TJER 2012, Vol. 9, No. 1, 21-30

Classification of Static Security Status Using Multi-Class Support Vector Machines

S Kalyani*[a] and KS Swarup[b]

[a] Department of Electrical and Electronics Engineering, Kamaraj College of Engineering & Technology, Tamilnadu, India

[b] Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai - 600036, India

Received 23 February 2010; accepted 1 December 2010

Abstract: This paper presents a Multi-class Support Vector Machine (SVM) based Pattern Recognition (PR) approach for static security assessment in power systems. The multi-class SVM classifier design is based on the calculation of a numeric index called the static security index. The proposed multi-class SVM based pattern recognition approach is tested on IEEE 57 Bus, 118 Bus and 300 Bus benchmark systems. The simulation results of the SVM classifier are compared to a Multilayer Perceptron (MLP) network and the Method of Least Squares (MLS). The SVM classifier was found to give high classification accuracy and a smaller misclassification rate compared to the other classifier techniques.

Keywords: Static security, Classifier, Multi-class SVM, Pattern recognition

تصنيف أوضاع الأمن باستخدام دعم متجه الآلات المتعددة الدرجات

س. قليان * وك. س. سواروب

الملخص: تستعرض هذه الورقة دعم متجه الآلات المتعددة الدرجات على أساس التعرف على الأنماط كنهج ثابت لتقييم الأمن في أنظمة الطاقة الكهربائية. حيث تم تصميم هذا المصنف المتعدد الدرجات على أساس احتساب مؤشر رقمي ثابت يسمى مؤشر الأمن. وتم اختبار هذا المصنف بالتعرف على نمط النهج القائم على ٥٧ ناقل، ١١٨ ناقل و ٣٠٠ ناقل كنظام للمعايرة. كما تمت مقارنة نتائج المحاكاة من المصنف مع شبكة متعددة الطبقات وطريقة المربعات الصغرى. وقد أظهرت نتائج المقارنه بأن المصنف متجه الآلات المتعددة الدرجات أعطى دقة عالية التصنيف، وأقل نسبة خطأ في التصنيف مقارنة بتقنيات المصنفات الأخرى.

الكلمات الدالة: الأمن الثابت، المصنفات، متجه الآلات المتعددة الدرجات، التعرف على الأنماط.

Nomenclature

S_{km}	Complex power flow in branch k-m in Mega-Volt Ampere (MVA)
MVA $Limit_{km}$	Thermal limit of branch k-m in MVA
$\|V_k^{min}\|$	Minimum allowable voltage limit of k^{th} bus in p.u. (taken as 0.90 p.u.)
$\|V_k^{max}\|$	Maximum allowable voltage limit of k^{th} bus in p.u. (taken as 1.10 p.u.)
$\|V_k\|$	Bus voltage magnitude of k^{th} bus in p.u.
$\|P_{Gi}^{min}\|$	Minimum generation limit of i^{th} generator bus in Mega Watts (MW)
$\|P_{Gi}^{max}\|$	Maximum generation limit of i^{th} generator bus in Mega Watts (MW)
$\|P_{Gi}\|$	Real power generation of i^{th} generator bus in Mega Watts (MW)
δk	Voltage angle at i^{th} bus in radians
S_{Gi}	Complex power generation at i^{th} bus in MVA
S_{Li}	Complex power load at i^{th} bus in MVA
N_L	Number of branches (includes both transmission lines and transformers) in the system
N_B	Number of buses in the power system network
N_G	Number of generators in the power system network

*Corresponding author's e-mail: kal_yani_79@yahoo.co.in

1. Introduction

The Power System Security is an important concern in the planning and operational studies of power systems. The primary aim of an electric power system is to provide an adequate uninterrupted supply of electrical power to customer premises within the set limits of frequency and voltage levels. This task has to be solved in real time and in a safe, reliable and economical manner. Security assessment is the analysis performed to determine whether, and to what extent, the system is reasonably safe from serious interference during its operation. Occurrence of certain severe disturbances may cause the system to shift go to an undesirable emergency state, if the system security level is not previously well defined. Hence, effective control of power systems demands a quick security evaluation of their operating states (Arora, Surana 1996).

Power System Security enables a system to remain secure without serious consequences to any credible contingencies on pre-selected list. Security analysis may be broadly classified as Static Security Assessment (SSA) and Transient Security Assessment (TSA). Static security analysis evaluates the post contingency steady state condition of the system neglecting transient behavior and other time-dependent variations. Transient security analysis evaluates system performance in terms of rotor angle stability, as it progresses after a disturbance (Shahidehpour 2003). The traditional method used for static security analysis involves full AC load flow for each contingency scenario. This procedure is highly time-consuming and infeasible for real time applications (Pang *et al*. 1973; Pang *et al*. 1974). A method is, therefore, required to access security using real-time data. This leads to the application of the Pattern Recognition (PR) approach. In recent years, many Artificial Intelligence (AI) techniques have been proposed to overcome the pitfalls of the traditional method of security evaluation. AI techniques like the Self-Organizing Feature Map (Swarup, Corthis 2006), and the Multilayer Feed forward with a back propagation algorithm (Saeh, Khairuddin 2008) have been applied for the problem of static security assessment. Various literatures has also reported the use of an ANN -based Pattern Recognition approach (Boudour, Hellal 2006; Luan *et al*. 2000) - a Genetic-Based Neural Network (Azah, Maniruzzaman 2001), - a Fuzzy Logic combined with a Neural Network (Haghifam, Zebarjadi 1996), and a Query-Based learning approach in Neural Networks (Huang 2001) for the static security evaluation process. The performance of all these existing techniques are highly problem dependent and hence their suitability cannot be underestimated/minimized. Moreover, because of the nature of the input features used, these methods are found to be incapable of quickly predicting the future insecure operation.

Nowadays, Pattern Recognition (PR) techniques have demonstrated great importance in security evaluation of large electric power systems (Sa, Munro 1984). In the pattern recognition approach, the main bulk of simulation is done off-line to generate sufficient data for training set (Pang *et al*. 1974). Using the training data set, the classification function is designed, from which system security can be judged in a short period of time. This paper presents the application of Pattern Recognition (PR) approach to static security assessment of large scale power systems in multi-class mode. The classifier in the PR system is designed by Support Vector Machines (SVM). SVM is a new and promising tool for learning separating functions in a PR system with the capability of handling non-linear separability. The SVM classifier is designed for multi-class classification based on the calculation of a term called 'Static Security Index' (SSI), for each specified contingency. In this paper, four class logic is used for the definition of system security viz., secure, critically secure, insecure, highly insecure. An operator needs to know the exact severity level of disturbances for a given system operating condition. On-line security evaluation allows the operator to know the security status and determine the corrective actions.

2. Static Security Assessment (SSA)

Static security is the ability of the system to reach a state within the specified secure region following a contingency. A set of the most probable contingencies is first specified for security evaluation. This set may include single line outage, a loss of a generator, or a sudden increase in load. The violations of thermal limits of transmission lines and bus voltage limits are the main concerns for static security analysis. In conventional practice, security assessment is obtained by analytically modeling the network and solving the load flow equations repeatedly for all of the prescribed outages, one contingency at a time (Lo, Peng 1997). This traditional approach is not entirely satisfactory because the huge number of simulations needed to be carried out.

A given system operating condition is said to be 'static secure', if the bus voltage magnitudes and real power generation of generator buses are well within their limits, without any occurrence of line overloads. In this paper, the term, statis security index (SSI) indicates the system security level for a given system operating condition and a specified contingency. The SSI is defined by calculating the Line Overload Index (LOI), Voltage Deviation Index (VDI) and Generation

$$LOI_{km} = \begin{cases} \dfrac{S_{km} - \text{MVA Limit}_{km}}{\text{MVA Limit}_{km}} \text{x}100 & \text{if } S_{km} > \text{MVA Limit}_{km} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

$$VDI_k = \begin{cases} \dfrac{\left|V_k^{min}\right| - \left|V_k\right|}{\left|V_k^{min}\right|} \text{x}100 & \text{if } \left|V_k\right| < \left|V_k^{min}\right| \\ \dfrac{\left|V_k\right| - \left|V_k^{max}\right|}{\left|V_k^{max}\right|} \text{x}100 & \text{if } \left|V_k\right| > \left|V_k^{max}\right| \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

$$GDI_i = \begin{cases} \dfrac{\left|P_{Gi}^{min}\right| - \left|P_{Gi}\right|}{\left|P_{Gi}^{min}\right|} \text{x}100 & \text{if } \left|P_{Gi}\right| < \left|P_{Gi}^{min}\right| \\ \dfrac{\left|P_{Gi}\right| - \left|P_{Gi}^{max}\right|}{\left|P_{Gi}^{max}\right|} \text{x}100 & \text{if } \left|P_{Gi}\right| > \left|P_{Gi}^{max}\right| \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

Deviation Index (GDI) as given by Eqs. (1), (2) and (3) respectively.

$$\text{Violation Index} = \frac{W_1 LOI + W_2 VDI + W_3 GDI}{N_1 + N_2 + N_3} \quad (4)$$

$$\text{Static Security Index (SSI)} = 100 - \text{Violation Index} \quad (5)$$

where S_{km} and MVA Limit_{km} represent the MVA flow and the MVA limit of branch k-m, $|Vk^{min}|$, $|Vk^{max}|$ and $|V_k|$ the minimum voltage limit, maximum voltage limit and bus voltage magnitude of the k^{th} bus respectively. In addition, P_{Gi}^{min}, P_{Gi}^{max} and P_{Gi} represent the minimum generation limit, maximum generation limit and real power generation of the i^{th} generator bus respectively, and N_L, N_B and N_G represent the number of lines, buses and generators respectively.

3. Pattern Recognition (PR) Approach

A pattern is a pair comprised of an observation and a meaning. A Pattern Recognition infers meaning from observation. Pattern Recognition is defined as 'the act of taking in raw data and taking an action based on the category of data'. It aims to classify the data or patterns based on either priori knowledge or on statistical information extracted from the patterns (Pecas *et al*. 1988). A complete pattern recognition system, as shown in Fig. 1, consists of a sensor that gathers observations to be classified; a feature extraction mechanism that computes numeric or symbolic information from observations and a classification scheme that classifies the observations, relying on extracted or selected features.

4. Application of Pattern Recognition to Static Security Assessment

The classification of power system state is the primary stage of security assessment in large scale real power system networks. From a pattern recognition perspective, the SSA problem is considered to be a classification problem whereas the pre-contingency system attributes are used to predict the post contingency system security status.

Pattern Recognition can be seen as a classification process which is normally employed to reduce the on-line computational requirements. In designing a Pattern Recognition system, a considerable amount of work is done off-line. This work is used for the generation of a set of characteristic operating points necessary to design a classification function called the 'security function'. Once the classifier is derived, an actual assessment of any new data sample located on-line can be made by evaluating the security function and can be classified as belonging to any one of the multi-classes described. This makes the PR system

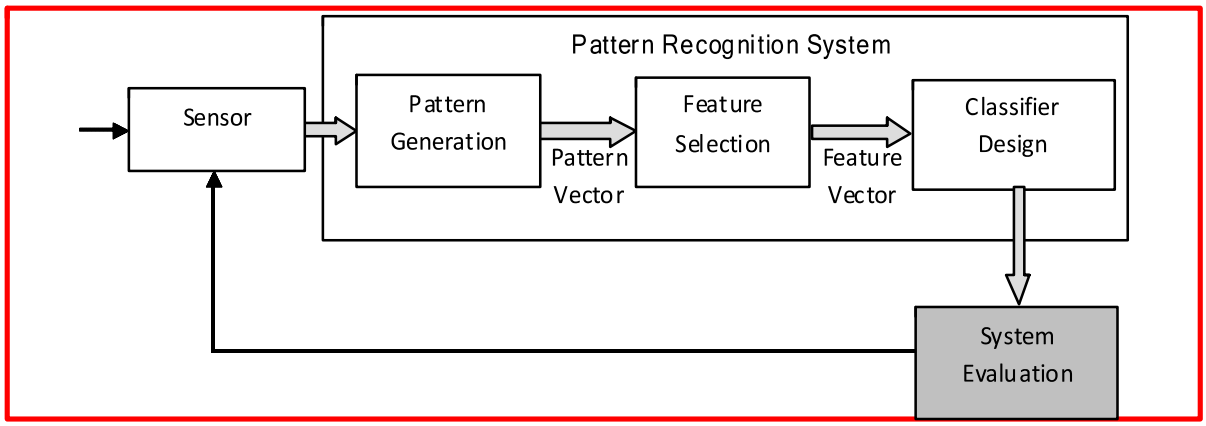


Figure 1. Block diagram of pattern recognition (PR) approach

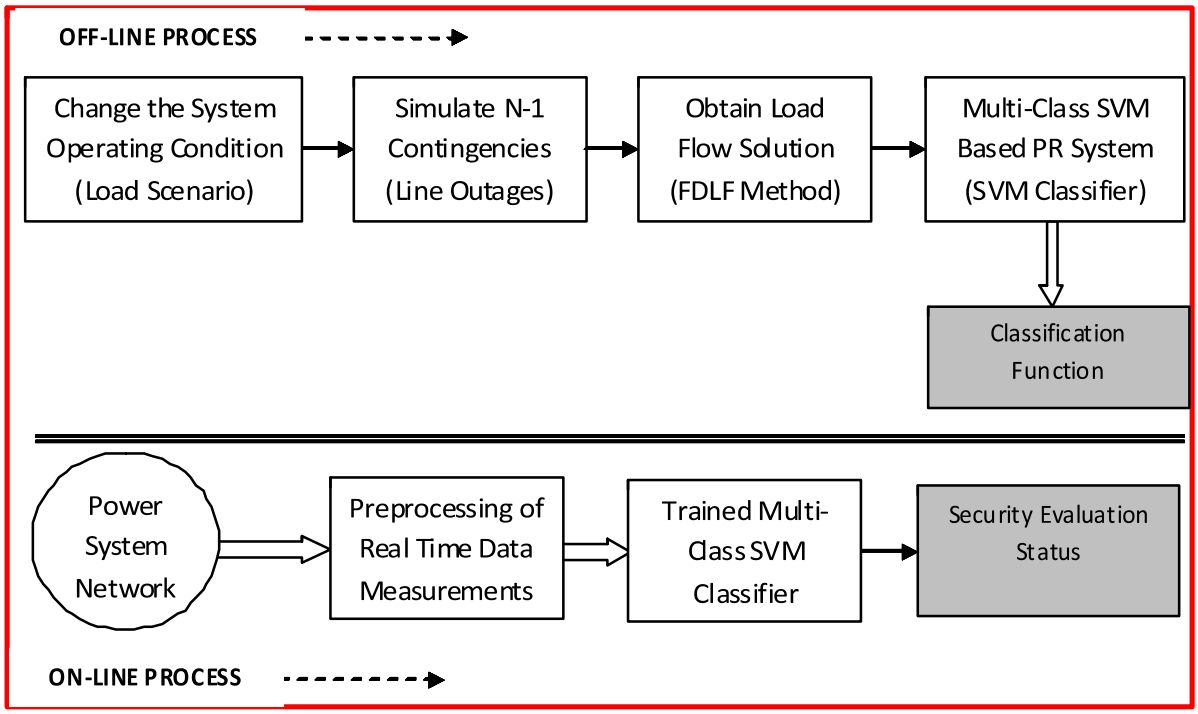


Figure 2. SVM based pattern recognition for static security assessment

much faster than any other method of security assessment. The sequence of steps performed in the off-line and on-line stages in applying a pattern recognition approach to static security evaluation is shown in Fig. 2.

4.1 Pattern Generation

The success of pattern recognition relies on a good training set. The training set patterns may be obtained on-line from real-time occurrences or can be synthesized from off-line simulations (Laveen 1974). In this paper, the train set and test set patterns are generated by off-line simulations. Different operating conditions were considered by varying the system load from 50% to 200% of base load. For each operating scenario, single line outages (one at a time) are simulated and a load flow solution is obtained. Evaluating the static security index (SSI) as given by Eq. (5), each pattern is labeled as belonging to one of four classes - Secure, Critically Secure, Insecure and Highly Insecure. All variables describing an operating condition constitute the components of Pattern vector represented as $X = \{x_1, x_2, x_n\}$. These variables include loads, generation's power flows in lines, voltage magnitude and angle at buses. The primary variables called steady state variables, forming the components of pattern vector are given below:

$$X = \{|V|_k, \delta k, S_{Gi}, S_{Li}, S_{km}\}$$

where

$|V|_k$ voltage magnitude at bus i

δ_k voltage angle at bus i
S_{Gi} complex power generation at generator bus i
S_{Li} complex power load at load bus i
S_{km} MVA power flow in branch k-m

4.2 Feature Selection

The number of variables describing the power system state in the pattern vector is significantly large. This phase involves selecting from a large set of variables that will give more useful information to build the classification function. These variables are termed features and the process of obtaining them is called feature selection (Siri *et al*. 1992). The features form the components of a vector called feature vector represented as $Z = \{Z_1, Z_2, \ldots, Z_m\}$. The importance of feature selection is to reduce the unclear of dimensionality and the search space for learning algorithm.

Input features may be selected by engineering judgment. But such selections will be subjective with the possibility of important variables that are rejected. A common method of feature selection is sequential feature selection, consisting of two components - an objective function called criterion and a sequential search algorithm. In this paper, a 'Sequential Forward Selection' (SFS) method for feature selection process is used. The criterion which this method seeks to minimize over all feasible feature subsets is the misclassification rate for classification models. The SFS method starts with an empty candidate set and adds feature variables sequentially until addition of further variables does not decrease the criterion (minimization of misclassification).

4.3 Multi-Class SVM Based Classifier Design

After extracting the desired features by using sequential forward feature selection method, the final step is to design a classification function. The classifier represents the boundary between the separating classes. The design of the classifier is based on the design (training) set. There are many training algorithms like least squares, linear programming, *etc*. Although these existing algorithms, are less time consuming to use, they were found to have poor classification accuracy. The main requirements for a security function are high classification accuracy and less misclassification rate. Hence, a need arises to devise a more suitable learning algorithm. This led to the idea of applying a recently introduced machine learning tool called the Support Vector Machine (SVM) in the classification phase of the PR system. The following section gives a brief introduction to the Multi-Class SVM and the procedure to use for classification.

Overview of SVM

Sims is a learning systems designed to automatically trade off accuracy and complexity by minimizing an upper bound on generalization error. SVM is more suitable for classification problems, particularly those involving more than two classes. The SVM paradigm, originally designed for the binary classification problem, has a nice geometrical interpretation of discriminating one class from another by a hyper plane with the maximum margin (Abhisek 2007). SVM performs the job of classification by implementing a non-linear mapping of input vectors to a high dimensional feature space, where a linear decision surface is constructed.

This paper focuses on a static security evaluation problem, which in also this paper, is a multi-class PR problem. Due to various complexities, a direct solution of a multi-class problem using a single SVM formulation is usually avoided. The better approach is to use a combination of several binary SVM classifiers to solve a given multi-class problem. Popular methods are: one-versus-all method using a winner- takes-all strategy; one-versus-one method implemented by max-wins voting (Kai-Bo, Sathiya 2005). In this paper, the latter technique was used,presisely, the one-versus-one method for designing the multi-class SVM classifier. Each of the two methods is briefly discussed as follows:

A) One-Versus-All (OVA)

This is conceptually the simplest multi-class SVM classification method. It constructs k SVM models, class 1 (positive) versus all other classes (negative), class 2 versus all other classes, ... , class K versus all other classes, where K is number of classes (Chih, Chih-Jen 2003), A comparison of methods for multi-class support vector machines. Taiwan). Given a set of training data samples of length £ $(x_1 , y_1) , (x_2, y_2) , \ldots , (x_e, y_e)$; $x_i \varepsilon R^M$, where each training sample x_i has M features describing a particular signature and belongs to one of the K classes, *ie*., $y \in \{y_1, \ldots , y_K \}$. The basic concept behind SVM is to search for a balance between the regularization term $\frac{1}{2} (w_i)^T w_i$ and the training errors. Classification of new instances in the one-versus-all method is done by a winner-takes-all strategy, in which the classifier with the highest output function assigns the class. For a multi-class problem defining K classes, one needs to solve k quadratic programming (QP) optimization problems of size £. Hence, this approach is computationally expensive and not commonly preferred.

B) One-Versus-One (OVO)

This method constructs K (K - 1)/2 binary classifiers, where each one is trained on data from two classes. In other words, for every pair of class, a binary SVM problem is solved. The classification in one-versus-one method is done by a max-wins voting strategy

(MWV). After each of the K (K - 1)/2 binary classifiers make its vote, the decision function assigns an instance x to a class having largest number of votes (Kai-Bo, Sathiya 2005; Chih-Wei, Chin 2006). In this case, a tie occurs with two classes having identical votes, the one with smallest index is selected. One of the benefits of this approach is that for every pair of classes, a smaller optimization problem is dealt with, thereby resulting in saving of total computation time. Hence, if in an average, each class has £/K data points, only the K (K - 1)/2 Quadratic Programming (QP) problems of size less than £ have to be solved. This is found to be quite less compared to the OVA approach, where K number of QP problems, each of size £ needs to solved.

SVM Training Algorithm for Classification Task

The procedure or steps involved in applying SVM for the problem of multi-class classification is as follows:

1. Data Scaling/Preprocessing

The input features in train set and test set needs to be scaled properly before applying SVM. This is important as the kernel values depend on the inner products of the feature vector. Scaling prevents the domination of any feature over the other because of higher numeric values involved and also avoids numerical difficulties during calculation. It is recommended to linearly scale each attribute to the range of [0, 1].

2. Design of SVM Model

Choice of Kernel

The Radial Basis Function (RBF) kernel is the first choice because of its widely-known accuracy. Further, it is capable of handling non-linear relations existing between the class labels and input attributes. The second reason is that RBF kernel, unlike other kernels, has only one kernel parameter, thereby reducing the complexity of the model.

Adjusting the Kernel Parameters

There are two parameters associated with RBF kernels - the Penalty parameter, C the and RBF Kernel parameter, γ. The goal is to identify optimal (C, γ) for the classifier to accurately predict the unknown data (test data). This can be achieved by a technique called 'Cross-Validation'. In a v-fold cross validation, the whole training set is divided into v subsets of equal size. Sequentially one subset is tested using the classifier trained on the remaining (v-1) subsets. Thus, each instance of the train set is predicted once and the cross-validation accuracy is the percentage of data samples that are correctly classified (Min *et al*. 2005). In this study, a grid search is used on C and γ using 5-fold cross validation. All pairs of (C, γ) were tried and the one with highest cross- validation accuracy was selected. It was also realized that using exponentially growing sequences of C and γ is a practical method to identify optimal parameters. These sequence was used $C = \{2^{-5}, 2^{-3}, \ldots, 2^{15}\}$ and $\gamma = \{2^{-15}, 2^{-13}, \ldots, 2^{5}\}$ in the SVM experiment.

3. Training and Testing the SVM Model

After designing the SVM model with the chosen kernel and optimal parameters, it is trained with the scaled input-output train set data samples. Once the performance of the SVM classifier is found satisfactory in the training phase, the model is validated with test data samples to access its overall performance.

5. Performance Evaluation of the Classfier

The performance of the SVM classifier is validated by calculating the following performance measures for train set, test set and combined set (combination of train and test sets).

(1) Mean Squared Error (MSE)

$$MSE = \frac{1}{N} \sum_{k=1}^{N} (E_k)^2 \; ; E_k = \left| DO_k - AO_k \right| \tag{6}$$

N No. of data set samples

DO_k Desired Output obtained from off-line simulation

AO_k Actual Output obtained from SVM classifier model

(2) Classification Accuracy (CA)

$$CA(\%) = \frac{No.\ of\ samples\ classified\ correctly}{Total\ \ no.\ of\ samples\ in\ the\ data\ set}\ x\ 100 \tag{7}$$

(3) Misclassification (MC) Rate

$$MC(\%) = \frac{No.\ of\ misclassifications\ in\ class\ K}{Total\ \ No.\ of\ samples\ in\ class\ K}\ x\ 100 \tag{8}$$

In power system security evaluation, it is important to ensure that the misclassification rate is kept at minimal. In particular, the chances of a highly insecure state being wrongly predicted as secure, needs to be reduced, as it may be lead to failure of control actions and hence a severe 'blackout'. Thus, the classification system for security evaluation must be efficiently designed to have high classification accuracy and a low misclassification rate.

6. Simulation Results and Discussion

The proposed multi-class SVM based pattern recognition approach to static security evaluation is implemented on 57 Bus, 118 Bus and 300 Bus IEEE standard systems. The multi-class SVM classifier is designed and tested using LIBSVM software package (Cin-Chung, Chih-Jen 2004). Normally in power system networks, transmission lines are permitted to carry power to a maximum limit of 125% to 130% of scheduled value so as to meet the small increase in demand. This will not pose serious problems as the transmission line is normally designed to meet this requirement. However, the system losses will increase due to large the amount of heat dissipation involved. Based on this, the MVA limit of the lines and transformers is taken as 130% of the base case MVA flow in the simulation work. The security limit of voltage magnitude at load buses is imposed in the range of 0.90 pu to 1.10 pu.

6.1 Data Generation

Different scenarios have been considered by varying the system real power generation and load from 50% to 200% of base case values. The variation in real power generation is limited to its minimum and maximum values. Contingencies of single-line outages are simulated for each operating condition. For a given operating condition and specified contingency, a load flow solution by Fast Decoupled method is obtained and the Static Security Index as given by Eq. (5) is calculated. In the calculation of SSI, the weighting factors for LOI, VDI and GDI are assumed as $W_1 = 3$, $W_2 = 2$ and $W_3 = 1.5$ respectively. These weighting factors are fixed based on the order of priority in requirement of system security. SSI is a percentage measure of system security level, taking value in the range between 0 and 100. Based on the computed value of SSI, data patterns in each operating condition are categorized in one of the following four classes.

SSI = 0% Static Secure (Class A)
SSI>0% & SSI ≤5% Static Critically Secure (Class B)
SSI>5% & SSI ≤15% Static Insecure (Class C)
SSI>15% Static Highly Insecure (Class D)

6.2 Design of Multi-class SVM Model

The steady state variables obtained from load flow solution are recorded as pattern variables. The variables included in the pattern vector are bus voltage magnitude, bus voltage angle, complex power generation at generator buses, complex power load at load buses and MVA flow in all branches. The large size pattern vector is reduced by sequential forward approach of the feature selection. This selects the pattern variables having higher discriminating power and hence determines the feature vector, which is an optimal subset of pattern vector. The data samples in the feature vector are randomly split into two parts - train set and test set. The multi-class SVM classifier model is designed using the training data samples. The performance of SVM classifier depends on the type of kernel function and SVM parameters. The Radial Basis Function (RBF) was chosen as kernel function in our SVM experiment. The parameters of SVM model to be tuned are the Penalty parameter (C) and the RBF kernel parameter (γ). The optimal values of these parameters are obtained by a '5-fold Cross Validation' procedure for a cross-validation accuracy of 100%. The SVM model designed is validated by rating its performance, when subjected to randomly generated test set samples, whose class labels are unknown.

6.3 Test Case Results

Table 1 shows the results of data generation and feature selection of the PR system. The total number of operating scenarios simulated and number of cases belonging to each class is shown for the test cases studied. The number of feature variables extracted from the pattern vector, as seen from Table 1 is significantly less, as is evident from the figure of Dimensionality Reduction (defined as the ratio of number of components in the feature vector to that in the pattern vector). The SVM classifier is trained using the normalized values of selected features. The data samples in the feature vector are normalized to a range of [0, 1] using the min-max normalization method. It is the one of the widely used techniques for the data scaling process. It performs linear transformation on original data by scaling the data in each attribute to fit in a specific range.

Table 2 shows the results of classification in training, testing and combined phases for IEEE 57 Bus, 118 Bus and 300 Bus test systems. The results of SVM classifier is compared with Multilayer Perceptron (MLP) and Method of Least Squares (MLS) classifiers in terms of performance measures. The MLP network, designed and trained using the Neural Network toolbox in Matlab 7.6, consists of a hidden layer with the 30 neurons of 'tansig' transfer function. The network is trained with the Levenberg Marquardt algorithm (Learning rate = 0.05; Performance goal = 0.001; Epochs = 600). It can be easily seen from Table 2 that the SVM classifier gives a fairly high classification accuracy and a less misclassification rate, in particular for class K=4, compared to MLP and MLS classifiers. Furthermore, the time taken by the SVM algorithm is much compared to MLP network, even for a large size system. Figure 3(a) and 3(b) shows the cross validation plot of the

Table 1. Results of pattern generation and feature selection stages of PR system

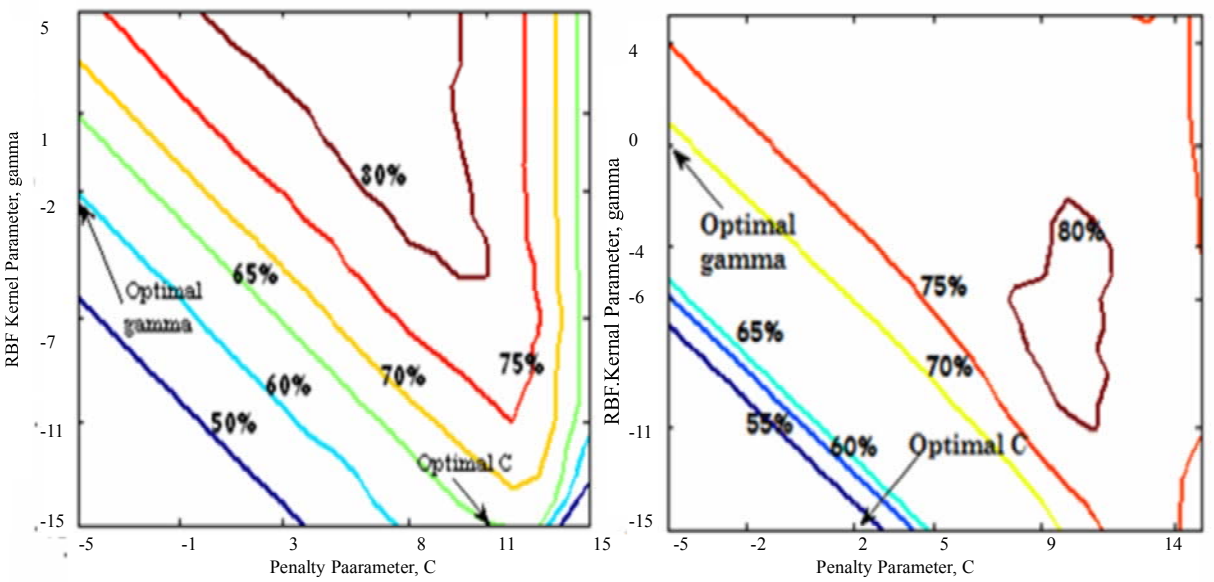
Case Studies →		IEEE 57 Bus	IEEE 118 Bus	IEEE 300 Bus
Operating Scenarios		1402	3537	5311
Static Secure (SS) cases		170	174	1089
Static Critically Secure (SCS) cases		672	2391	4141
Static Insecure (SI) cases		191	344	81
Static Highly Insecure (SHI) cases		369	628	0
Train Set	Static Secure (SS) cases	128	130	815
	Static Critically Secure (SCS) cases	503	1797	3104
	Static Insecure (SI) cases	138	254	64
	Static Highly Insecure (SHI) cases	282	471	0
	Total Train Samples	1051	2652	3983
Test Set	Static Secure (SS) cases	42	44	274
	Static Critically Secure (SCS) cases	169	594	1037
	Static Insecure (SI) cases	53	90	17
	Total Test Samples	87	157	0
No. of Components in Pattern Vector		351	885	1328
No. of Components in Feature Vector		243	568	1311
Dimensionality Reduction (%)		39	52	84
		16.05%	9.16%	6.41%

Table 2. Classification results on train, test and combined sets for multi-class SSA

		IEEE 57 Bus			IEEE 118 Bus			IEEE 300 Bus		
		SVM	MLS	MLP	SVM	MLS	MLP	SVM	MLS	MLP
Train Set	CA (%)	98.86	78.31	91.06	98.79	91.44	94.76	98.97	84.08	94.98
	MC (%) Class K=1	4.69	75.78	36.72	6.92	100.00	63.85	3.56	69.08	13.01
	MC (%) Class K=2	1.19	6.76	4.77	1.17	2.23	1.56	0.39	1.77	2.80
	MC (%) Class K=3	0.00	15.94	10.87	0.79	10.63	7.87	0.00	25.00	10.94
	MC (%) Class K=4	0.00	26.60	2.84	0.00	6.37	1.70	Not Applicable*		
Test Set	CA (%)	93.16	79.20	90.03	95.82	91.53	94.12	97.06	83.36	93.83
	MC (%) Class K=1	11.90	66.67	28.57	29.55	100.00	59.09	7.30	70.44	17.52
	MC (%) Class K=2	4.73	6.51	4.14	2.86	2.53	2.02	1.74	2.31	2.99
	MC (%) Class K=3	15.09	15.09	11.32	6.67	12.22	11.11	5.88	23.53	17.65
	MC (%) Class K=4	3.45	29.89	11.49	0.64	3.18	2.55	Not Applicable*		

* As there are no samples belonging to the class of Static Highly Insecure (Class K=4)

SVM classifier trained with the RBF kernel using 5-fold cross validation technique for the IEEE 57 bus and IEEE 300 bus systems respectively. The optimal values of SVM parameters obtained for a cross validation accuracy of 80%, as seen from Fig. 3(a) for IEEE 57 bus, are Penalty parameter, $C = 2^{11} =$



(a) IEEE 57 Bus Systesm (b) IEEE 300 Bus System

Figure 3. Selection of SVM parameters for multi-class SSA problem

2048 and RBF kernel parameter, $\gamma = 2^{-2} = 0.25$. The SVM parameters selected for the IEEE 300 bus for a cross validation accuracy of 80%, seen in Fig. 3(b), are Penalty parameter, $C = 2^2 = 4$ and RBF kernel parameter, $\gamma = 2^0 = 1.00$.

7. Conclusions

In this paper, the SVM based Pattern Recognition (SVM-PR) approach for static security evaluation in multi-class mode is presented. The proposed multi-class SVM-PR model was tested on IEEE standard test systems. Simulation results showed that high accuracy security functions are realizable with an SVM classifier. The SVM classifier also proved to give a lower misclassification rate compared to MLP or any equivalent methods. A good classification system should to reduce the chances of highly insecure states being erroneously predicted to almost zero (misclassification rate corresponding to Class K=4). This is achieved by the SVM classifier, thereby reducing the posibility of failure of the control actions. Future work will focus on the improvement of performance of the SVM classifier by adopting different methods for feature selection and SVM parameter tuning.

References

Abhisek U (2007), Intelligent systems and signal processing in power engineering. pringer-Verlag, Switzerland.

Arora CM, Surana SL (1996), Transient security evaluation and preventive control of power systems using PR techniques. IE (India) 76:199-203.

Azah MS, Maniruzzaman HA (2001), Static security assessment of a power system using genetic-based neural networks. Electric Power Components and Systems 29:1111-1121.

Boudour M, Hellal A (2006), Combined use of unsupervised and supervised learning for large scale power system static security assessment. Int. J. of Power & Energy Systems 26(2):157-163.

Chih-Chung C, Chih-Jen L (2001), LIBSVM: A library for support vector machines. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

Chih-Wei H, Chih-Jen L (2005), A comparison of methods for multi-class support vector machines. Taiwan (cjlin@csie.ntu.edu.tw).

Haghifam MR, Zebarjadi V (1996), 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 3:2009-2013.

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

http://www.pserc.cornell.edu/matpower (Matpower 3.2).

Huang SJ (2001), Static security assessment of a power system using query-based learning approaches with genetic enhancement. IEE Proceedings-Generation, Transmission & Distribution 148(4):319-325.

Kai-Bo D, Sathiya KS (2005), Which is the best multi-class SVM method? An empirical study. Springer-verlag, Berlin Heidelberg 278-285.

Laveen K (1974), Patterns in pattern recognition.

IEEE Transactions on Information Theory IT-20(6):697-722.

Lo KL, Peng LJ (1997), Design of artificial neural networks for on-line static security assessment problems. Proc. of the 4th Int. Conf. on APSCOM-97, Hong Kong 288-293.

Luan WP, Lo KL, Yu YX (2000), ANN based pattern recognition technique for power system security assessment. IEEE Int. Conf. on Electric Utility Deregulation, Restructuring and Power Technologies, London 197-202.

Min JHY, Chan L (2005), Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters. Expert Systems with Applications 28(5):603-614.

Pang CK, Kovio AJ, El-Abiad, AH (1973), Application of pattern recognition to steady state security evaluation in a power system. IEEE Transactions on Systems, Mans and Cybernetics SMC-3(6):622-631.

Pang CK, Prabhakara FS, El-Abiad AH, Koivo AJ (1974), Security evaluation in power systems using pattern recognition. IEEE Transactions on Power Apparatus & Systems PAS-93:969-976.

Pecas LJA, Machiel BFP, Marques DSJP (1988), On-line transient stability assessment and enhancement by pattern recognition techniques. Electrical Machines and Power Systems 25:293-310.

Sa DCJMG, Munro N (1984), Pattern recognition in power system security. Int. J. of Electrical Power & Energy Systems 6(1):31-36.

Saeh IS, Khairuddin A (2008), Static security assessment using artificial neural network. IEEE 2nd Int. Power & Energy Conference (PECon'08) 1172-1178.

Shahidehpour SM (2003), Communication and control in electric power systems. Wiley Interscience, John Wiley & Sons, Third Edition.

Siri W, Sharkawi MAEl (1992), Feature selection for static security assessment using neural networks. IEEE Int. Symposium on Circuits & Systems, San Diego, California 10-13:1693-1696.

Swarup KS, Corthis BP (2006), Power system static security assessment using self-organizing neural network. J. of Indian Institute of Science 86(4):327-342.