International Journal of Engineering Studies.
ISSN 0975-6469 Volume 7, Number 1 (2015), pp. 31-43
© Research India Publications
http://www.ripublication.com

An overview of Integrated Security modeling for Steady State Security Assessment in Power systems

R.Thamizhselvan

*Assistant Professor, Department of Electrical Engineering,
Annamalai University, Tamil nadu – 608 002, India.*

Abstract

Currently, the field of pattern classification is admired one because of growth in Artificial intelligence and neurocomputing models. An well-organized integrated security modeling of power system operation via artificial intelligence techniques has been investigated in this paper. An integration of Artificial neural Networks (ANN) Based pattern classifier with feature selection is able to classify the power system operating condition into secure or insecure state expertly replacing existing Models for real time computations. Simulation results were obtained from ANN models such as Back propagation neural networks (BPNN) and Probabilistic neural networks (PNN) with Correlation based F-Value feature reduction overcomes the difficulties of longer computational time and voluminus results of existing ANN security Classifiers.

Keywords: Artificial Neural Networks, Probabilistic Neural Networks, Steady state Security Assessment, Feature Selection.

INTRODUCTION

Due to current rise in demand of electrical energy, almost power systems networks which comprise generation, transmission and distribution will grow both in size and complications, all together security highly concerns. Therefore, it is forced to operate most of the power system utilities closer to their security limits.

Our confidence on electricity is so large that it is momentous to have continuous deliver of electrical power within pre fixed limits of frequency and voltage levels. Uncertainties in load demand does not attain certain safe secure limits due to propagation of unplanned disturbances consequently creates a severe load on power system operators. During such delicate situation, any disturbance could cause danger to system security and may lead to system collapse. Therefore, there is a pressing need to develop fast on-line security assessing technique, results security evaluation is carried out in a short time [1].

Power system security assessment may be separated into three modes: (i) steady state security characterizing the steady state performance of the system, *(ii)* transient security which concerns with the transient stability of the system when it is subjected to a disturbance and *(iii)* dynamic security which pertains to the system responses of the order of a few minutes [1,2].

The development of Static Security Assessment (SSA) is only considered in this paper work. Static security evaluates post contingency steady state condition of the system, neglecting the transient behavior and other time dependent variations[4].

Existing literatures, expose that, Conservative security assessment procedures such as comprehensive steady-state load flow analysis with all possible contingencies and it makes real time security analysis for practical power systems impracticable. In this connection, the computation of Security assessment problems are classified into Quantitative approach and Qualitative approach [3]. The Quantitative approach relates to linear non-iterative, linear iterative and alternative methods. The qualitative approach deals with pattern recognition approaches like Experts Systems (ES), Artificial Intelligence techniques so on[4].

Many Artificial Intelligence (AI) techniques, based on neural networks have been presented [5,6] to solve static security assessment problems. Self-Organizing Feature Map have been applied for the problem of static security assessment in [6] and Decision tree based security classifier[7], genetic based neural network [8], fuzzy logic combined with neural network [9], query-based learning approach in neural networks [10] for static security evaluation process have also been reported in [10,11,12,13,14]. But these procedures are found to be highly time consuming and infeasible for real time applications as they are based on the nature of inputs provided [3]. Hence to overcome this problem, ANN based fast learning networks are significantly ultimate choice for solving static security assessment problems and overcomes the flaw of Existing ANN models such as slower computation, inconsistent results due larger networks, etc.

The ANN based pattern classification for security evaluation has few steps, namely, training process which performed off-line and Classification which performed on-line. the proper selection of training feature set, characterizing the behavior of entire power system [4]. Moreover, it is not necessary to keep all the relevant datas even preprocessing of pattern classification. A rule based or knowledge based feature selection algorithms are accessible to evade unwanted and repeated datas in the dataset which improves the performance of classifier.

The proposed ANN and SVM based classification approach is implemented on standard IEEE 14 bus system. The simulation results prove that the ANN based proposed PNN classifier gives an efficient classification, enhancing its suitability for on-line security assessment even reduction in Computation time and space remarkably.

METHODOLOGY

Power System Operation and security concepts

In practice, considering safe and reliable power transaction, The power system should operate in steady state, must satisfy load flow constraints the power flow between the lines and transformers in a power system is strictly governed by the network equations and expressed as a set of mathematical equalities and inequalities [15],i.e.

$$P_{G\,i} - P_{L\,i} = V_i \sum_{J=1}^{n} V_j \,.Y_{i\,j}.cos(\delta_i - \delta_j - \theta_{i\,j}) \qquad (1)$$

$$Q_{G\,i} - Q_{L\,i} = V_i \sum_{J=1}^{n} V_j \,.Y_{i\,j}.sin(\delta_i - \delta_j - \theta_{i\,j}) \qquad (2)$$

$$P_{G_{Max\ i}} \geq P_{G\,i} \geq P_{G_{Min\ i}} \qquad (3)$$

$$Q_{G_{Max\ i}} \geq Q_{G_{\ i}} \geq Q_{G_{Min\ i}} \qquad (4)$$

$$V_{Max\ i} \geq V_{i_{.}} \geq V_{Min\ i} \qquad (5)$$

$$\alpha_{i\,j} \geq |\delta_{i\,j}| = |\delta_i - \delta_j|, \qquad (6)$$

i =1, 2….n /j = i+1… n

The above equalities and inequalities (1)-(6), may be expressed in compact form,

$$g(x, u) = 0 \qquad (7)$$

$$h(x, u) \leq 0 \qquad (8)$$

where *u* is a set of independent variables and *x* is a set of dependent variables, the constraints *g(x,u)=0* and *h(x,u) ≤ 0,* are satisfied, the power system is said to be in the normal operating state. Likewise the constraints *g(x,u)=0* are satisfied and inequality constraints *h(x,u) ≤ 0* is violated, it said to be in the emergency state. the subset of euality constraints *g(x,u) = 0* is violated and all the inequality constraints *h(x, u)* ≤ 0 are satisfied, the power system is said to be in the restorative operating state[2].

Suppose that, a power system persists in the normal operating state is subjected to the set of disturbances such as a single line outage, loss of generator, sudden loss of load, and sudden change of power flow in inter-tie, then the system condition is said to be secure, otherwise ,it is insecure.

Steady state security assessment

A power system is said to be “static secure,” if the bus voltage magnitudes and line flows are well within their prescribed limits, refer equations *(1)* to *(6)* [19].

In this work, the minimum and maximum bus voltage magnitude limits are lies between 0.94 p.u –1.06 p.u for IEEE 14 bus system and line over load limit in MVA

[5] is taken as 130 % of base MVA flow. In power system static security assessment process, the power system operating state is said to be secure if the bus voltage magnitude limits and line over load limits are within the specified limits, if anyone of the constraint is violated, the system is said to be insecure.

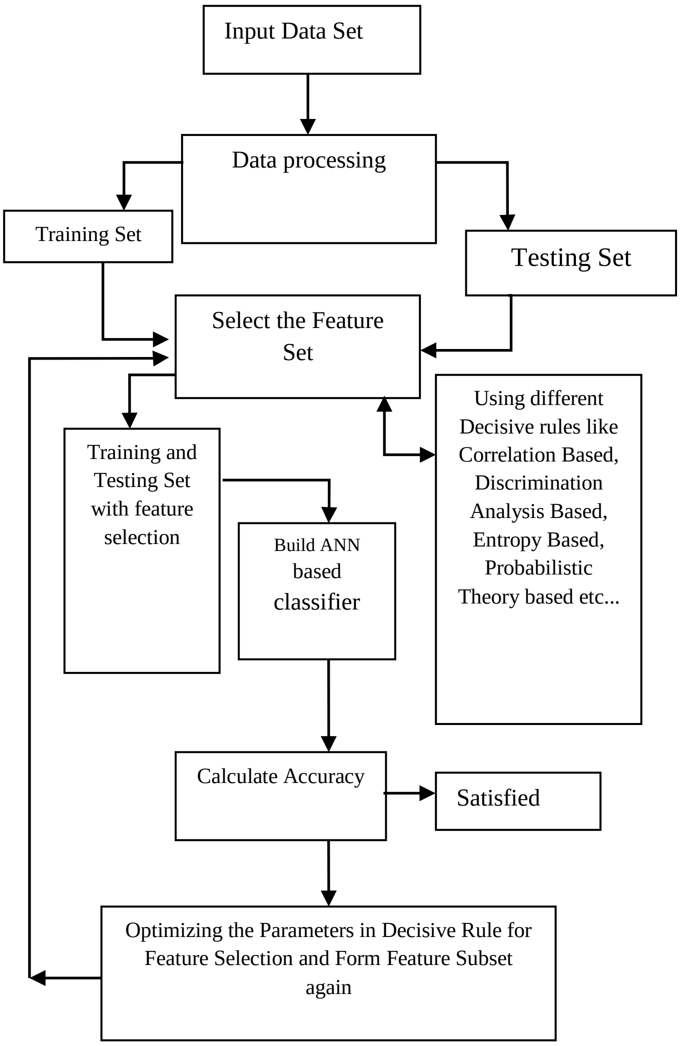
Input Data Set
Data processing
Training Set
Testing Set
Select the Feature Set
Using different Decisive rules like Correlation Based, Discrimination Analysis Based, Entropy Based, Probabilistic Theory based etc...
Training and Testing Set with feature selection
Build ANN based classifier
Calculate Accuracy
Satisfied
Optimizing the Parameters in Decisive Rule for Feature Selection and Form Feature Subset again

Figure 1. Integrated steady state security Classifier Model

The block diagram of Integrated steady state security Classifier Model is shown in Figure.1. The need for determination of small of variables which will be unique for every class of patterns has been analysed.

Generation of Training and Testing Data set

In this off-line process, The data are generated for various operating condition by varying the load between 90 to 130% of the base case and The variation in generation is bounded to their min-max generation limits and the voltage magnitude are taken between 0.94 pu –1.06 pu for all test systems and line over load limit in MVA [5] is taken as 130% of base MVA flow. For each operating condition, Single line outage is simulated and load flow solution by Newton Raphson (NR) method is obtained. For each operating condition, the corresponding pattern vectors are obtained. Each operating condition has number of operating variables called as pattern vectors. In this paper, voltage magnitude $V_{i,}$ voltage angle $\delta_{i,}$ real power generation P_{gi}, reactive power generation Q_{gi}, real power demand $P_{Di,}$ reactive power demand $Q_{Di,}$ active P_{i-j} the real power flow in line connected between buses i and j, Qi_{-j} the reactive power flow in line connected between buses i and j, S_{i-j} line MVA between buses i and j have been considered. Evaluating the security constraints, each pattern is labeled as secure or insecure state.

FEATURE SELECTION TECHNIQUES

Correlation based F-Value Feature selection method

In general, the number of variables characterizing a power system operating state is quite large. This makes the security classifier design complicated and requires large computational resources [15]. Also, all the variables characterizing the system operating state may not contain useful information for the purpose of classification. Thus, there is a need to reduce the number of variables to be used for classifier design. The process of extracting a subset of features from the set of variables is termed as feature selection [10].

The feature selection process can be concluded in the following stages; first the features are selected from pattern vector based on maximization of a criterion function. The F-value defined by eqn (9.0) is used as the criterion function for selection of a variable as feature

$$F = \frac{|m_s - m_i|}{(\sigma_s^2 + \sigma_i^2)} \qquad (9)$$

Where, m_s - Mean of the variable in the secure class, m_i- Mean of the variable in the insecure class; σ_s^2 - Variance of the variable in the secure class; σ_i^2- Variance of the variable in the insecure class.

The selection of features begins with the computation of F-values for all components (variables) of pattern vector in the training set. The variable with the largest F value is selected as the first feature. Let this variable be z_1. When selecting other features, redundant information is omitted by discarding these variables which are correlated to z_1, i.e. those variables having a correlation coefficient greater than 0.8,[10] say. Now from the remaining variables, the one with the largest F-value is selected as the second feature,z_2. The procedure is repeated until all the variables are considered and required features are selected .The optimal set of above features serves as an input database for designing AI based classifier.

ANN Based Security Classifier

In the recent years, the evolution of the AI techniques, particularly, Artificial Neural Network (ANN) based techniques has been productively established in performing numerous complicated tasks, for instance character recognition and pattern recognition.

Back Propagation Neural Network

Back-propagation (BP) is a supervised learning procedure implemented for training ANNs[16]. The BP is employed to feed forward ANN having one or more hidden layers. In BPNN, the errors extend in the reverse direction from the output nodes to the interior nodes. it computes the increase or decrease in the magnitude of error with respect to the changes in weights.

It differs in the manner in which the weights are computed during the learning phase. The complexity with multilayer neural network is the computation of weights for the hidden layers in an efficient way that results in minimum output error. To revise the weights, the errors have to be calculated. The magnitude of errors can be measured easily at the output. The error is actually the variations at the hidden layers among the actual and desired output. To acquire the optimum number of neurons in the hidden layer, the number of neurons is varied from 5 to 30 and the average errors are compared. For every change in the hidden units, the minimum average errors are noted**.**

The ANN trains with the binary outputs of 1 and 0. Practically, the output is closer to analog values in a range 0 and 1. An acceptable classifier result can be reset to 1 and 0 if the output value is > 0.5 and ≤ 0.5, respectively. The output layer provides the information on the severity level of the limit violation.

Probabilistic Neural Network

PNN is a NN with multi layer utilized for pattern classification problems[17].The PNN is a non-linear, nonparametric pattern recognition algorithm based on probability density function of the train set optimized kernel width parameter[18].The PNN has four layers that is, input, pattern, summation and output layers as revealed in Figure.2. The input layer has distribution units, which offers analogues assessments to the complete pattern layer. RBF has been utilized as activation function for the pattern layer of the projected Security assessment

The output can be articulated as,

$$a = \textit{radbas}\ (||IW_{1.1} - p||b) \qquad (10)$$

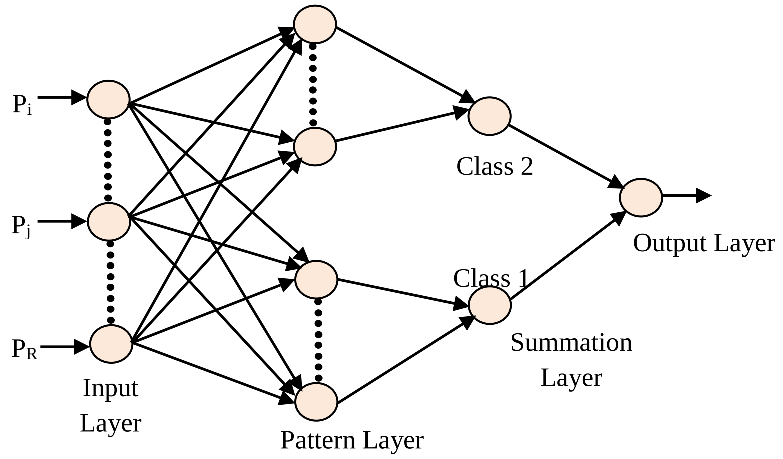

Figure 2. Layers of the PNN

Where 'radbas' symbolizes the RBF activation function.
In general ,RBF activation function is expressed as

$$\text{radbas (n)} = e^{n^2} \tag{11}$$

PNN Algorithm

Step1: The data for training are standardized and given as input.

Step 2: The training data are passed into the pattern layer and after that the Euclidean distances for every the training data is determined.

Step 3: The predicted Euclidean distances of each element are multiplied with bias and provided as input for the RBF.

Step 4: The network is trained in the pattern layer by setting every pattern in training data equal to the weight vector in one of the pattern neurons and connecting its output to the appropriate summation neurons.

Step 5: At the summation layer, by referring to the desired outcome of the training data, the calculated RBF centers are separated between class 1 and 0. The amount of neurons in the summation layer is equivalent to the number of classes. Every neuron there in summation layer relates to the computation of an approximation of probability density for class 1 and 2.

Step 6: The outcome of the summation neurons is written as follows:

$$S_k(x) = \sum_{i=1}^{n_k} \phi_i(\| x - c_{ki} \|^2) \tag{12}$$

$$\text{Where}\, \phi_i(\| x - c_{ki} \|^2) = \exp\left(- \frac{\| x - c_{ki} \|^2}{\sigma_i^2} \right) \tag{13}$$

S_k, the output of summation neuron, k =1,2, ... , N.

N denotes the entire layer of neurons in the summation layer; x, input data; C_{ki}; i^{th} hidden RBF center vector for the k^{th} pattern class of the pattern layer; n_k, number of the hidden center vector for the k^{th} pattern class of the pattern layer; $\|\cdot\|$ is Euclidean distance; $\phi i(\cdot)$ is RBF activation function and σ_i smoothing factor.

Step.7: The output layer is the decision layer used for implementing the decision rule by selecting the maximum posteriori probability of each class from the outputs preceding the summation layer.

$$d(x) = Cj, \quad \text{if } Sj\ (x) > Sl\ (x) \ \text{ and } j \neq l \qquad (14)$$

Where d(x) is decision of the output layer, Sj(x) and Sl(x) are summation neurons for class j and class l; C_j is class j.

Step 8:Testing of the trained PNN with the testing data to classify the test system according to class 1 (secure) or class 0 (insecure).

Performance Evaluation of ANN based classifier
To evaluate the performance of ANN based classifiers as follows,

$$\text{Classification Accuracy (\%)} = \frac{\text{Number of correct samples}}{\text{Total samples}} \text{ x } 100$$

$$\text{Misclassification (\%)} = \frac{\text{Number of false samples}}{\text{Total samples}} \text{ x } 100$$

$$\text{False Alarm (\%)} = \frac{\text{Number of false alarms}}{\text{Total true secure states}} \text{ x } 100$$

$$\text{False Dismissal (\%)} = \frac{\text{Number of false dismissals}}{\text{Total true insecure states}} \text{ x } 100$$

SIMULATION RESULTS AND DISCUSSION

The design of ANN based classifier models for static security assessment is implemented and tested on IEEE 14 bus standard test system [26] and the effectiveness of the proposed classifier has been demonstrated by comparing these two Neural Networks. The data set required for training and testing phases are obtained by off-line simulation performed using MATPOWER Toolbox with MATLAB 7.1[25]. This data set is obtained by varying the generation and load from 90% to 130% of their base case value with generation variation restricted to their minimum and maximum limits.

The IEEE-14 bus sample system has 2 generators, 14 buses, 20 lines and 3 condensers. One at a time, outage studies are performed and form the set of disturbances to be utilized for steady state security in the Power system. The patterns or variables are generated through the load flow results. Table-1 shows the results of data generated for training, testing of ANN classifier and feature reduction process. For a possible 209 operating scenarios, 84 operating scenarios are found to be secure and the remaining 125 cases are found to be insecure. The training and testing samples are split in random by the ratio of 80 %(167 cases) for training phase and 20% (42 cases) for testing phase.

Table 1. Data set for Training and Testing Phase

Scenarios	**Overall cases**	**Training cases**	**Testing cases**
Total no of cases	209	167	42
Secure cases	84	61	23
Insecure cases	125	106	19

Table-2 shows an optimal set of patterns selected by F-Value method with a threshold value of 0.8.

Table 2. Feature Selection Process

Case study	**IEEE14 Bus system**
No. of pattern variables	110
No. of features selected	47

Performance Evaluation of BPNN classifier

Table.3and 4 shows, The performance evaluation of neural network based BPNN classifier is computed with and without use of feature selection process.

Table 3. Performance Evaluation of BPNN classifier without Feature selection

Per**formance Evaluation**	**Without Feature selection (110 patterns)**	
	Training	Testing
Accuracy (%)	100(167/167)	**83.3** (35/42)
Misclassification (%)	0(0/167)	16.6 (7/42)
False alarm (%)	0(0/60)	20.8(5/24)
False Dismissal (%)	0(0/107)	11.1 (2/18)

Table 4. Performance Evaluation of BPNN classifier with Feature selection

Performance evaluation	**With Feature selection (47 patterns)**	
	Training	Testing
Accuracy (%)	100(167/167)	92.8(39/42)
Misclassification (%)	0(0/167)	7.14 (3/42)
False alarm (%)	0(0/60)	8.33(2/24)
False Dismissal (%)	0(0/107)	5.5(1/18)

Performance Evaluation of PNN classifier

Table.5 and 6 shows, The performance evaluation of PNN classifier is calculated with and without use of F-value feature selection method.

Table 5. Simulation results of performance calculation of PNN classifier without Feature selection

Per**formance Evaluation**	**Without Feature selection (110 patterns)**	
	Training	Testing
Accuracy (%)	100(167/167)	**90.47** (38/42)
Misclassification (%)	0(0/167)	9.52(4/42)
False alarm (%)	0(0/60)	16.6(4/24)
False Dismissal (%)	0(0/107)	0 (0/18)

Table 6. Simulation results of proposed PNN classifier with Feature selection

Performance evaluation	**With Feature selection (47 patterns)**	
	Training	Testing
Accuracy (%)	100(167/167)	**95.23** (40/42)
Misclassification (%)	0(0/167)	4.76 (2/42)
False alarm (%)	0(0/60)	8.33(2/24)
False Dismissal (%)	0(0/107)	0(0/18)

Results shown in Table 6 and 4, prove that the classification accuracy of PNN classifier with feature selection is 95.23% as compared with accuracy of BPNN classifier is 92.8% with feature selection. This is clearly evident that the performance of the PNN classifier is improved with selection of good feature variables and suitable for online /real time security evaluation.

CONCLUSION

An integrated methodology of ANN based steady state security classifiers with feature selection have been proposed in this paper. The proposed correlation based F-value feature selection algorithm is an efficient tool to deal with the problem of high dimensionality and well fitted with both BPNN and PNN classifiers. Results prove that, the reduced dimensional features are more accurately classified using PNN classifier even better than BPNN. simulation results reveals PNN with F value feature selection predicts well either secure or insecure states with astonishingly online execution time of 0.3 secs .

REFERENCES

[1] S.L surana, application of PR Techniques to steady state security evaluation of power systems.

[2] D. Kirschen, “Power system security”, Journal of Power Engineering, Vol. 16, No. 5, pp. 241–248, 2002.

[3] F.M. Echavarren, E. Lobato, L. Rouco,T. Gómez, “Formulation, Computation and Improvement of Steady State Security Margins in Power Systems. Part II: Results”, Electrical Power and Energy Systems, Vol. 33, pp.347–358, 2011.

[4] I. Pisica, T. Gareth, L. Laurentiu,“Feature Selection Filter for Classification of Power System Operating States”, Computers and Mathematics with Applications,Vol. 66 ,pp.1795–1807, 2013.

[5] S. Kalyani, K.S. Swarup, “Study of Neural Network Models for Security Assessment In Power systems”, International Journal of Research and Reviews in Applied Sciences, Vol. 1,No. 2, pp. 104-117,2009.

[6] I. Saeh and A. Khairuddin, “Static security assessment using artificial neural network,” in Proceedings of IEEE 2nd International overseas Energy Conference, pp. 1172– 1178, 2008.

[7] I.S.Saeh, A.Khairuddin, “Decision Tree for Static Security Assessment and Classification”, International Conference on Future Computer and Communication (ICFCC), pp.681-684, 2009.

[8] K. Swarup, P. Corthis, “Power System Static Security Assessment using Self-Organizing Neural Network. Journal of Indian Institute of Science,Vol. 86,pp.327–342, 2006.

[9] M. Boudour, A. Hellal, “ Combined use of supervised and unsupervised learning for large scale power system static security assessment”,. International Journal of Electrical Power & Energy Systems, Vol. 26, No. 2, pp. 157–163, 2006.

[10] K. R. Niazi, C. M. Arora, S. L. Surana, “Power system security evaluation using ANN: feature selection using divergence”, Electric Power Systems Research, Vol. 69, No.3, pp. 161-167, 2004.

[11] A. Mohamed, S. Maniruzzaman, A. Hussain, "Static Security Assessment of a Power System Using Genetic-Based Neural Network", Electric Power Components and Systems, vol. 29, No. 12, pp. 1111–1121, 2001.

[12] J. Srivani, K.S. Swarup, "Power system static security assessment and evaluation using external system equivalents", International Journal of Electrical Power & Energy Systems,Vol. 30,No.2,pp. 83–92, 2008.

[13] S. Huang, "Static security assessment of a power system using query-based learning approaches with genetic enhancement", IEEE Proceedings of Generation, Transmission and Distribution, Vol. 148, pp.319-321, 2001.

[14] W. Luan, K. Lo, Y.Yu, "ANN-based Pattern Recognition Technique for Power System Security Assessment", International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, pp.197–202,2000.

[15] C.K. Pang, A.J. Koivo, and A.H. El-Abiad. "Application of Pattern Recognition to Steady-State Security Evaluation in a Power System", IEEE Transactions on Systems, .Man and Cybernetics, Vol. 3, No. 6, pp. 622–631,1973.

[16] S. Shah, S. Shahidehpour, "Automated reasoning: a New Concept in Power System Security Analysis", International Workshop on Artificial Intelligence for Industrial Applications, pp. 58–63, 1988.

[17] Wahab, N.I.A., Mohamed, A. and Hussain, "Fast Transient Stability Assessment of Large Power System Using Probabilistic Neural Network With Feature Reduction Techniques",, Expert Systems with Applications, Vol.38,No.9, pp. 112-119,2011.

[18] Wahab, N.I.A., Mohamed, A. and Hussain, A., "Transient stability assessment of a power system using PNN and LS-SVM methods",Journal of applied sciences, Vol.7,No.21, pp.3208-3216,2007.

[19] C.K. Pang, F.S. Prabhakara, A.H.El-Abiad, A.J. Koivo, "Security Evaluation in Power Systems Using Pattern Recognition", IEEE Transactions on Power Apparatus and Systems, Vol PAS-93, pp. 969–976, 1974.

[20] S.Weerasooriya, M.A. El-Sharkawi, M.Damborg , R.J.Marks II, "Towards Static-Security assessment of a Large –scale Power System using Neural Networks," Proceedings of IEEE-C,Vol. 139,No.1,pp. 64-70 ,1992.

[21] C.M.Arora and S.L.Surana,"Transient Security Evaluation by Pattern recognition Method Using Steady State Variables", Journal of Institution of Engineers(India),Vol. 73,pp.123-128,1992.

[22] D. Niebur and A. Germond, "Power system static security assessment using the Kohonen neural network classifier," IEEE Transactions of Power Systems, Vol. 7, No. 2, pp. 865–872,1992.

[23] M. Haghifam, V. Zebarjadi, "Fuzzy Logic and Neural Network Approach to

Static Security Assessment for Electric Power Systems", Proceedings of 4th European Congress on Intelligent Techniques and Soft Computing, Vol. 3, pp. 2009–2013, 1996.

[24] C.S.Chang, T.S.Chung and K.L.Lo, "Application of Pattern recognition technique to Power system Security Analysis and Optimization," IEEE Transactions on Power systems, Vol. 5, No. 3, pp. 835-841, 1990.

[25] S. Weerasooriya and M. El-Sharkawi, "Feature selection for static security assessment using neural networks," IEEE International Symposium on Circuits and Systems, 1992. ISCAS'92.Proceedings, Vol. 4, pp. 1693–1696, 1992.

[26] R. Zimmerman, D. Gan, "MATPOWER: A MATLAB Power System Simulation Package (Ver. 5.0)", software package, 2014.

[27] http://www.ee.washington.edu/research/pstca (Power System Test Case Archive), 1996.