International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 38362-38367
© Research India Publications. https://dx.doi.org/10.37622/IJAER/10.17.2015.38362-38367

Application of Support Vector Machine to Static Security Assessment in Power systems

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

S.Ganapathy
Professor
Department of Electrical Engineering,
Annamalai University,
Tamil nadu – 608002, India,

Abstract- In this paper, an accurate and efficient security assessment of power system operation using Support Vector Machine (SVM) has been presented. SVM is able to classify the power system operating condition into secure or insecure state efficiently. One of the most important aspects for an efficient power system security evaluation is the proper selection of training features. This paper investigates the use of correlation based F- value method for feature selection process. The SVM and feature selection algorithm were tested for security assessment on IEEE-14 bus system and test results are obtained. Simulation results obtained using SVM not only offer a very reliable security classification, but also provide a quantitative level of confidence for the security classification.

Keywords: Support Vector Machine, Static Security Assessment, Feature Selection, F-value method.

Introduction

Modern interconnected power systems are outsized and complex in nature and have forced power system utilities to operate closer to their security limits. Our dependence on electricity is so large that it is significant to have continuous supply of electrical power within set limits of frequency and voltage levels. Uncertainties in load demand forecasts and unplanned outages of equipment create a severe load on power system operators in trying to persuade all the consumers. 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, that can analyze the level of security and caution system operators to take some preventive actions in case need arises [1].

Conventional security assessment procedure involves comprehensive steady-state load flow analysis for all possible contingencies and it makes real time security analysis for practical power systems impossible. Automatic Contingency Selection schemes have been developed to lessen the computational burden by approximate methods. They also compute the severity of contingencies based on linear system model and uses fast approximate power flow solutions [9].

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 present work discusses in brief the process of Static Security Assessment (SSA) only. Static security evaluates post contingency steady state condition of the system, neglecting the transient behavior and other time dependent variations. In literature, many Artificial Intelligence (AI) techniques, based on neural networks have been presented [15, 16] to solve static security assessment problems. Self-Organizing Feature Map have been applied for the problem of static security assessment in [6] and Multilayer Feed forward with back propagation algorithm have been applied for the problem of static security assessment in [16]. The use of ANN based pattern recognition (PR) approach [14,17],Decision tree based security classifier[7], genetic based neural network [22], fuzzy logic combined with neural network [9], query-based learning approach in neural networks [13] for static security evaluation process have also been reported in [18,19, 20,21,22,23]. 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, Support Vector Machine (SVM) is found to be the opt method for solving static security assessment problems.

One of the important considerations in applying SVM to power system security assessment is the proper selection of training feature set, characterizing the behavior of the power system [4]. Many feature selection algorithms are available, such as fisher discrimination analysis, entropy maximization, etc [24].The key problem with the existing feature algorithms is that it works well with linearly separable classes, but not well established on non-linearly separable classes [25]. In this paper, the process of feature selection is performed by a simple approach called F-value method [15].

The proposed SVM based classification approach is implemented on standard IEEE 14 bus system. The simulation results prove that the SVM classifier gives an efficient classification, enhancing its suitability for on-line security assessment even evidences reduction in size of feature space and error rate by exploiting by way of an efficient feature selection method.

Power System Model and Approximations

The main intention of a power system is to provide adequate uninterrupted supply of power of certain quality to meet all the demand of the customers. The power system, when operating in steady state, must satisfy load flow constraints. These constraints are described in the following sections.

The power flow through the lines and transformers in a power system is strictly governed by the network equations. The power flow pattern depends on the load and the generation distribution and the network configuration. All the above conditions may be expressed in the following set of mathematical equalities and inequalities [15],

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

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

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

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

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

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

$i =1, 2....n$ / $j = i+1... n$

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, When all the equality and inequality constraints $g(x,u)=0$ and $h(x,u) \leq 0$, are satisfied, the power system is said to be in the normal operating state. When all the equality constraints $g(x,u)=0$ are satisfied and a subset of inequality constraints $h(x,u) \leq 0$ is violated, it said to be in the emergency operating state. When a subset of the equality constraints, $g(x,u) = 0$ is violated and all the inequality constraints $h(x, u) \leq 0$ are satisfied, the power system is said to be in the restorative operating state[2]. Now, the control objective is to restore all the supply and return the system to normal operating state. This concept has been utilized to understand the security status of the power system models.

Concept of Power System Security

In practice, it is not sufficient just to maintain a system in the normal operating state. Under certain conditions, the occurrence of some disturbances may cause the system to go into an emergency such as the overloading of lines and violation of voltage limits[15].security has come to mean the ability of a system to withstand without serious consequences any one of a preselected list of “credible” disturbances (“contingencies”) such as a single line out, a loss of a generator, sudden loss of a load, sudden change of flow in an inter-tie, a three phase fault in a system, loss of lines on the same right of way. Suppose that a power system in the normal operating state is subjected to the set of disturbances in the specified list then the system is said to be secure. Otherwise it is insecure.power system is “reasonably” safe from serious interference to its operation. Thus security assessment involves the evaluation of available data to estimate the relative robustness (security level) of the system in its present state or some near-term future state. The form that such assessment takes will be a function of what types of data are available and of what underlying formulation of the security problem has been adopted. Power system security may be split into three different modes, such as steady state security mode, transient security mode and dynamic security mode respectively [10]. Only studies on the steady state security mode are presented herein.

Understanding static security

Static security is the capability of the system to reach a steady state within the specified secure region following a contingency [1,2]. A power system is said to be “static secure,” if the bus voltage magnitudes and line flows are well within their prescribed limits [19].In this paper, the minimum and maximum bus voltage magnitude limits are taken between 0.94 p.u –1.06 p.u for test systems 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 status is assessed for different possible contingencies by solving the load flow equations. Different contingencies have been included such as outage of a transmission line or a transformer or a generating unit. 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.

Analysis of Data Classification Scheme

The situation of the power system is never static as the system load demand is always shifting; therefore some kind of security assessment must be carried out often to check if the system is secure or not [18]. The traditional security assessment requires repeated analysis of power flows. The effects of transmission and generator outage contingencies are simulated by power flow solution methods.

Generation of Training and Testing Data set

The data generation process is an off line process which should contain data for all possible operating condition of the power system. The data are generated for various operating condition by varying the load between 80 to 120% 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 $P_{i\text{–}j}$ the real power flow in line connected between buses i and j, $Qi_{\text{–}j}$ the reactive power flow in line connected between buses i and j, $S_{i\text{-}j}$ line MVA between buses i and j have been considered. Evaluating the security constraints, each pattern is labeled as secure or insecure state.

The overall performance of any security classifier is scaled by the following measures,

Accuracy: It defines the quality or state of being correctly classified.

Misclassification rate: It defines the numbers of samples wrongly classified.

False alarm: Is one in which the assessment says that the system is insecure while in reality no system constraints have been violated.

False dismissals: Is one in which the assessment says that, a critically insecure case was judged to be secure.

In power system security, the false alarms are not of much harm, but false dismissals may lead to brutal blackout [18].

Having selected the data set, the next step is to determine the number of features from the data set, before designing the SVM classifier.

Importance of Feature Selection

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 [18].

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,[15] 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 the SVM classifier.

Role of SVM Classifier

Support Vector Machine (SVM) is a comparatively new method for learning separating functions in pattern recognition (classification) problem [27].SVMs are often found to provide better classification results that other widely used pattern recognition classifiers, such as the maximum likelihood and neural network classifiers[25,26].

SVM performs the task of classification by first mapping the input data to a multidimensional feature space and then constructing an optimal hyperplane classifier separating the two classes with maximum margin. SVM performs minimization of error function by an iterative training algorithm to construct an optimal hyperplane [28].

Consider a training set $T = \{x_i, y_i\}$, where xi is a real valued n-dimensional input vector and $y_i \in \{+1,-1\}$ is a label that determines the class of data instance, x_i. The SVMs are employed for such two class problems. The optimal hyper plane (line between two classes) is determined by an orthogonal vector (*w*) and a bias (*b*). The points closest to the optimal separating hyperplane with the largest margin *ρ* are called as Support Vectors (SVs).

To construct this optimal separating hyper plane, the SVM classifier solves the following primal problem described as an optimization problem.

$$Min\ w, b, \xi\ \frac{1}{2} w^T w + C \sum_{i=1}^{N} \xi_i \qquad (10)$$

Subject to Constraints

$$y_i(w^T \phi(x_i) + b) \geq 1 - \xi_i\ ;$$

$$\xi_i \geq 0,\ i = 1, 2 \ldots N \qquad (11)$$

Where *w* is the weight vector of the hyper plane, C is the penalty parameter proportional to the amount of the constraint violation, ξ_i is the slack variable, ϕ (.) is a mapping function called 'kernel' function and b is the threshold. The kernel function maps data in input space to feature space where they are linearly separable. The concept of kernel mapping allows SVM models to perform separations even with very complex boundaries. Linear, radial and polynomial are mostly recommended kernel mapping functions in most SVM models [25].In this paper, Polynomial kernel has been selected for mapping the feature space under non linear environment.SVM for classification problem is performed by the following steps.

i). Data Scaling

The data samples in train and test sets need to be scaled properly before applying SVM. This is essential as kernel values depend on the inner products of feature vector. Scaling will prevent the domination of any feature over others and helps in improving generalization ability of SVM model [29, 31].

ii).SVM Model Selection

a. Choice of Kernel

The polynomial kernel is chosen because of its wide known accuracy. It is capable of conduct non-linear relation existing between class labels and input attributes. [28].

b.Adjusting the Kernel Parameters

The polynomial kernel is defined as,

$$K(x, y) = (x^T y+c)^d \tag{12}$$

where x and y are vectors in the input space, i.e. vectors of features computed from training or test samples and $c \geq 0$ is a free parameter trading off the influence of higher-order versus lower-order terms in the polynomial. When $c = 0$, the kernel is called homogeneous. As a kernel, K corresponds to an inner product in a feature space based on some mapping φ:

$$K(x, y) = [\varphi(x), \varphi(y)] \tag{13}$$

Using the multinomial theorem and regrouping the above equations(12)&(13), we get

$$K(x, y) = (x_i y_i+c)^2 \tag{14}$$

$$K(x, y) = \sum_{i=1}^{n} (x_i{}^2)(y_i{}^2) + \sum_{i=2}^{n} \sum_{j=1}^{i-1} (\sqrt{2 x_i x_j})(\sqrt{2 x_i x_j}) + \sum_{i=1}^{n} (\sqrt{2 x_i x_j})(\sqrt{2 x_i x_j}) + c^2 \tag{15}$$

Since, The final expression for SVM classifier can be written as

$$Sign\, (\textstyle\sum_{i}^{N} \alpha_i y_i K(x_i, x_j) + b) \tag{16}$$

The range of *'c'* , *'γ'* using grid search method and *'d'* are as given below

$c = 2^{-5}, 2^{-3} \ldots\ldots, 2^{15}$, $\gamma = 2^{-15}, 2^{-13}, \ldots, 2^{0}$ and d = 1,2,3 [25].

The optimal pair of (c, γ) is found to predict the performance of SVM in addition with the third kernel parameter ***d*** (degree). The above parameters are capable of generating various support vectors in predefined input feature space. These support vectors allow the network to rapidly converge on the data boundaries and consequently classify the inputs. The SVM is trained using the chosen kernel with optimal parameters, the scaled input and output data. After training the SVM, the model is tested with the test samples generated [26, 28, and 29].

Performance Evaluation of SVM classifier:

To evaluate the performance of the trained SVM classifier, the following parameters has to computed [31]:

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

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

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

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

Simulation results and discussion:

The design of SVM based classifier models for static security assessment is implemented and tested on IEEE 14 bus standard test system [23] and the effectiveness of the proposed classifier has been demonstrated by comparing with Back Propagation Neural Network. The data set required for training and testing phases are obtained by off-line simulation performed using MATPOWER Toolbox with MATLAB 7.1[30]. This data set is obtained by varying the generation and load from 80% to 120% of their base case value with generation variation restricted to their minimum and maximum limits.

The IEEE-14 bus sample system [32] 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. The generated variable set consists of 14 numbers of voltage magnitude variables (V_i), 14 numbers of voltage angle (δ_i), 2 numbers of real power generation variables (P_{gi}), 5 numbers of reactive power generation variables (Q_{gi}), 11 numbers of real power demand variables (P_{Di}), 11 numbers of reactive power demand variables (Q_{Di}), 20 numbers of active real power flow variables ($P_{i\text{-}j}$) , 20 numbers of reactive power flow variables ($Q_{i\text{–}j}$) and 20 numbers of line MVA variables ($S_{i\text{-}j}$). The trivial variables at certain buses such as zero load , zero generation and constant values are neglected and finally 110 patterns are considered for classification process [5]. All feasible 110 patterns are subjected to static security check with voltage limit and line flow limit.

Table-1 shows the results of data generated for training, testing of SVM classifier and feature extraction. 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	Training	Testing
Total no of cases	209	167	42
Secure cases	84	61	23
Insecure cases	125	106	19

Table. 2: Feature Selection Process

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

Table-2 shows an optimal set of patterns selected by using feature selection process, F-Value method. The effectiveness of the dimensionality reduction is determined with a threshold value of 0.8 and the highly correlated variables are discarded from the total pattern variables.

The performance of SVM classifier is computed with and without use of feature selection process. Table 3 shows the performance parameter selection of SVM classifier for static security assessment. The proper selection of optimal values for SVM performance parameters (*c, γ, d)* decides the higher value of classification accuracy and minimal error rate. In SVM, 'c' is a penalty weight for the slack variables. That means a high value of 'c' forces the SVM towards a hard-margin and a low 'c' value allows a softer bound and generally produces more support vectors resulting in higher classification accuracy [25]. The degree '*d*' is selected as 1. This is because higher value of '*d*' decreases the overall accuracy of SVM.

Table 3: Performance of SVM model for various'd'

Model (kernel)	*c*	*γ*	*d*	Prediction accuracy (%)
Polynomial	2^{15}	2^{-1}	1	95.23
	2^{15}	2^{-1}	2	92.85

Table.4: Classification of Static Security using SVM classifier

Performance 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)	4.16(1/24)
False Dismissal (%)	0(0/107)	16.6 (3/18)
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)	4.16(1/24)
False Dismissal (%)	0(0/107)	5.5(1/18)

Results shown in Table 4 prove that, the classification accuracy of SVM classifier with feature selection is 95.23% as compared with accuracy of 90.47 without feature selection. This is clearly evident that the performance of the SVM classifier is improved with selection of good feature set and elimination of redundant data from the overall data set.

Table 5 shows the comparative study of SVM classifier with Back Propagation Neural Network (BPNN) classifiers for static security assessment. Results prove that SVM is a preeminent classifier within a preselected contingent environment.

Table. 5: Comparative results of Static Security classification

Performance	SVM classifier	Back propagation NN classifier
Accuracy (%)	95.23	82.6
Misclassification (%)	4.76	13.29
False alarm (%)	4.16	8.79
False Dismissal (%)	5.5	12.86

Conclusion:

SVM-based static-security-assessment technique for IEEE 14 bus power system is proposed. The proposed SVM is a comparatively novel method adopted for constructing an optimal hyper plane via different kernels that separates the two classes with optimal margin in classification problems. A systematic methodology for feature selection of SSA using F-Value method has been implemented for the selection of optimal set of training features, which has improved the performance in assessing the security of the power system. The proposed correlation based feature selection algorithm is an efficient method to deal with the problem of high dimensionality in the design of machine learning classifiers. Results prove that, the reduced dimensional features are more accurately classified using SVM. The proposed model holds the promise as fast classifier for static security of large scale power systems.

References

[1] N. Balu , T. Bertram , A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M.G. Lauby, B.F. Wollenberg, J.N. Wrubel, "On-line power system security analysis", Proceedings. of IEEE Vol. 80 No. 2, pp. 262–282, 1992.

[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] A.K.Sinha and I.J.Nagrath,"Pattern Recognition Method for Power System Steady state Security Assessment", Journal of Institution of Engineers(India),Vol. 64,pp. 269-271,1984.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] J. Min and Y. Lee, "Bankruptcy prediction using support vector machine with optimal choice of kernel function parameter", Expert Systems with Applications, Vol. 28, No. 4, pp. 603–614, 2005.

[26] C. Hsu and C. Lin, "A comparison of methods for multi-class support vector machines", IEEE transactions on Neural Networks, Vol. 13, No.2, pp. 415–425, 2002.

[27] D. Duttam, "Trends in Pattern Recognition and Machine Learning", Defence Science Journal, Vol. 35, No. 3, pp. 327-351, 1985.

[28] N. Christianini, J. Shawe-Taylor, "An Introduction to Support Vector Machines and Other Kernel-based Learning Methods", MIT Press, Cambridge, 2000.

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

[30] C.-C. Chang, C. J. Lin, "LIBSVM: a Library for Support Vector Machines, 2001.(Software Available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.)

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