vm44_280
31	0.0236768	Qli48_40_222
32	0.0233093	Vm43_279
33	0.0226079	Pli35_45_156
34	0.0217885	Qli32_33_211
35	0.0216842	Va41_345
36	0.0216744	Va66_370
37	0.0216343	Vm34_270
38	0.0204959	Qli41_40_235
39	0.020062	Qli1_47_219
40	0.0193876	Va51_355
41	0.0191021	Va42_346
42	0.019057	Va67_371
43	0.0182957	Qli47_48_220
44	0.0182957	Qli47_48_221
45	0.0182167	Pli46_49_151
46	0.0182012	Pli49_52_165
47	0.0179116	Vm40_276
48	0.0178933	Qli7_8_182
49	0.0172161	Va50_354
50	0.017091	Pli38_46_150
51	0.0161109	Qli5_8_179
52	0.0160485	Pli44_45_159
53	0.0158999	Va65_369
54	0.015217	Vm48_284
55	0.0150002	Qg66_30
56	0.0147074	Vm33_269
57	0.0144493	Va40_344

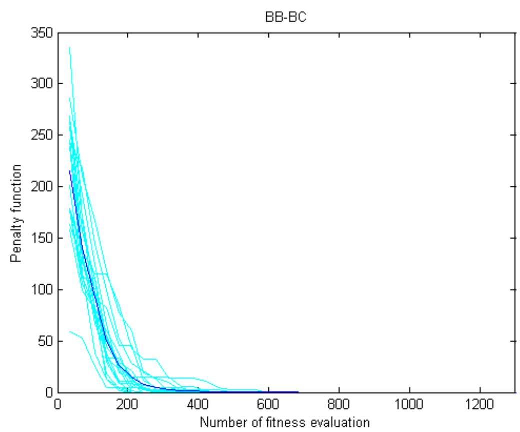
APPENDIX B: Detailed results of optimization of preventive control action



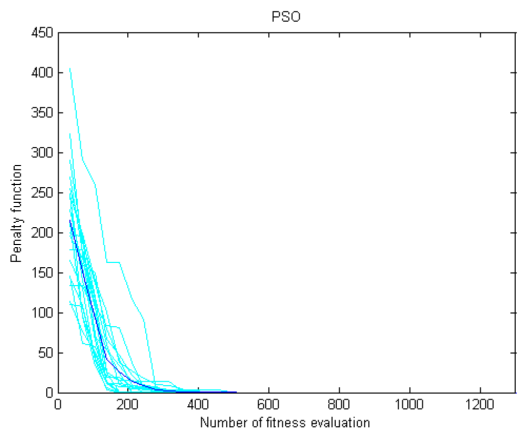
(a)



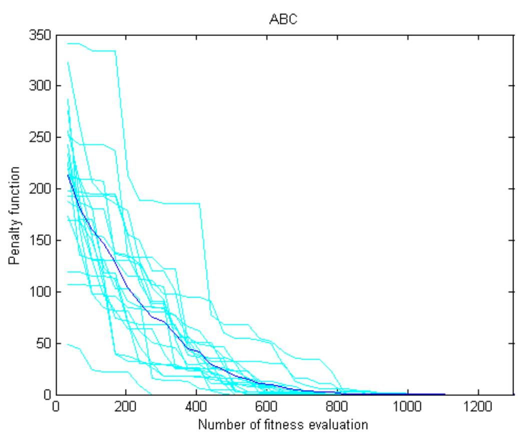
(b)



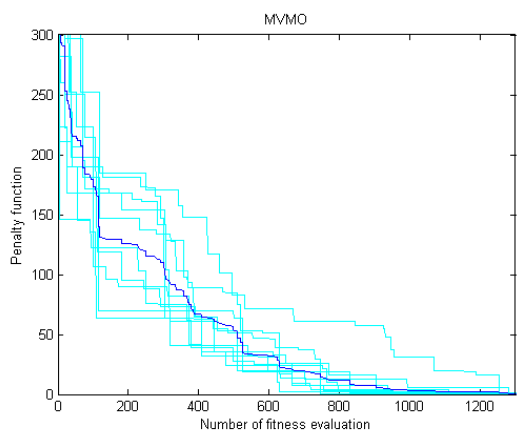
(c)



(d)



(e)



(f)

Figure B.1 : Evolution of penalty function of best solutions during optimizations: (a)GA. (b)DE. (c)BB-BC. (d)PSO. (e)ABC. (f)MVMO.

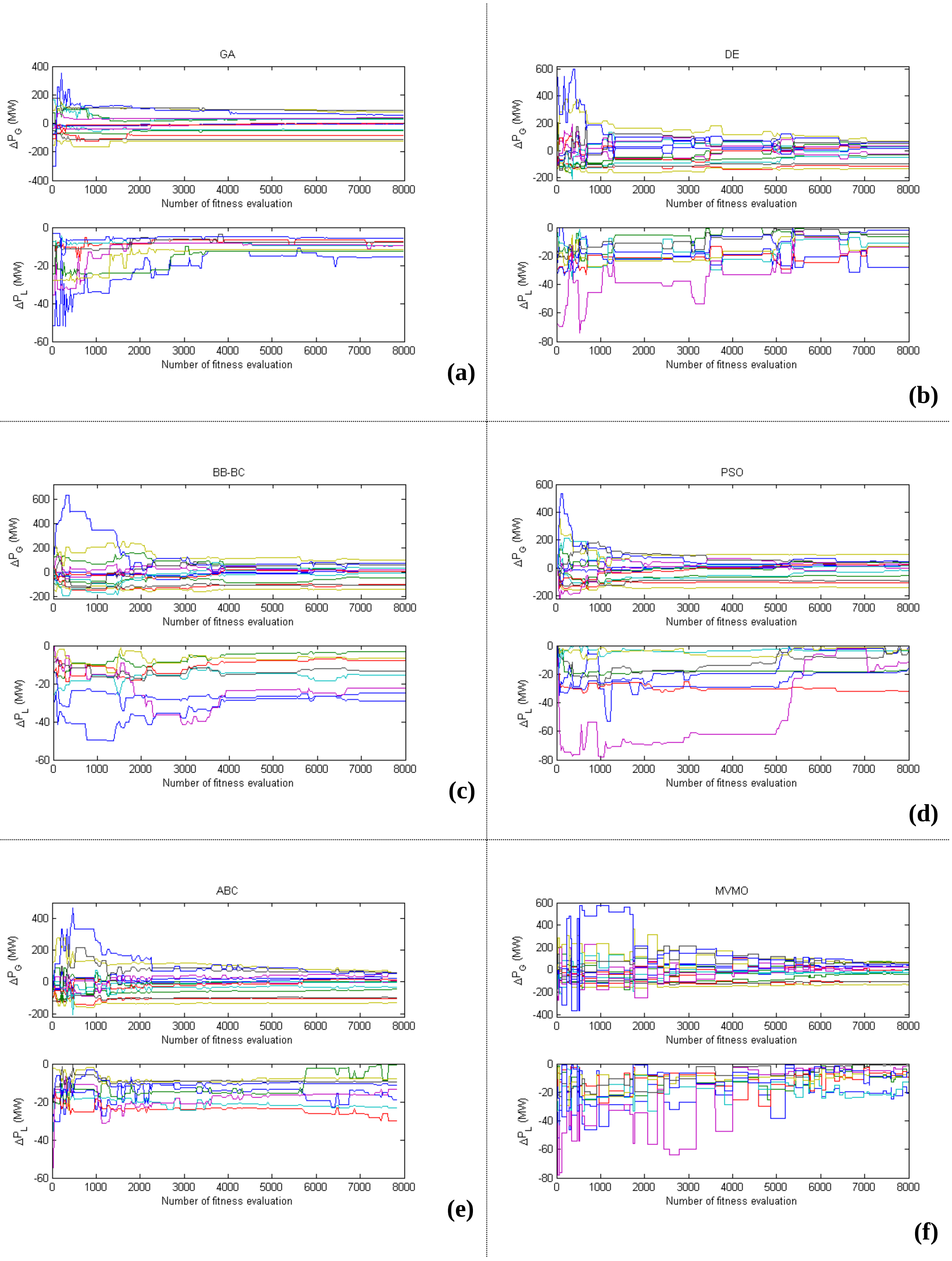


Figure B.2 : Changes on the parameters of best solutions during optimizations (a)GA. (b)DE. (c)BB-BC. (d)PSO. (e)ABC. (f)MVMO.

CURRICULUM VITAE

Name Surname: Cavit Fatih Küçüktezcan

Place and Date of Birth: Giessen, Germany, 17.06.1983

Address: ITU, Faculty of Electrical & Electronics, 34469, Istanbul

E-Mail: kucuktezca@itu.edu.tr

B.Sc.: ITU, Electrical Engineering, 2005

M.Sc.: ITU, Electrical Engineering, 2008

Professional Experience and Rewards: ITU, Department of Electrical Engineering, Research Asst., 2005

List of Publications on the Thesis:

International Journal Papers (SCI)

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2015). Preventive and Corrective Control Applications in Power Systems via Big Bang-Big Crunch Optimization, *International Journal of Electrical Power & Energy Systems, 67*, 114-124.

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2012). A New Dynamic Security Enhancement Method via Genetic Algorithms Integrated with Neural Network Based Tools, *Electric Power Systems Research, 83* (1), 1-8.

International Conference Papers

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2013). A Comparison Between ANN Based Methods of Critical Clearing Time Estimation, *8th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, Turkey.

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2012). Big Bang-Big Crunch Based Optimal Preventive Control Action on Power Systems, *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT) Europe*, Berlin, Germany.

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2011). Optimal Load Shedding Scheme in Power Systems Based on Big Bang Big Crunch Method, *International Conference on Power and Energy Systems and Applications*, Pittsburgh, USA.

- **Kucuktezcan, C. F. and Genc, V. M. I.** (2010). Dynamic Security Assessment of a Power System Based on Probabilistic Neural Networks, *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT) Europe*, Gothenburg, Sweden.