International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:4, 2009

Power System Security Assessment using Binary SVM Based Pattern Recognition

S Kalyani, *Member, IEEE,* and K Shanti Swarup, *Senior Member, IEEE*

Abstract—Power System Security is a major concern in real time operation. Conventional method of security evaluation consists of performing continuous load flow and transient stability studies by simulation program. This is highly time consuming and infeasible for on-line application. Pattern Recognition (PR) is a promising tool for on-line security evaluation. This paper proposes a Support Vector Machine (SVM) based binary classification for static and transient security evaluation. The proposed SVM based PR approach is implemented on New England 39 Bus and IEEE 57 Bus systems. The simulation results of SVM classifier is compared with the other classifier algorithms like Method of Least Squares (MLS), Multi-Layer Perceptron (MLP) and Linear Discriminant Analysis (LDA) classifiers.

Keywords—Static Security, Transient Security, Pattern Recognition, Classifier, Support Vector Machine.

I. Introduction

SECURITY evaluation is an important issue in planning and operation stages of an electric power system. The present trend toward deregulation has forced modern electric utilities to operate the systems under stressed operating conditions closer to their security limits. Under such fragile conditions, any disturbance could endanger system security and may lead to system collapse. Therefore, there is a pressing need to develop fast on-line security monitoring method, which could analyze the level of security and forewarn system operators to take necessary preventive actions in case need arises [1]. Power System Security is defined as the ability of the system to withstand unexpected failures and continue to operate without interruption of supply to consumers [2].

One of the challenging problems in the real-time operation of power system is security assessment. 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 the transient behavior and other time dependent variations. Transient Security Analysis evaluates the performance of the system as it progresses after a disturbance. Analysis of rotor angle stability is an essential component in TSA [3]. Any on-line TSA tool must provide a fast stability evaluation and system security analysis under perturbations.

This paper presents a Support Vector Machine (SVM) based approach for on-line security evaluation. One of the important consideration in applying SVM to power system security evaluation is the proper selection of training feature set, characterizing the behavior of the power system. Many feature selection algorithms are available in the literature such as fisher discrimination analysis, entropy maximization, fisher discrimination [4]. The main problem with the existing feature algorithms is that it works well with linearly separable classes, but not well established on non-linearly separable classes [5]. In this paper, feature selection is performed by a simple approach called Sequential Forward Selection (SFS) method.

Power system security evaluation is a complex non-linear problem, which has non-linear separability between secure and insecure classes. Literatures have reported the use of conventional algorithms like linear programming, least squares [6], decision trees [7] and different artificial neural network architectures [8] for design of classifier. To handle the problem of non-linear separability, SVM technique is adopted in the classification phase of the Pattern Recognition system. Furthermore, in this paper, the logic of binary security assessment is considered, i.e., a given operating condition is deemed as either secure (1) or insecure (0). An operator likes to know exactly the disturbances that could cause insecurity and abnormality resulting from each disturbance for a given system operating condition, rather than its degree of security. The proposed SVM based classification approach is implemented on New England 39 bus and IEEE 57 bus systems. The simulation results prove that SVM classifier gives a better classification, enhancing its suitability for on-line security evaluation.

II. Power System Security

The term 'Security' as defined by NERC (1997) is the ability of the electric systems to withstand sudden disturbances such as electric short-circuits or unanticipated loss of system element [9]. The main goal in security analysis is to increase the power system's ability to run safely and operate within acceptable economic bounds. A set of most probable contingencies is first specified for security evaluation. This set may include outage of a line/generator, sudden increase in load, three phase fault in the system, etc [10].

A. Static Security Assessment

Static security (also referred to as steady state security) is the ability of a power system to reach a steady state operating point without violating system operating constraints [11]. The violations of thermal limits of transmission lines and bus voltage limits are main concern for static security analysis. Under normal operating conditions, the following constraints

S. Kalyani is with the Department of Electrical Engineering, Indian Institute of Technology, Madras, Chennai-600036. She is on deputation from K.L.N College of Engineering, Pottapalayam, Sivagangai, Tamilnadu to pursue Ph.D programme at IIT Madras (e-mail: kal_yani_79@yahoo.co.in).

K. Shanti Swarup is working as Professor in the Department of Electrical Engineering, Indian Institute of Technology, Madras, Chennai - 600036. (e-mail: swarup@ee.iitm.ac.in).

must be satisfied:

$$\sum_{i=1}^{N_g} P_{Gi} = P_D + P_{loss} \; ; \; P_{Gi}^{min} \leq P_{Gi} \leq P_{Gi}^{max} \quad (1)$$

$$\left|V_k^{min}\right| \leq |V_k| \leq |V_k^{max}| \; ; \; S_{km} \leq S_{km}^{max} \; \forall \; branch \; k-m \quad (2)$$

where P_{Gi} represents real power generation at i^{th} bus, P_D is the total system demand; P_{loss} is the total real power loss in the transmission network; $|V_k|$ is the voltage magnitude at k^{th} bus; S_{km} represents MVA flow in branch k-m; N_g is the number of generators. Constraints (1) and (2), when referred to the post contingency scenarios, are referred to as Security Constraints [12]. If any of the constraint violates, the system may experience disruption resulting in a **'severe black out'**.

B. Transient Security Assessment

Transient security is the ability of a power system to operate consistently within the limits imposed by system stability phenomena [11]. One of the primary requirements of reliable service in electric power systems is to retain the synchronous machines running in parallel with adequate capacity to meet the load. Transient security assessment consists of determining, whether the system oscillations, following the occurrence of a fault or a large disturbance, will cause loss of synchronism among system generators [13].

Transient security assessment is a subset of transient stability of the power system. Transient stability pertains to rotor angle stability, where the stability phenomena are characterized by the rotor oscillations under a severe perturbation. The goal of TSA is to solve non-linear dynamic equations describing the transient behavior of the system under a set of credible contingencies. In this paper, generators are represented by simple classical model and rotor dynamics of the system is studied.

III. SVM Based Pattern Recognition (SVM-PR) Approach for Security Assessment Problem

A security system designed should be accurate, consistent, quick, easy to implement, adaptable to system changes, able to provide results which can be easily interpreted and of reasonable cost. The main objective of applying pattern recognition is to reduce the on-line computational requirements.

A. Pattern Recognition (PR) Approach

Pattern Recognition is defined as 'the act of taking in raw data and taking an action based on the category of data'. The patterns to be classified are usually groups of measurements or observations, defining points in a multidimensional space. The basic components of a pattern recognition system are preprocessing, feature selection and classifier design [14]. The role of preprocessing is to define a compact representation of the pattern. The goal of feature selection is to select the optimal feature subsets by computing numeric information from observations. After the optimal feature subset is selected, a classifier is designed relying on the selected features.

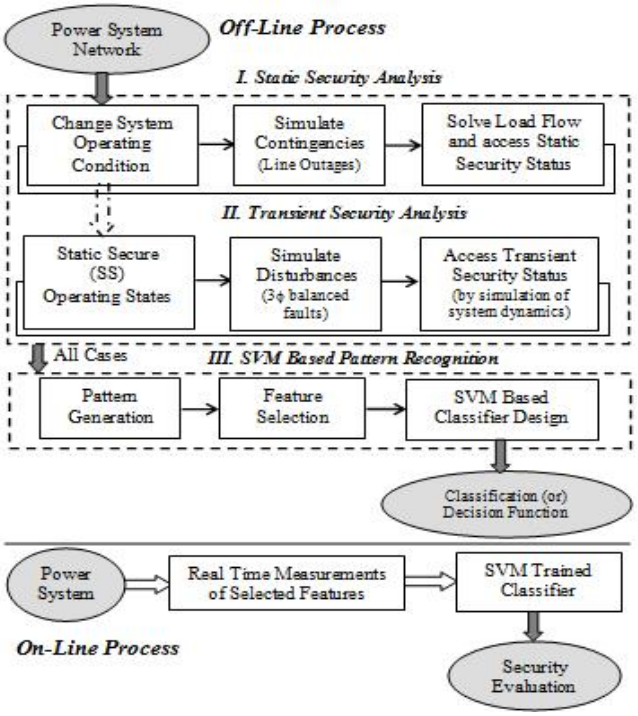

Fig. 1. Design and Implementation of SVM Based PR System for Static and Transient Security Evaluation

In the design of Pattern Recognition (PR) system, a bulk amount of work is done in off-line to generate a set of characteristic operating points called 'training set' necessary to design a security function. If the equation governing the surface separating the secure and insecure classes is evaluated as a security function, system security can be accessed at any time. This is the basic idea behind pattern recognition approach. The sequence of processes carried out in the off-line and on-line modes in applying the proposed SVM based Pattern Recognition approach to security evaluation process is shown in Fig. 1.

The success of pattern recognition system relies on good training set. The patterns needed for training and testing may be generated by real time occurrences or from off-line simulations [15]. In this paper work, we have generated sufficient data samples through off-line simulation studies. The number of variables in the pattern vector is sufficiently large and hence needs to be reduced for ease of classifier design. A suitable feature selection is identified to select the optimal input features for classification. In this paper, we have used a 'Sequential Forward Selection' (SFS) method for the feature selection process. The SFS method starts with an empty candidate set and adds feature variables sequentially until addition of further variables does not decrease the criterion. The criterion which this method uses is minimization of misclassification rate for classification models.

B. Binary SVM Based Classifier Design

After selecting the desired features by SFS method, the next step is to design a decision function or classifier based on the train set. There are many training algorithms like least

squares, back propagation, linear programming, etc available to design the classifier [6-8]. The existing training algorithms, although less time consuming, have certain limitations like poor classification accuracy and poor performance with larger size problems. This led to the thought of applying a more efficient training procedure for the problem. Therefore, in this paper, we propose the application of a recently introduced machine learning tool, namely, Support Vector Machine (SVM) for classifying the power system security status.

Overview of SVM

Support Vector Machine (SVM) is a relatively new method for learning separating functions in pattern recognition (classification) problem [16]. SVM classifier minimizes the generalization error by optimizing the trade-off between the number of training errors and the so-called Vapnik-Chervonenkis (VC) dimension, a new concept of complexity measure [17]. 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.

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. Consider a training set $T = \{x_i, y_i\}$, where x_i 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 employed for such two class problem is illustrated in Fig. 2. The hyperplane (dotted line) 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).

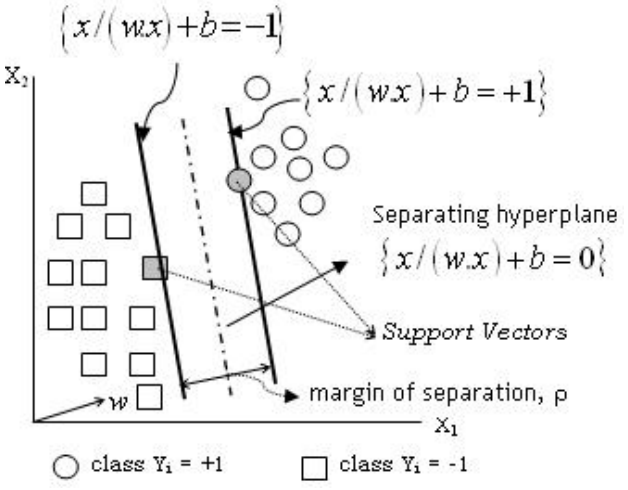

Fig. 2. Illustration of Optimal Hyperplane SVM Classifier

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

$$Min_{w,b,\xi} \frac{1}{2} w^T w + C \sum_{i=1}^{N} \xi_i \quad (3)$$

subject to the constraints

$$y_i \left(w^T \phi(x_i) + b\right) \geq 1 - \xi_i \; ; \; \xi_i \geq 0, \; i = 1, 2 \ldots N \quad (4)$$

where w is the weight vector of the hyperplane, C is the penalty parameter proportional to the amount of the constraint violation, ξ_i is the slack variable, $\phi(.)$ is a mapping function called 'kernel' function and b is the threshold. The kernel function maps the data in the input space to feature space where they are linearly separable. The concept of kernel mapping allows the SVM models to perform separations even with very complex boundaries. Many kernel mapping functions are available. The Radial Basis Function (RBF) kernel is the most commonly used kernel mapping function in most of the SVM models [16]. In this paper, we have used RBF kernel function in the design of SVM model.

SVM Training Algorithm for Classification Task

The procedure or steps involved in applying SVM for classification problem is discussed herein.

Data Scaling

The data samples in train and test set needs to be scaled properly before applying SVM. This is important 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.

SVM Model Selection

Choice of Kernel

The RBF kernel is chosen as a first choice because of its wide known accuracy. It is capable of handling non-linear relation existing between class labels and input attributes. Moreover, RBF kernel has only one tuning parameter, thereby reducing the complexity of model selection.

Adjusting the Kernel Parameters

With the use of RBF kernel, there are two parameters associated with SVM model, viz., Penalty parameter, C and RBF kernel parameter, γ. The goal is to identify optimal (C, γ) so that the classifier can accurately predict the unknown data. This can be achieved by a technique called 'Cross-Validation'. In a v-fold cross validation, we divide the whole training set 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 that are correctly classified [18]. This cross-validation procedure can prevent the over fitting problem. In this study, we use a grid search on C and γ using 5-fold cross validation. All pairs of (C, γ) was tried and the one with the highest cross-validation accuracy was selected as optimal values of SVM parameters. We have used the sequence $C = \{2^{-5}, 2^{-3}, \ldots, 2^{15}\}$ and $\gamma = \{2^{-15}, 2^{-13}, \ldots, 2^{5}\}$ in the SVM experiment.

Training and Testing the SVM Model

The SVM is trained using the chosen kernel with optimal parameters and the scaled input and output data. After training the SVM, the model is tested with the test samples generated.

IV. Performance Evaluation of Classifier

The performance of SVM classifier model designed is gauged by calculating the following performances measures for train set and test set separately.

(a) *Mean Squared Error (MSE)*

$$MSE = \frac{1}{N}\sum_{k=1}^{N}(E_k)^2 \; ; \; E_k = |DO_k - AO_k| \quad (5)$$

N No. of samples in the data set
DO_k Desired Output obtained from off-line simulation
AO_k Actual Output obtained from SVM classifier model

(b) *Classification Accuracy (CA)*

$$CA\,(\%) = \frac{No.\ of\ samples\ classified\ correctly}{Total\ No.\ of\ samples\ in\ data\ set} \times 100 \quad (6)$$

(c) *Misclassification (MC) Rate*

(i) Secure Misclassification(SMC) / False Dismissal

$$SMC\,(\%) = \frac{No.\ of\ 0's\ classified\ as\ 1}{Total\ No.\ of\ Insecure\ States} \times 100 \quad (7)$$

(ii) Insecure Misclassification(ISMC) / False Alarm

$$ISMC\,(\%) = \frac{No.\ of\ 1's\ classified\ as\ 0}{Total\ No.\ of\ Secure\ States} \times 100 \quad (8)$$

In power system security evaluation, the false alarms do not bring any harm to power system operation. False dismissals, on the other hand, makes the system operation becomes unknown, leading to failure of control actions and hence 'system blackout' [12]. It is, therefore, important to ensure that the false dismissals are kept at minimal. The classification system must be efficiently designed to meet this requirement.

V. Simulation Results and Discussion

The proposed SVM based Pattern Recognition (SVM-PR) approach is implemented in 39 Bus New England and 57 Bus IEEE standard systems [19-20]. The machine data of test cases are shown in Appendix. An acceptable limit of 0.90 p.u.-1.10 p.u. is assumed for the bus voltage magnitude. The MVA limit of transmission lines and transformers is taken as 130% of base case MVA flow. Simulation programs are developed in MATLAB 7.0 package running on a Pentium IV 2.4 GHz with Windows XP operating system. The design and testing of SVM model is done using LIBSVM tool [21]. Different operating states are considered by varying the total real power load and generation of the system from 50% to 200% of their base values. The variation in generation is limited to its minimum and maximum values in each scenario considered.

A. Results of Static Security Assessment (SSA)

The process of static security assessment considers single line outages as contingencies for each operating scenario. For each operating scenario and specified contingency, Load Flow (LF) solution by Fast Decoupled method is obtained and the static security status is accessed by evaluating the security constraints, given by equations (1)-(2). The system variables obtained from LF solver are recorded as pattern variables, which includes voltage magnitude and angle at buses, complex generation at generator buses, complex load at load buses and MVA flow in all branches. Each pattern vector is labeled as belonging to secure/insecure class, based on its security status. An optimal subset of pattern vector called feature vector is identified by SFS method. The number of data patterns generated pertaining to the two classes and number of features selected for classification are shown in Table I.

TABLE I
Pattern Generation and Feature Selection for SSA

Case Study ⟶	**NE 39 Bus**	**IEEE 57 Bus**
Operating Scenarios	**531**	**1378**
Secure Classes	74	156
Insecure Classes	457	1222
No. of Train Samples	**481**	**1241**
No. of Test Samples	**50**	**137**
No. of Pattern Variables	153	243
No. of Features Selected	13	21
Dimensionality Reduction	**8.497%**	**8.640%**

The data samples in the feature vector are randomly split into train (90%) and test (10%) sets. The SVM classifier is designed based on train set. Table II (a) and (b) shows the results of classification for static security assessment problem obtained for New England 39 bus and IEEE 57 bus systems respectively. The performance measures of SVM classifier are compared with other classifiers like MLS, MLP and LDA.

TABLE II
Performance Evaluation of Classifiers for SSA

(a) Test Case 1: New England 39 Bus System

Classifier ⟶		SVM	MLP	MLS	LDA
Train Set	CA (%)	**97.297**	33.264	57.381	65.073
	MSE	0.0270	0.6674	0.4264	0.3493
	SMC (%)	**0.4878** (2/410)	78.293 (321/410)	49.512 (203/410)	38.781 (59/410)
	ISMC (%)	15.943 (15/71)	0.000 (0/71)	2.8169 (2/71)	12.676 (9/71)
	Time (s)	0.0246	0.3192	3.4493	0.4259
Test Set	CA (%)	**94.000**	18.000	42.000	60.000
	MSE	0.0600	0.8200	0.5800	0.4000
	SMC (%)	**0.0000** (0/47)	87.231 (41/47)	59.575 (28/47)	42.553 (20/47)
	ISMC (%)	100.00 (3/3)	0.000 (0/3)	33.333 (1/3)	0.0000 (0/3)
	Time (s)	0.0042	0.0005	0.0231	0.0458

The MLS classifier is defined by a function, $S(z) = [w]^T \times$

$[z]+w_0$, with weights, w, trained by multiple linear regression analysis. In MLS classifier, data patterns with $S(z) > 0$ are labeled as Secure (0) and those with $S(z) \leq 0$ are labeled as Insecure (1). The MLP network for classification is designed and trained using Neural Network toolbox in MATLAB 7.0. The MLP network consists of 30 hidden neurons (selected after repeated experiment trials) of 'tansig' function and the output layer uses 'hardlim' function to limit the classifier's output to a logical value of 0/1. Levenberg Marquardt (Learning Rate = 0.05, Goal = 0.001, Epochs = 600) is the back propagation training algorithm used. The LDA classifier is a machine learning method, closely related to regression analysis. Unlike regression analysis, LDA outputs a categorical or logical variable, defining the class to which the data sample belongs. The LDA classifier uses linear combination of selected features to define separating classes.

(b) Test Case 2: IEEE 57 Bus System

Classifier ⟶		SVM	MLP	MLS	LDA
Train Set	CA (%)	**99.597**	33.763	45.286	68.251
	MSE	0.0040	0.6624	0.5471	0.3175
	SMC (%)	**0.3646** (4/1097)	74.932 (822/1097)	61.896 (679/1097)	35.278 (387/1097)
	ISMC (%)	0.6944 (1/144)	0.0000 (0/144)	0.0000 (0/144)	4.8611 (7/144)
	Time (s)	0.1216	0.6219	21.836	1.0988
Test Set	CA (%)	**95.620**	24.818	27.007	64.234
	MSE	0.0438	0.7518	0.7299	0.3577
	SMC (%)	**4.800** (6/125)	82.400 (103/125)	80.00 (100/125)	39.200 (49/125)
	ISMC (%)	0.000 (0/12)	0.000 (0/12)	0.000 (0/12)	0.000 (0/12)
	Time (s)	0.0056	0.0013	0.0316	0.0528

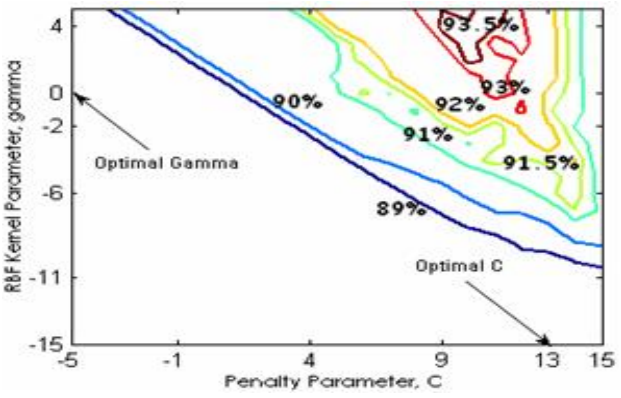

Fig. 3. Selection of SVM Parameters for SSA (IEEE 57 Bus)

The classification results in Table II shows that SVM classifier gives high classification accuracy and less false dismissals, nearing zero, compared to the other classifiers. Further, the SVM classifier, compared to other equivalent classifier algorithms, proves to give better performance for test set samples, whose class labels are unknown. Fig. 3 shows the cross validation plot used in selecting optimal values of SVM parameters for IEEE 57 bus system. This is the contour plot showing cross validation accuracy as contour heights for various values of SVM parameters. The values of SVM parameters for a cross validation accuracy of 93% (maximum arrived) are $C = 2^{13} = 8192$ and $\gamma = 2^0 = 1.00$.

B. Results of Transient Security Assessment

The process of transient security assessment starts by first evaluating static security status for each operating scenario considered by running LF program. All static secure cases are identified and subjected to transient security check, by simulating transient disturbances (three phase faults) on all lines, one at a time. The fault application time (t_a) and fault clearing time (t_c) are taken as 0 sec and 0.25 sec respectively, with system frequency as 60Hz. The transient stability program solves the system non-linear dynamic equations by the 4th order Runge-Kutta method. A simple classical model of generators is adopted. For any specified disturbance and operating condition, if the relative rotor angle of any generator with respect to slack generator does not exceed 180^0, the corresponding data pattern is labeled as Transient Secure (TS), else classified as Transient Insecure (TI).

TABLE III
PATTERN GENERATION AND FEATURE SELECTION OF TSA

Case Study ⟶		**NE 39 Bus**	**IEEE 57 Bus**
SSA	*Operating Scenarios*	**31**	**25**
	Static Secure (SS) Cases	13	14
	Static Insecure (SI) Cases	18	11
TSA	*Operating Scenarios*	**884**	**1764**
	Transient Secure (TS) Cases	602	1072
	Transient Insecure (TI) Cases	282	692
No. of Train Samples		**783**	**1589**
No. of Test Samples		**101**	**175**
No. of Pattern Variables		157	198
No. of Features Selected		25	7
Dimensionality Reduction		**15.92%**	**3.54%**

The variables included in the pattern vector comprises of steady state variables (bus voltage magnitude and angle, complex power generation and load) and dynamic variables (mechanical input power, electrical power output and relative rotor angle at fault application time, t_a and fault clearing instant, t_c) pertaining to the system transient behavior. The pattern vector size being large, we identify an optimal subset comprising of variables with high discriminating power by SFS feature selection method. The variables selected called features serve as the input database for the design of classifier. About 90% of data samples are used in train set and remaining 10% in test set. The results of data generation and feature selection phases of the pattern recognition system are shown in Table III.

The performance of classifiers obtained during training and testing phases are shown in Table IV (a) and (b) for NE 39 bus and IEEE 57 bus systems respectively. Like static

TABLE IV
PERFORMANCE EVALUATION OF CLASSIFIERS FOR TSA

(a) Test Case 1: New England 39 Bus System

Classifier ⟶		SVM	MLP	MLS	LDA
Train Set	CA (%)	**99.106**	73.180	72.542	95.913
	MSE	0.0089	0.2682	0.2746	0.0409
	SMC (%)	**1.9011** (5/263)	79.848 (210/263)	81.749 (215/263)	7.6051 (20/263)
	ISMC (%)	0.3846 (2/520)	0.000 (0/520)	0.000 (0/520)	2.3077 (12/520)
	Time (s)	0.0813	0.5714	22.187	0.8689
Test Set	CA (%)	**100.00**	99.009	90.099	99.009
	MSE	0.0000	0.0099	0.0990	0.0099
	SMC (%)	**0.0000** (0/19)	5.2632 (1/19)	52.632 (10/19)	5.2632 (1/19)
	ISMC (%)	0.000 (0/82)	0.000 (0/82)	0.000 (0/82)	0.0000 (0/82)
	Time (s)	0.0425	0.0010	0.0306	0.0695

(b) Test Case 2: IEEE 57 Bus System

Classifier ⟶		SVM	MLP	MLS	LDA
Train Set	CA (%)	**99.748**	71.554	79.421	94.965
	MSE	0.0025	0.2845	0.2058	0.0503
	SMC (%)	**0.6126** (4/653)	69.219 (452/653)	50.077 (327/653)	11.945 (78/653)
	ISMC (%)	0.000 (0/936)	0.000 (0/936)	0.000 (0/936)	0.2317 (2/936)
	Time (s)	0.0656	0.3531	17.485	0.5726
Test Set	CA (%)	**99.429**	77.714	86.286	91.429
	MSE	0.0057	0.2229	0.1371	0.0857
	SMC (%)	**2.5461** (1/39)	100.0 (39/39)	61.538 (24/39)	38.462 (15/39)
	ISMC (%)	0.000 (0/136)	0.000 (0/136)	0.000 (0/136)	0.000 (0/136)
	Time (s)	0.0050	0.0016	0.0263	0.0495

security assessment problem, the classification results of SVM model prove to be quite encouraging for transient security assessment problem also. The high classification accuracy and less false dismissal (SMC) rate makes the SVM classifier suitable for application in on-line security monitoring system. Although time taken by SVM classifier during testing phase is not comparably less compared to MLS, it is of a less significant figure, meaning that the system security status for any future operating condition can be accessed in few seconds without involving much computation. Fig. 4 shows the cross validation plot of the SVM classifier trained with RBF kernel for New England 39 bus system. The optimal values of SVM parameters are $C = 2^{15} = 32768$, $\gamma = 2^{-7} = 0.007813$.

VI. CONCLUSIONS

This work presented the use of Support Vector Machines (SVM) for security assessment by classifying the system state as secure or insecure considering a wide range of system operating scenarios and credible list of contingencies. The application of pattern recognition has proved to reduce the on-line computational requirement. The proposed Binary SVM based Pattern Recognition approach was implemented in standard test systems for both static and transient security evaluation. Simulation results show that the SVM classifier well fits the task of classification, independent of the system size. High accuracy classifiers are realizable with SVM algorithm, making it feasible for on-line implementation. Further, the SVM classifier gives less false dismissals (SMC) compared to MLP or any other equivalent classifier algorithm, thereby reducing the chances of failure of control actions. Future work will focus on the application of Multi-class SVM approach for real time security assessment and classification.

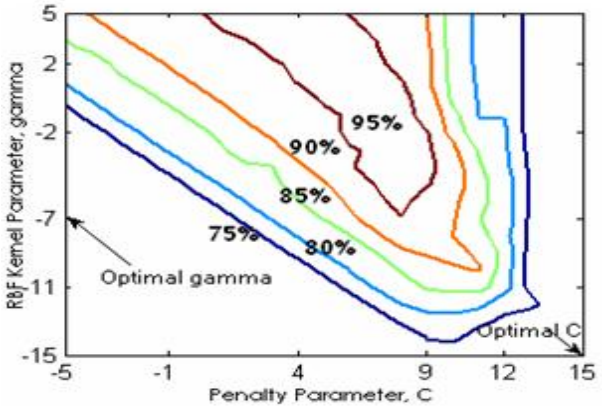

Fig. 4. Selection of SVM Parameters for TSA (NE 39 Bus)

APPENDIX A
GENERATOR DATA OF TEST SYSTEMS

Test Case 1: New England 39 Bus System

Gen No	Bus No	P_{min} (MW)	P_{max} (MW)	R_a (pu)	X'_d (pu)	H (sec)
1	30	0	350.00	0.0000	0.0310	42.00
2	31	0	1150.00	0.0000	0.0697	30.30
3	32	0	750.00	0.0000	0.0531	35.80
4	33	0	732.00	0.0000	0.0436	28.60
5	34	0	608.00	0.0000	0.1320	26.00
6	35	0	750.00	0.0000	0.0500	34.80
7	36	0	660.00	0.0000	0.0490	26.40
8	37	0	640.00	0.0000	0.0570	24.30
9	38	0	930.00	0.0000	0.0570	34.50
10	39	0	1100.00	0.0000	0.0060	500.00

Test Case 2: IEEE 57 Bus System

Gen No	Bus No	P_{min} (MW)	P_{max} (MW)	R_a (pu)	X'_d (pu)	H (sec)
1	1	0	575.88	0.0000	0.2500	4.000
2	2	0	100.00	0.0000	0.2000	3.000
3	3	0	140.00	0.0000	0.2000	3.000
4	6	0	100.00	0.0000	0.2500	5.000
5	8	0	550.00	0.0000	0.2000	2.500
6	9	0	100.00	0.0000	0.2000	3.000
7	12	0	410.00	0.0000	0.2500	5.000

ACKNOWLEDGMENT

The first author would like to thank the Management of K.L.N. College of Engineering, Pottapalayam for having given an opportunity for pursuing PhD in Indian Institute of Technology Madras under sponsorship category. The authors also like to thank IIT Madras for providing necessary facilities and resources for this research work.

REFERENCES

[1] 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, Issues 2-3, May 2004, pp.161-167.
[2] Daniel S. Kirschen, "Power System Security", *Power Engineering Journal*, October 2002, pp. 241-248.
[3] Prabha Kundur, John Paserba, Venkat Ajjarapu, Goran Anderson, Anjan Bose, Claudio Canizares, Nikos Hatziargyriou, David Hill, Alex Stankovic, Carson Taylor, Th.Van Cutsem, Vijay Vittal, "Definition and Classification of Power System Stability", *IEEE Transactions on Power Systems*, Vol. 19, No. 2, May 2004, pp. 1387-1401.
[4] Craig A.Jensen, Mohamed A.El.Sharkawi, Robert J.Marks, "Power System Security Assessment using Neural Networks: Feature Selection using Fisher Discrimination", *IEEE Transactions on Power Systems*, Vol. 16, No. 4, Nov 2001, pp.757-763.
[5] Sa Da Costa, N.Munro, "Pattern Recognition in Power System Security", *International Journal of Electrical Power & Energy Systems*, Vol. 6, No. 1, Jan 1984, pp. 31-36.
[6] C.K. Pang, F.S. Prabhakara, Ahmed H. El-Abiad, A.J. Koivo, "Security Evaluation in Power Systems using Pattern Recognition", *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-93, May/June 1974, pp. 969-976.
[7] I.S.Saeh, A.Khairuddin, "Decision Tree for Static Security Assessment and Classification", *International Conference on Future Computer and Communication (ICFCC)*, 2009, pp.681-684.
[8] I.S.Saeh, A.Khairuddin, "Static Security Assessment using Artificial Neural Network", *IEEE 2nd International Conference on Power & Energy (PECon 2008)*, 2008, pp.1172-1178.
[9] Leonard L.Grigsby, "Power System Stability and Control", *Electric Power Engineering Handbook*, Second Edition, CRC Press, 2007.
[10] Chok K.Pang, Antti J.Kovio, Ahmed H.El.Abiad, "Application of Pattern Recognition to Steady State Security Evaluation in a Power System", *IEEE Transactions on Systems, Mans & Cybernetics*, Vol. SMC-3, No. 6, Nov 1973, pp. 622-631.
[11] M. Shahidehpour, "Communication and Control in Electric Power Systems", *Wiley Interscience*, John Wiley & Sons, 2003, pp. 265-270.
[12] J.C.S.Souza, M.B.Do Coutto, M.Th.Schilling, "Fast Contingency Selection through a Pattern Analysis approach", *Electric Power Systems Research*, Vol. 62, Issue 1, May 2002, pp. 13-19.
[13] Hossein Hakim, "Application of Pattern Recognition in Transient Security Assessment", *Electric Power Components and Systems*, Vol. 20, Issue 1, January 1992, pp. 1-15.
[14] D. Duttam, "Trends in Pattern Recognition and Machine Learning", *Defence Science Journal*, Vol. 35, No. 3, July 1985, pp. 327-351.
[15] Se-Young Oh, "Pattern Recognition and Associative Memory Approach to Power System Security Assessment", *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-16, No. 1, Jan/Feb 1986, pp. 62-72.
[16] Abhisek Ukil, "Intelligent Systems and Signal Processing in Power Engineering", '*Springer-Verlag*, 2007.
[17] L.S.Moulin, A.P.Alves Da Silva, M.A.El-Sharkawi, Robert J. Marks, "Support Vector Machines for Transient Stability Analysis of Large-Scale Power Systems", *IEEE Transactions on Power Systems*, Vol. 19, No. 2, May 2004, pp. 818-825.
[18] Jae H.Min, Young-Chan Lee, "Bankruptcy Prediction using Support Vector Machine with Optimal Choice of Kernel Function Parameters", *Expert Systems with Application*, Vol. 28, Issue 5, 2005, pp. 603-614.
[19] M.A.Pai, "Computer Techniques in Power System Analysis", *Tata McGraw Hill*, Second Edition, 1979.
[20] http:// www.pserc.cornell.edu/matpower
[21] Chin-Chung Chang, Chih-Jen Lin, "LIBSVM: A Library for Support Vector Machines", Software available at www.csie.ntu.edu.tw / cjlin/.

S. Kalyani received her Bachelors Degree in Electrical and Electronics Engineering from Alagappa Chettiar College of Engineering Karaikudi, in the year 2000 and Masters in Power Systems Engineering from Thiagarajar College of Engineering, Madurai in December 2002. From 2003 to 2007, she was a faculty member with the Department of Elecrical and Electronics Engineering, KLN College of Engineering, Madurai, India. She is currently a Research Scholar in Dept. of Electrical Engineering, Indian Institute of Technology Madras. Her research interests are power system stability, Pattern Recognition, Neural Networks and Fuzzy Logic applications to Power System studies. She is a Member of IEEE since June 2009.

K. Shanti Swarup (S'87-M'92-SM'03) is currently a Professor in the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India. Prior to his current position, he held positions at Mitsubishi Electric Corporation, Osaka, Japan, and Kitami Institute of Technology, Hokkaido, Japan, as a Visiting Research Scientist and a Visiting Professor, respectively, during 1992 to 1999. His areas of research are artificial intelligence, knowledge-based systems, computational intelligence, soft computing, and object oriented modeling and design of electric power systems. He is a Senior Member of IEEE since 2003.