MultiCraft

International Journal of Engineering, Science and Technology
Vol. 4, No. 2, 2012, pp. 77-88

INTERNATIONAL JOURNAL OF ENGINEERING, SCIENCE AND TECHNOLOGY

www.ijest-ng.com
www.ajol.info/index.php/ijest

Gene expression programming for power system static security assessment

S. F. Mekhamer[1], A. Y. Abdelaziz[1*], H. M. Khattab[2], M. A. L. Badr[1]

[1]Electrical Power and Machines Department, Ain Shams University, Cairo, EGYPT*
[2] ENPPI (Engineering for the Petroleum and Process Industries), Cairo, EGYPT
[*]Corresponding Author: e-mail: almoatazabdelaziz@hotmail.com, Tel. +20-100-1372930

Abstract

In this paper, a novel gene expression programming (GEP) algorithm is presented for power system static security assessment. The GEP algorithms as evolutionary algorithms for pattern classification have recently received attention for classification problems because they can perform global searches and achieve high classification accuracy. The proposed methodology introduces the GEP based classifier for the first time in static security assessment problems. The proposed algorithm is examined using different IEEE standard test systems available in the literature. Different contingency case studies have been used to test the proposed methodology performance. The GEP based algorithm formulates the problem as a multi-class classification problem using the one-against-all binarization method. The algorithm classifies the static security of the power system into three classes, namely normal, alert and emergency. Performance of the algorithm is compared with other probabilistic and deterministic algorithms including different neural network based classifiers. Simulation results show the superiority of the proposed technique in static security assessment.

Keywords: static security, gene expression programming, probabilistic neural network, radial basis function neural network, power system classifier.

DOI: http://dx.doi.org/10.4314/ijest.v4i2.6

1. Introduction

Nowadays power systems are considered the most complex control system in existence, since they are extremely interconnected, highly complex and can spread over vast continents. Power systems design and operation must be in such a way as to ensure that all operating variables are controlled and fall within acceptable ranges at all operating conditions. Power system security main goal and essence is to ensure proper system operation within acceptable limits. Conversely, failure of power system to operate securely can lead to outages which may have wide ranging consequences including power interruption to customers, damage of equipment, huge financial losses, or even loss of life. Technical and economic outcomes can be maintained by ensuring power system security (Stott et al., 1987; Huang et al., 2002).

With the recent advent of the deregulated electricity market, modern utilities have been forced to operate power systems closer to their security boundaries. This trend has encouraged the need for fast and accurate assessment of power system security, focusing on the ability of the power system to maintain the electrical energy delivery from the generators to the end customers, especially under unexpected contingencies that could interrupt the normal system operation (Santo et al., 2004).

Operation of the power system is governed by the load flow equations, which is determined by load consumption, generation and network configuration or topology. Constraints are imposed on different power system equipment, for instance each generator has limited active and reactive power capacity, each line or transformer has limits on the flow through it. Constraints are also imposed on power system, where bus voltage magnitude levels have to be within acceptable limits, bus voltages angles have limits across the buses for stability, where these constraints are expressed in terms of a set of equality and inequality constraints. The power system is considered to be in the normal operating state when all the above constraints are satisfied and fulfilled, whereas in the normal operating state, all the loads are supplied within acceptable voltage and frequency levels, and all system components

are operated within acceptable limits. In practice, it is very difficult to keep a system in the normal operating state as the system may be subjected to sudden changes or outages and may become insecure (Pang et al., 1974).

The EPRI report states the following definitions: *Normal State*: is defined as: "all equipment and operating constraints are within limits, including the generation is adequate to supply the load, with no equipment overloaded. There is sufficient margin such that the loss of any element will not result in a limit being violated".

Alert State: is defined as: "if a system enters a condition where the loss of some elements covered by the operating criteria will result in a current or voltage violation, then the system is in the alert state. The alert state is similar to the normal state in that all constraints are satisfied, but there is no longer sufficient margin to withstand an outage. The system can enter the alert state by the outage of equipment, by a change in generation schedule, or a growth in the system load".

Emergency State: is defined as: "a power system is in an emergency state condition when operating limits are violated. If a contingency occurs or the generation and load changes before corrective action can be (or is) taken, the system will enter the emergency state. No load is curtailed in the emergency state, but equipment or operating conditions have been violated. If control measures are not taken in time to restore the system to the alert state, the system will transfer from the emergency state to the extreme emergency state".

Extreme Emergency (restorative) State: is defined as: "in the extreme emergency state, the equipment and operating constraints are violated and the load is not supplied".

Power system security encounters the above problems by implementing certain functions to help maintaining the power system in the normal state. Three main functions are carried out for power system security achievement broadly classified as measurements, security analysis (SA) and preventive or corrective actions (Morison et al., 2004). Effective operation of the power system requires that critical quantities are measured and their values are transferred to central control locations therefore power systems measurements can monitor voltages, currents, power flows and the status of circuit breakers and switches in every power system portion. Since much information are tele-metered simultaneously, it is difficult for a human operator to check all information simultaneously. Hence digital computers are usually installed in operations control centers to gather data, process them and place them in database where operators can display information.

Static security assessment, starts from the grid topology, structure and energy market transactions, performs a load flow solution to verify that electrical constraints and thermal constraints are respected. If these conditions are not respected the system is not secure, therefore static security is guaranteed only if the electrical and thermal constraints are verified for all cases.

In order to assess system static security conventional analytical methods have been applied, which demand large computation time compared with system real time operation in order to solve the power system equations, simulate each contingency, and determine the bus voltages and line flows. These large computation times challenge even today's fast computers, and in order to overcome these computational requirements, application of artificial intelligence based algorithms like decision trees, pattern recognition, fuzzy logic, artificial neural networks and expert systems have been explored for static security assessment problems (Bansal et al., 2006; Swarp et al., 2002).

Power system security assessment using Kohonen neural network has been illustrated by Niebor et al. (1994), El-Sharkawi et al. (1993) and Lo et al. (1995), and using Back propagation neural network has been applied by Saeh et al. (2008) and Wang et al. (2007). Shukla et al. (2004) presents an artificial neural network based methodology to assess the steady state security of a power system, where the security of the system is assessed on the basis of the voltage profile at each bus with reference to changes in generation and load in the system. The ANN used is a feed-forward multilayer network trained with a back-propagation algorithm, where the output of the ANN classifies the security of the power system into normal, alert and emergency states. An IEEE 14-bus test system is considered to demonstrate the results of the methodology. Abdelaziz (2005) presented an approach for line contingency evaluation based on radial basis function neural network (RBFNN). Two different methods were adopted for static security assessment using the proposed RBFNN. The first method determines the security condition directly when one line of the system is overloaded, and was applied to a standard 5-bus, 7-line test system. The second method was applied to the IEEE 14-bus system, in which the RBFNN is able to yield system states consequent upon a contingency by predicting the bus voltage magnitudes and angles. The results were compared with conventional back-propagation neural network (BPNN) with better results in terms of speed and accuracy.

Khattab et al. (2011) and Abdelaziz et al. (2012) presented a probabilistic neural network (PNN) based classifier to judge the static security of the power system, in which the proposed probabilistic approach classifier classifies the security of the power system based on the voltage profile of each bus in reference to changes in the generation and load profile. The probabilistic neural network is compared with the radial basis function neural network (RBFNN) and the back-propagation neural network (BPNN). The PNN shows superior results in comparison to other techniques in terms of classification accuracy, where the proposed methodology has been examined using three IEEE standard test systems, where the input to the neural network is the voltage profile at each bus, the output of the PNN classifies the security of the power system into three classes, normal, alert and emergency.

Gene expression programming (GEP) is a new evolutionary algorithm for data classification and uses fixed length, linear strings of chromosomes to represent different solutions in the form of expression trees of different shapes and sizes, and implements genetic variation to find the best solution. GEP combines the advantages of both genetic algorithm (GA) and genetic programming (GP), while overcoming some of their individual limitations.

GEP has been used for solving classification problems of power systems since its evolution, where (Yin et al., 2008) applied Gene Expression Programming (GEP) to short-term load forecasting.

In this paper, a novel gene expression programming based classification algorithm is used for static security of power system; results are compared to different deterministic and probabilistic classifiers, namely; probabilistic neural network based classifier, radial basis function neural network and the back-propagation neural networks. The output of each algorithm classifies the security of the power system under study into three classes, normal, alert and emergency. The designed models have been applied to 9-bus, 14-bus, 30-bus and 57- bus IEEE standard test systems and the classification results are compared to show superiority of the proposed approach.

2. Gene Expression Programming

2.1 Gene Expression Programming: An Evolutionary Algorithm:

Gene Expression Programming belongs to the so called Evolutionary Algorithms (EA's). Like all evolutionary algorithms, natural or artificial, GEP uses populations of individuals (populations of models or solutions), selects and reproduces them according to fitness, and introduces genetic variation using one or more genetic operators such as mutation or recombination. GEP works with populations of models and selects them according to their respective fitnesses. By repeating this process for a certain number of generations, one is bound to get evolution, which in this case means better and better solutions to the problem under investigation to find the best solutions. In fact, there are several artificial evolutionary algorithms such as the Genetic Algorithms (GAs) and Genetic Programming (GP), for they serve to illustrate some of the fundamental characteristics of the GEP technique and why GEP surpasses the old GP technique. The main difference is in the nature of individuals each algorithm deals with. In GA the individuals are linear strings of fixed length (chromosomes). In genetic programming (GP) the individuals are non-linear entities of different sizes and shapes. In GEP the individuals are encoded as linear strings of fixed length (genomes or chromosomes) afterwards expressed expression trees (ETs). The introduction of expression trees introduces wide variety of solutions to the problem under study. The GEP system is a full-fledged genotype/phenotype system with expression trees of different sizes and shapes encoded in linear chromosomes of fixed length. GEP chromosomes are multigenic, encoding multiple expression trees or solutions that can be organized into a much more complex program. So, like the DNA/protein system of life on earth, the genes/trees system of GEP can not only explore all the crannies and paths of the solution space but it's also free to explore higher levels of organization.

2.2 The Architecture of GEP Programs:

There are two main players in GEP: the chromosomes and the expression trees (ETs), being the latter the expression of the genetic information encoded in the former. As in nature, the process of information decoding is called translation. This translation implies obviously a kind of code and a set of rules. The genetic code of GEP is very simple: a one-to-one relationship between the symbols of the genes and the nodes they represent in the trees. The rules are also very simple: they determine the spatial organization of nodes in the expression trees and the type of interaction between sub-ETs. Therefore, there are two languages in GEP: the language of genes and the language of expression trees, it is possible to infer immediately the expression tree given the sequence of a gene, and vice versa. This unequivocal bilingual notation is called Karva language.

The structural organization of GEP genes is better understood in terms of open reading frames (ORFs). In biology, an ORF or coding sequence of a gene begins with the start codon, continues with the amino acid codons, and ends at a termination codon. However, a gene is more than the respective ORF, with sequences upstream of the start codon and sequences downstream of the stop codon. And although in GEP the start site is always the first position of a gene, the termination point does not always coincide with the last position of a gene. Consequently, it is common for GEP genes to have noncoding regions downstream of the termination point. These noncoding regions obviously do not interfere with expression but, nonetheless, they play a crucial role in evolution, for they alone allow the creation of valid solutions no matter how profoundly their chromosomes are modified. Consider, for example, the algebraic expression:

$$\sqrt{(a-b)(c+d)} \tag{1}$$

It can also be represented as a diagram or an expression tree (Figure 1):

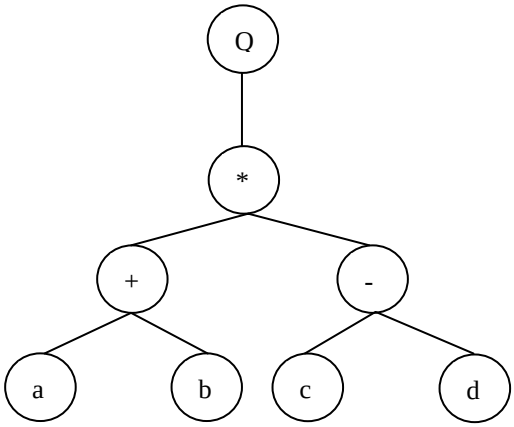

Figure 1. Tree presentation for equation (1).

where "Q" represents the square root function.

This kind of diagram representation is what is called the phenotype in gene expression programming. And the genotype can be easily inferred from the phenotype as follows:

$$\begin{matrix} 01234567 \\ Q*-+abcd \end{matrix} \quad (2)$$

which is the straightforward reading of the expression tree from left to right and from top to bottom. The expression (2) is an ORF, starting at "Q" (position 0) and terminating at "d" (position 7). These ORFs were named K-expressions from Karva notation.

Looking at the structure of GEP K-expressions, it is difficult or even impossible to see the advantages of such a representation, except perhaps for its simplicity and elegance. However, when K-expressions are analyzed in the context of a gene, the advantages of this representation become obvious. Thus, in GEP, what varies is not the length of genes which is constant, but the length of the K-expressions. Indeed, the length of a K-expression may be equal to or less than the length of the gene.

The genes are composed of a head and a tail. The head contains symbols that represent both functions and terminals, whereas the tail contains only terminals. For each problem, the length of the head h is chosen, whereas the length of the tail t is a function of h and the number of arguments n of the function with more arguments (also called maximum arity) and is evaluated by the equation:

$$t = h(n-1)+1 \quad (3)$$

In GEP, chromosomes are usually composed of more than one gene of equal length. For each problem or run, the number of genes, as well as the length of the head, is chosen. Each gene codes for a sub-ET and the sub-ETs interact with one another forming a more complex multi-subunit ET. Figure 2 presents a flow chart of gene expression programming algorithm.

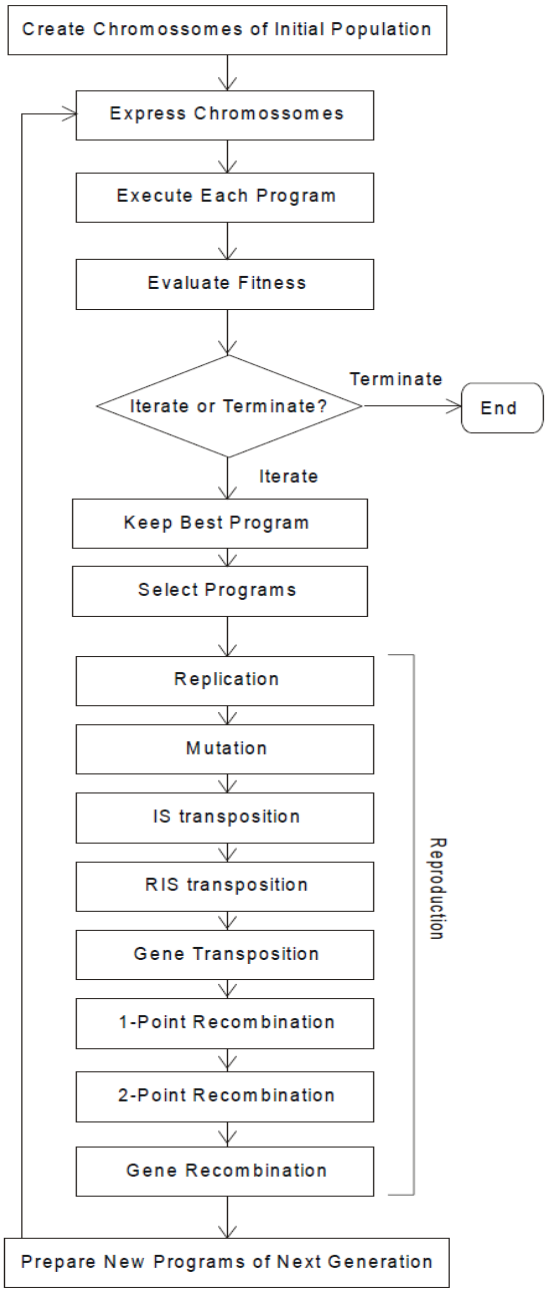

Figure 2. Flowchart of gene expression programming.

3. Implementation of Classification Algorithms

The GEP algorithm has been applied to the IEEE 9-bus, 14-bus, 30-bus and 57-bus test systems. Results have been compared to the different neural network models presented by the same authors (Abdelaziz et al., 2012) Figure 3 shows a flowchart for the application of the different algorithms to the test power systems.

In this flowchart, offline simulations based on Newton-Raphson load flow are performed to work out the different operating scenarios and contingencies the system may encounter. Next, static security status is evaluated for each contingency. Data is then split randomly into training data that will be utilized to train the classification algorithm, and test data that will be used to examine and measure the performance of the different classifiers.

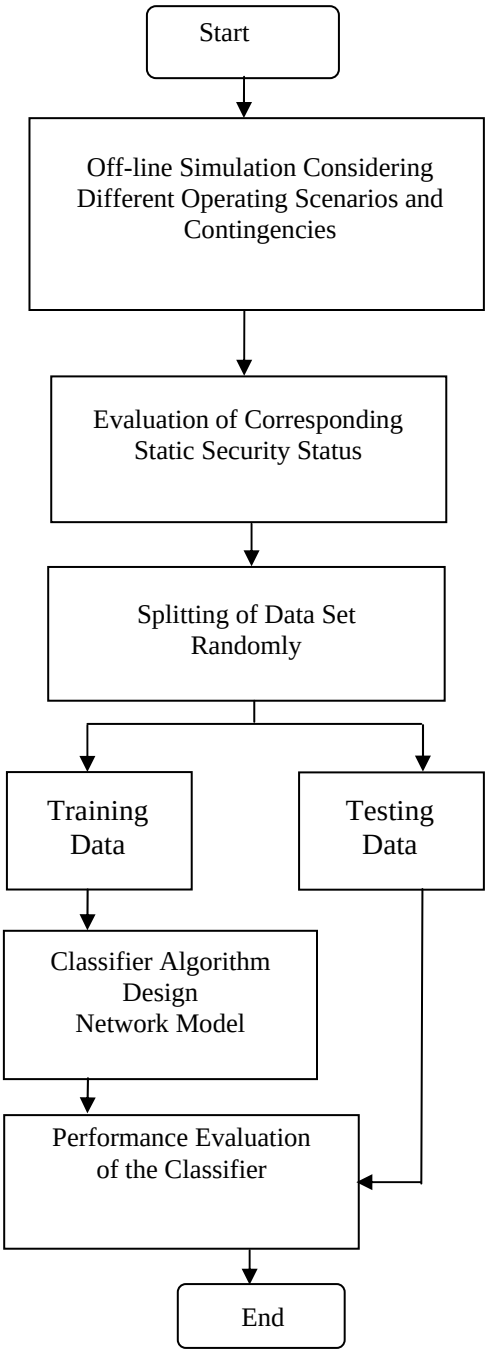

Figure 3. Flowchart for application of different classifiers models.

3.1 Classification Algorithm Architecture:

3.1.1 Classification Algorithm Input:

For load variation contingencies, the input consists of the normalized values of the voltage magnitude of the system buses. For single and double line outages contingencies, line status in service (binary "1") or line outage/out of service (binary "0") is the input to the algorithm.

3.1.2 Classification Algorithm Output:

The output of the algorithm determines the security state of the system; 1 (Normal state), 2 (Alert state) and 3 (Emergency state). The GEP is a two-class classification algorithm, and since the problem in hand involves decision of system security class among

three different classes, the problem is formulated as multiple two-class problems by using the one-against-all learning method by (Zho et al., 2003). The algorithm firstly determines if the system is normal state or not-normal state, then the algorithm determines if the system is alert state or emergency state.

3.2 Data Generation:

3.2.1 First Test Case (Load Variation Contingencies):

The real time security assessment requires continuous monitoring of the input signals. With appropriate data transformation, normalized values of voltage level of the buses in the system are fed to the classification algorithm. The application of classification algorithm for classifying the patterns requires considerable amount of data for training and testing of the network. The training and testing data for the present work are generated by varying the active and reactive load at the buses from 0.8 pu to 3.6 pu for the IEEE 14-bus system and to 2.5 pu for IEEE 30-bus and IEEE 57-bus systems. The active power generated at the generator bus is incremented with reference to changes in the active load.

Three different data patterns are generated for training the algorithm by running the load flow as follows:

- Increments of only active load at all the buses.
- Increments of only reactive load at all the buses.
- Simultaneous increments of active and reactive load at all the buses.

The output directly indicates the desired state assessment. The desired output is '1' when voltage level at the bus is between 0.9 pu and 1.1pu (Normal state), '2' when the voltage level at the bus is between 0.8 pu and 0.9 pu (Alert state) and '3' when the voltage level at the bus is between 0.7 pu and 0.8 pu (Emergency state).

3.2.2 Second Test Case (Single and Double Line Contingencies):

The status of the lines in each power system line topology is fed to the classification algorithm as an input pattern. A line outage/out of service is input as "0" while a line in service is input as "1", this binary coding for the line status simplifies the input and accordingly enhances the classifier performance. Single and double line outage contingencies have been studied in the training and testing in the present work for all test systems.

The output directly indicates the desired state assessment. The desired output is '1' when voltage level at the bus is within 0.95 pu and 1.05 pu (Normal state), the desired output is '2' when the voltage level at the bus is within 0.9 pu and 1.1 pu (Alert state) while the desired output is '3' when the voltage level at the bus is less than 0.9 pu or greater than 1.1 pu (Emergency state).

3.3 Performance Evaluation of the Classifier

The performance of the different classifiers are judged by evaluating measures similar to those by (Kalyani et al, 2009) after implementing required modifications to account for the problem under study.

3.3.1 Mean Squared Error (MSE)

$$MSE = \frac{1}{n}\sum_{k=1}^{n}(E_k)^2; E_k = | DO_k - AO_k | \tag{4}$$

where n is equal to the number of samples in the data set, DO_k is the desired output obtained from off-line simulations and AO_k is the actual output obtained from the trained classifier.

3.3.2 Classification Accuracy (CA)

$$CA = \frac{\text{No. of samples classified correctly}}{\text{Total number of samples in data set}} \tag{5}$$

3.3.3 Misclassification Rate (MC):

(i) Normal Misclassification (NMC):

$$NMC = \frac{\text{No. of normal samples classified as alert or emergency}}{\text{Total number of normal states}} \tag{6}$$

(ii) Alert Misclassification (AMC):

$$AMC = \frac{\text{No. of alert samples classified as normal or emergency}}{\text{Total number of alert states}} \quad (7)$$

(iii) Emergency Misclassification (EMC):

$$EMC = \frac{\text{No. of emergency samples classified as normal or alert}}{\text{Total number of emergency states}} \quad (8)$$

4. Simulation Results

4.1 First Test Case (Load Variation Contingencies):

The above mentioned data patterns results in different loading patterns, the classifiers were trained using a group of loading patterns and were then tested using group of loading patterns it has never seen. MATLAB version 7.6 neural network toolbox was used for the implementation and training of the neural networks. The BPNN gave best results with 20 hidden nodes and was trained using the standard gradient descent algorithm. Learning rate of BPNN was assumed to be 0.12 and momentum constant was taken as 0.93. A spread constant of 1.21 was chosen for the RBFNN. A smoothing parameter of 0.65 was chosen for the PNN. The different parameters represent the optimum parameters for the problem under study in terms of the above mentioned performance measures using experience with such networks and engineering judgment to provide the best accuracy measures achievements. GEP different parameters as follows (number of chromosomes 30, head size 7, mutation rate 0.046, inversion 0.12, one-point recombination 0.34, two-point recombination 0.30). Table 1 shows the data generation for the static security assessment for the three test systems.

Table 1. Data generation results

Test Case	IEEE 14 Bus	IEEE 30 Bus	IEEE 57 Bus
Operating Scenarios	627	901	1101
Normal State Cases	440	736	832
Alert State Cases	154	93	164
Emergency State Cases	33	72	105

Operating scenarios and training patterns have been chosen to cover a wide range of operating conditions for the test systems in order to adequately present all possible configurations for training the different classifiers. Normal, alert and emergency conditions have been concluded from load flow simulations of the different test systems. Load flow simulation results were fed to the different classifiers models after splitting the data randomly into training set and test set. Tables 2-4 shows the classification results of static security assessment on the training set and test set for the different classifiers algorithms. The above mentioned accuracy measures have been calculated and presented in this table for means of comparison between the classifier architectures.

Table 2. Classification results of static security assessment for the IEEE 14-bus test system

	TRAIN SET				TEST SET			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	3.63	1.26	0.00	0.00	3.09	1.46	0.44	0.39
CA%	67.72	96.87	100.0	100.0	68.84	92.15	97.23	98.15
NMC%	31.23	26.56	00.00	00.00	60.32	37.21	07.32	7.12
AMC%	10.65	09.65	00.00	00.00	40.39	35.28	03.23	2.98
EMC%	07.03	05.96	00.00	00.00	15.21	10.84	05.26	04.86

Table 3. Classification results of static security assessment for the IEEE 30-bus test system

	TRAIN SET				TEST SET			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	0.33	1.57	0.00	0.00	1.23	1.61	0.82	0.51
CA%	80.27	95.26	100.0	100.0	78.87	89.27	93.68	95.63
NMC%	26.87	22.18	00.00	00.00	48.39	37.24	5.87	4.93
AMC%	17.36	10.94	00.00	00.00	19.32	12.34	5.24	4.90
EMC%	12.15	11.65	00.00	00.00	17.37	11.94	08.03	7.54

Table 4. Classification results of static security assessment for the IEEE 57-bus test system

	TRAIN SET				TEST SET			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	1.69	1.82	0.00	0.00	2.37	1.93	0.96	0.82
CA%	78.69	91.68	100.0	100.0	72.65	87.23	90.23	92.87
NMC%	40.36	39.24	00.00	00.00	67.03	50.21	11.25	10.62
AMC%	31.26	26.57	00.00	00.00	50.21	41.26	6.08	5.69
EMC%	20.45	18.39	00.00	00.00	23.54	19.64	5.70	4.81

It is shown from the above accuracy measures comparison tables that the GEP is very superior in classification rather than other classifier models in terms of higher classification accuracy and less error and less misclassifications. The GEP and PNN classifier algorithms yield zero error or 100% accuracy for classifying the data patterns it has been previously trained to, whereas other neural network models fail to achieve this property. Moreover, the tables show that the GEP provides the best results during testing patterns it had never seen in terms of least error, best accuracy classification and least misclassification in comparison to other classifier models.

The classification accuracy of the GEP algorithm is guaranteed and superior in comparison to other classifiers which decline considerably with increasing number of the test patterns fed to the classifier as clearly shown by testing larger size test systems. The misclassification rates are minimized using the GEP and PNN classifiers considering the test patterns achieving a considerable decrease in misclassification rates in comparison to other classifiers. The BPNN achieves the worst results in comparison to GEP, PNN and RBFNN classifiers. The proposed methodology training time is in the order of few minutes with testing is instantaneous allowing use of such techniques in real time security assessment.

4.2 Second Test Case (Single and Double Line Contingencies):

The classifier models were trained using a group of single and double line outage contingencies then tested using group of single and double line outages it has never seen. Optimum parameter selections have been performed for the case study for optimizing the performance of the different classifier models. The BPNN gave best results with 14 hidden nodes and was trained using the standard gradient descent algorithm. Learning rate of BPNN was assumed to be 0.15 and momentum constant was taken as 0.96. A spread constant of 1.1 was chosen for the RBFNN. A smoothing parameter of 0.63 was chosen for the PNN that provided the best simulation results in terms of accuracy measures. GEP different parameters as follows (number of chromosomes 40, head size 9, mutation rate 0.042, inversion 0.10, one-point recombination 0.31, two-point recombination 0.27). Table 5 shows the data generation for the static security assessment for the three test systems.

Table 5. Data generation results

Test Case	IEEE 9 Bus	IEEE 14 Bus	IEEE 30 Bus	IEEE 57 Bus
Number of Buses	9	14	30	57
Number of Branches	9	20	40	80
Operating Scenarios	46	211	821	3241
Normal State Cases	16	93	256	1054
Alert State Cases	18	47	67	706
Emergency State Case	12	71	498	1481

Normal, alert and emergency conditions have been concluded from off-line load flow simulations based on Newton-Raphson method for the different test systems. Load flow simulation results were fed to the different classifier models after splitting the data randomly into training set and test set. Tables 6-9 compare the classification results of static security assessment on the training set and test set for the different classifiers for the different test systems. Comparison has been performed in terms of the different formulated performance measures including classification error, classification accuracy and misclassification rates.

Table 6. Classification results of static security assessment for the IEEE 9-bus test system

	TRAIN SET				TEST SET			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	1.12	1.08	0.00	0.00	2.78	2.07	1.61	1.30
CA%	80.31	93.14	100.0	100.0	78.44	85.26	90.21	91.23
NMC%	40.71	31.36	00.00	00.00	36.54	35.22	10.46	10.28
AMC%	05.59	05.38	00.00	00.00	20.65	10.71	08.55	07.85
EMC%	04.36	03.93	00.00	00.00	12.21	10.47	06.57	05.96

Table 7. Classification results of static security assessment for the IEEE 14-bus test system

	TRAIN SET				**TEST SET**			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	5.31	1.01	0.00	0.00	6.65	1.18	1.95	1.87
CA%	79.24	93.62	100.0	100.0	74.84	86.53	92.54	92.84
NMC%	39.58	28.64	00.00	00.00	42.36	30.24	10.57	10.28
AMC%	19.31	05.36	00.00	00.00	23.35	08.64	07.49	07.38
EMC%	12.45	04.65	00.00	00.00	16.61	05.86	05.35	04.77

Table 8. Classification results of static security assessment for the IEEE 30-bus test system

	TRAIN SET				**TEST SET**			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	6.45	2.36	0.00	0.00	7.01	4.12	1.69	1.64
CA%	80.54	85.69	100.00	100.00	79.64	84.19	91.07	92.36
NMC%	40.84	30.55	00.00	00.00	36.95	35.64	09.32	08.54
AMC%	25.46	10.84	00.00	00.00	29.54	16.18	08.11	07.14
EMC%	15.67	06.54	00.00	00.00	18.36	08.56	06.47	05.46

Table 9. Classification results of static security assessment for the IEEE 57-bus test system

	TRAIN SET				**TEST SET**			
Samples	BPNN	RBFNN	PNN	GEP	BPNN	RBFNN	PNN	GEP
MSE%	2.34	1.94	0.00	0.00	3.98	2.17	1.45	1.26
CA%	88.32	90.05	100.0	100.0	84.26	89.12	92.64	93.47
NMC%	20.54	18.41	00.00	00.00	33.47	23.24	20.54	18.31
AMC%	14.21	13.36	00.00	00.00	20.62	14.88	09.04	08.78
EMC%	10.68	08.65	00.00	00.00	15.48	10.21	06.87	05.37

Performance of the different classifiers is similar to the first test case study, it is also clearly shown for single and line outage contingencies that the GEP algorithm is very advantageous and superior in classification rather than other classifier models in terms of achieving the best classification accuracy as well as the least error and misclassification rates. The GEP and PNN algorithms have the intrinsic property of achieving zero error or 100% accuracy for classifying the training data patterns it has been previously trained to, while other neural network models still fail to achieve this advantage. The GEP algorithm provides the best results in terms of least error, best accuracy classification and least misclassification in comparison to other classifier models. Superior performance is guaranteed with increasing the test better where as performance declines considerably with increasing the test patterns with other architectures.

5. Conclusion

This paper presented a novel classifier algorithm based on gene expression programming (GEP). The GEP algorithm is used for the first time in literature to judge the static security of power system. The GEP classification algorithm is formulated as a multi-class classification problem based on using the one-against-all binarization method. The algorithm classifies the static security of the power system into three classes, normal, alert and emergency. Performance of the proposed algorithm shows that it is suitable for online applications, allowing its applicability for online static security assessment.

The classifier is used to judge the static security of the power system for single and double line outages as well as load variation contingencies. The GEP classifier algorithm is compared to the probabilistic neural network (PNN), radial basis function neural network (RBFNN) and the back-propagation neural network (BPNN). The GEP classifier algorithm shows superior results in comparison to other techniques regarding maximum classification accuracy and minimum classification error and misclassification rates. The GEP and PNN algorithms solely have the intrinsic property of achieving zero error and zero misclassification rates on training patterns, which compels classification accuracy of 100%. It is clearly evident that the GEP classifier algorithm is leading in static security assessment of power system. It is also apparent that the GEP classifier algorithm is very promising for application in future power system security assessment researches.

Nomenclature

GEP Gene Expression Programming
EA Evolutionary Algorithm
GP Genetic Programming

GA Genetic Algorithm
ET Expression Tree
ANN Artificial Neural Network
BPNN Back Propagation Neural Network
RBFNN Radial Basis Function Neural Network
PNN Probabilistic Neural Network
ORF Open Reading Frame

References

Abdelaziz A. Y., Mekhamer S. F., Badr M. A. L. and Khattab H. M., 2012. Probabilistic Neural Network Classifier for Static Voltage Security Assessment of Power Systems, *Electric Power Components and Systems Journal*, Vol. 40, No. 2, pp. 147-160.

Abdelaziz A. Y., 2005. Static Security Assessment using Radial Basis Function Neural Networks, *Proceedings of the 10th MEPCON Conference*, Port-Said, Egypt, pp. 535-540.

Bansal R. C., 2006. Overview and Literature Survey of Artificial Neural Networks Applications to Power Systems (1992-2004), *IE (I) Journal-EL*, Vol. 86, pp. 282-296.

Bizjak G., Kerin U., Kerbs S. R., Lerch E. and Ruhle O., 2008. Vision 2020 Dynamic Security Assessment in Real time Environment, *Proceedings of the IEEE Conference on Conversion and Delivery of Electrical Energy*, pp. 1-7.

Ejebe G. C., Van H. P., Meeteren and Wollenberg B. F., 1988. Fast Contingency Screening and Evaluation for Voltage Security Analysis, *IEEE Trans. Power Syst.*, Vol. 3, No. 4, pp. 1582–1590.

EPRI REPORT. Composite-System Reliability Evaluation: Phase-1 Scooping Study. *Technical Report EPRI EL-5290*, 1987.

El-Sharkawi M. A. and Atteri R., 1993. Static Security Assessment of Power System Using Kohonen Neural Network, *Proceedings of the 2nd International Forum on Applications of Neural Networks to Power System (ANNPS)*, pp. 373-377.

El-Sharkawy M. and et al., 1989. Dynamic Security Assessment of Power Systems Using Back Error Propagation Artificial Neural Network, *Second Symposium on Expert Systems Application to Power Systems*, Seattle, WA.

Ferreira C., 2001. Gene Expression Programming: A New Adaptive Algorithm for Solving Problems, *Complex Systems*, Vol. 13, No. 2, pp. 87–129.

Huang J. A., Valette A., Beaudoin M., Morison K., Moshref A., Provencher M. and Sun J., 2002. An Intelligent System for Advanced Dynamic Security Assessment. *Proceedings of the IEEE PowerCon 2002, International Conference on Power System Technology*, Vol. 1,pp. 220-224.

Kalyani S. and Swarup K. S., 2009. Study of Neural Network Models for Static Assessment in Power Systems, *International Journal of Research and Reviews in Applied Sciences*, Vol. 1, Issue 2, pp. 104-117.

Khattab H. M, Abdelaziz A. Y., Mekhamer S. F. and Badr M. A. L., 2011. Static Security Assessment Using a Probabilistic Neural Network Based Classifier, *Online Journal on Electronics and Electrical Engineering (OJEEE)*, Vol. 3, No. 4, pp. 454–461.

Lo K. L., Peng L. J., Maqueen J. F., Ekwue A. O. and Cheng D. T. Y., 1995. Application of Kohonen Self-Organising Neural Network to Static Security Assessment, *Artificial Neural Network's Conference Publication*, No. 409, pp. 387-392.

Mansour Y., Vaahedi E., El-Sharkawi M. A., 1997. Large Scale Dynamic Security Screening and Ranking using Neural Networks, *IEEE Trans. on Power Systems*, Vol. 12, No. 2, pp. 954-958.

Morison K., Wang L. and Kundur P., 2004. Power System Security Assessment, *IEEE Power & Energy Magazine*, Vol. 2, No. 5, pp. 30-39.

Niebur D. and Germond A. J., 1992. Power System Security Assessment Using Kohonen Neural Network Classifier, *IEEE Trans. on Power Systems*, Vol. 7, No. 2, pp. 865-872.

Pang C., Prabhakara F., Al-Abiad A. and Koivo A., 1974. Security Evaluation in Power Systems Using Pattern Recognition, *IEEE Trans. on PAS*, Vol. 93, No. 2, pp. 969-976.

Saeh I. S. and Khairuddin A., 2008. Static Security Assessment Using Artificial Neural Network, *Proceedings of the 2nd IEEE International Conference on Power and Energy (PECon 08)*, Juhor Baharu, Malysia, pp. 1172-1177.

Santo M. D. and Vaccaro A., 2004. A Distributed Architecture for Online Power System Security Analysis, *IEEE Trans. on Industrial Electronics*, Vol.51 No. 6, pp. 1238-1248.

Shukla M. and Abdelrahman M., 2004. Artificial Neural Networks Based Steady State Security Analysis of Power Systems, *Proceedings of the Thirty-Sixth Southeastern Symposium on System Theory*, pp. 266-269.

Sterpu S., Lu W., Basenger Y. and Hadjisaid N., 2006. Power System Security Analysis, *Proceedings of the IEEE Power Engineering Society General Meeting*.

Swarup K. S. and Corthis P. B, 2002. ANN Approach Assesses System Security, *IEEE Computer Applications in Power*, Vol. 15, No. 3, pp. 32-38.

Stott B., Alsac O. and Monticelli A. J., 1987. Security Analysis and Optimization. *Proceedings of the IEEE*, Vol. 75, No. 12, pp. 1623-1644.

Wang H., Lai J., Liu X. and Liang Y., 2007. A Quantitative Forecast Method of Network-Situation-Based on the BP Neural Network with Genetic Algorithm, *Proceedings of the Second International Multi-symposium on Computer and Computational Sciences Theory, IMSSCS*, pp. 374-380.

Wardwick K., Ekwue A., Aggarwal A., 1997. Artificial Intelligence Techniques in Power Systems, *IEE, London, UK*.

Yin J., Huo L., Gue L. and Hu J., 2008. Short Term Load Forecasting Based on Improved Gene Expression Programming, *Proceedings of the 7th World Congress on Intelligent Control and Automation*, Chongain, China, pp. 5847–5850.

http://www.ee.washington.edu/research/pstca/Power System Test Case Archive.

Zhou C., Xiao W., Nelson P. C. and Tripak T. M., 2003. Evolving Accurate and Compact Classification Rules with Gene Expression Programming, *IEEE Transactions on Evolutionary Computation*, pp. 519–531.

Biographical notes

Said F. Mekhamer was born in Egypt in 1964. He received the B.Sc. and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, and the Ph.D. degree in electrical engineering from Ain Shams University with joint supervision from Dalhousie University, Halifax, NS, Canada, in 2002. He is currently an Assistant Professor in the Department of Electric Power and Machines, Ain Shams University. His research interests include power system analysis, power system protection, and applications of AI in power systems.

Almoataz Y. Abdelaziz was born in Cairo, Egypt, on September 14, 1963. He received the B. Sc. and M. Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt in 1985, 1990 respectively and the Ph. D. degree in electrical engineering according to the channel system between Ain Shams University, Egypt and Brunel University, England in 1996. He is currently a professor of electrical power engineering in Ain Shams University. He was the head of consultant engineers of the electrical group in the General Directorate for Projects & Maintenance, King Saud University, Riyadh, KSA from 2005 to 2007. His research interests include the applications of artificial intelligence to power systems and protection and new optimization techniques in power systems operation and planning. He has authored or coauthored more than 100 refereed journal and conference papers. Dr. Abdelaziz is a member of the editorial board and a reviewer of technical papers in several journals. He is also a member in IET and the Egyptian Sub-Committees of IEC and CIGRE`. Dr. Abdelaziz has been awarded Ain Shams University Prize for distinct researches in 2002 and for international publishing in 2010, 2011.

H. M. Khattab was born in Cairo, Egypt in 1980. He received the B. Eng. Degree (Honors) and M. Sc. in electrical engineering from Ain-Shams University in Cairo, Egypt in 2001 and 2005, respectively. He is now working for the Ph. D degree in electrical engineering from Ain-Shams University in Cairo, Egypt. Currently he is an electrical engineer in the Engineering for the Petroleum and Process Industries (ENPPI). His research interests include the application of artificial intelligent techniques to power systems and new optimization techniques in power systems operation, protection and planning.

Mohamed A. L. Badr was born in Cairo, Egypt in 1944. He received the B. Eng. Degree (Honors) and M. Sc. in electrical engineering from Ain-Shams University in Cairo, Egypt in 1965 and 1969, respectively. He received Ph. D degree from the Polytechnic Institute of Leningrad in the former Soviet Union in 1974. Currently he is emeritus professor of electrical power and machines in Ain Shams University. Dr. M. A. L. Badr had been Professor of Electrical Machines in Ain Shams University since 1984. He had been the chairman of the Dept. of Electrical Power and Machines for 6 years. He headed the Electrical Engineering Dept. at the University of Qatar at Doha for five years. He was granted a post-doctor fellowship at the University of Calgary, Alberta, Canada between 1980 and 1982. Dr. Badr is a senior member IEEE since 1990. Dr. Badr has supervised a large number of Ph. D. and. M. Sc. research work in electrical machines and power systems, the areas in which he is interested. He is the author and co-author of many published refereed papers.

Received July 2012
Accepted August 2012
Final acceptance in revised form August 2012