2

STATIC SECURITY ASSESSMENT USING BINARY-CLASS SUPPORT VECTOR MACHINE

Astik Dhandhia, Vivek Pandya and Siddharth Joshi

ABSTRACT: In the present day due to the increase of load demands day by day, Power system becomes complex, and it is operating near its bus voltage regulation limits and thermal capacity limits of the lines. So, it is vital to maintaining power system security for every possible operating condition including contingencies. The traditional method of static security assessment using load flow requires long computation time and complex calculations. This paper presents a Support Vector Machine based Binary-classifier for static security assessment of the power system. The proposed classifier classifies power system operating condition into secure and insecure, based on the computation of the Composite Security Index (CSI). Thermal limit of the transmission lines is chosen on the base of load ability limit of the short, medium and long transmission line. Single ranking and Correlation Coefficient Method is used for feature selection. The proposed approach is implemented, and classification accuracy is verified on IEEE 14 and 30 bus systems.

KEYWORDS

Static Security, Support Vector Machine, Feature Selection, Composite Security Index

1. INTRODUCTION

Power system mainly deals with generation, transmission, and distribution of electrical power. Due to increasing of day to day requirement of power one has to increase generation of electrical power. At the same time, there is a need for enough structure for distribution and transmission networks. All generating stations, transmission lines, and distribution lines are working in overloaded condition due to limited structure and limited sources of electrical power generation. Power system security includes the process of keeping the system operating when disturbances occur in the power system. Disturbances in the power system are due to outages of transmission lines, Generators, and Transformers, etc.

Power system security analysis is carried out in control center, and it is divided into mainly three categories, viz., power system monitoring, contingency analysis, and security constrained optimal power flow (Wood&Wollenberg, 2012). A power system security assessment is the steps performed to determine whether the system is safe from serious outages and to what extent it is safe in its operation (Kalyani&Swarup, 2009).

The concepts of power system security and stability are interrelated in power systems. There are three modes of the stability on operational point of view, viz., steady-state stability, which is related to the system steady-state condition following any small disturbance, transient stability, which discusses with the capacity of the system to remain in synchronism when a large disturbance occurs, and dynamic stability, which concerns with the system's long-term response. Based on the three modes of stability System security can be classified into the three modes. The method of security is classified based on the specific outages, variables used for analysis and time after the outage. Nevertheless, after analyzing the condition, the system can be classified as Steady state or transient or dynamic secure if it is stable for every outage in the contingency list defined for each

mode respectively. Otherwise, it is called as insecure (Costa&Munro, 1984).

Static security is the ability of a power system to reach a steady state operating point without violating the system operating limits following a contingency (Mohammad&Yaoya, 2003). Evaluation of Static security is called as static security assessment. Traditional methods used for contingency analysis is time-consuming. Full AC load flow is utilized for each outage in traditional contingency analysis. The complete procedure required for contingency analysis requires lots of time and gives many results. The traditional methods are not suitable for real-time applications due to varying nature of the power system (Pang&Koivo, 1973).The engineer working in the control center requires enough time to take the control action. If enough time is not given to the engineer cascade tripping of the several types of equipment may occur. The main requirement of the consumer from the utility is the availability of the power as and when required. So, the growth of the country or the society depends on the reliability and quality of the power.

Several Artificial Intelligence techniques were used in security assessment since last four decades. Artificial intelligence techniques like the Self-Organization feature map (Niebur&Germond, 1992; Swarup&Corthis, 2002), and Multi-layered feed forward network (Swarup&Corthis, 2002), (Saeth&Khairuddin, 2008) have been applied to the problem of static security assessment. Some of the literature also reported the use of Radial Basis Function Neural Network (Refaee et al.,1999; Jain et al. ,2003), a Genetic-Based Neural Networks (Aini, 2001) and Query-Based learning approach in Artificial Neural Network (Huang, 2001). Techniques other than Artificial Neural Network (ANN) used in the static security assessment are problem dependent. Neural Networks are good in interpolation but not so good in the extrapolation, which reduces its generalization ability (Kalyani&Swarup, 2001). To overcome the disadvantages of ANN the researchers started use of Support Vector Machine (SVM) based classifier for static security assessment (Kalyani&Swarup, 2011). In the available literature, Static Security states were classified based on either by Equality and Non-equality constraints or using Performance Index. In most of the literature, the crucial part is to decide weighting factor to calculate Security Index. Selection of weighting factor depends on knowledge and experience of the concerned person associated with the particular system. The wrong choice of weighting factor leads to misclassification of security states. Static Security Index was used in the classification of static security states (Kalyani&Swarup, 2011)in which weighting factor is assumed on the base of knowledge and experience. Composite Security Index (CSI) is defined in (Sunitha&Kumar, 2011) and builds on the concept of a hyper-ellipse inscribed within the hyper-box. The main advantage of CSI is that in the calculation there is no need to select proper value of weighting factor. In the most of the literature found, thermal limits of the transmission lines are assumed in the Static Security assessment.

The main work presented in this article are (Wood&Wollenberg, 2012) Composite Security Index is used instead of Performance index with weighting factors. (Kalyani&Swarup, 2013) The thermal limits of the transmission lines are calculated and considered on the base of load ability of the transmission line for short, medium and long lines for calculation of CSI. The load ability limits of short, medium and long lines are considered based on surge impedance loading, percentage voltage regulation, and steady-state stability limit's of the lines respectively. The SVM classifier is designed for Binary-class classification. Based on the value of CSI the classifier is intended to classify the state into secure and insecure following Static Security assessment. The proposed SVM classifier is applied to the IEEE 14 and 30 bus systems.

The remaining part of this paper is structured as follows: Static Security Assessment using the composite security index based on the concept of a hyper-ellipse inscribed within the hyper-box is explained in Section 2. The approach utilized for the calculation of the thermal limit of the transmission line is briefly described in Section 3. The design of Static Security Classifier using Pattern Recognition Approach is explained in Section 4. Performance evaluation of the classifier is given in Section 5 and Results, and discussions are presented in Section 6.

2. STATIC SECURITY ASSESSMENT USING COMPOSITE SECURITY INDEX

The composite security index is the combination of the two terms line flow and bus voltage limit violations. Two kinds of limits are defined for bus voltage, and line flows, viz., the security limit and the alarm limit. The security limit is the maximum limit specified for the bus voltages and line flows. The alarm limit represents alarm zone adjacent to the security limit, which gives an indication of nearness to limit violations (Sunitha et al., 2011).The system is said insecure if any bus voltages or line flows violate their security limit. If any bus voltages or line flows violate their alarm limit without violating their security limit, the system is considered to be in the alarm state. If none of the voltages or line flows violates an alarm limit,the system is called secure. This is specified by a value of “0”. The upper and lower alarm limits and security limits of bus voltages are denoted as A_i^u, A_i^l, V_i^u and V_i^l respectively. The normalized upper and lower voltage limit violations above the alarm limits are given in (1):

$$Y_{v,i}^{\ u} = \frac{[V_i - A_i^u]}{V_i^d} \quad ; if\ V_i > A_i^u$$

$$Y_{v,i}^{\ u} = 0 \quad ; if\ V_i \le A_i^u$$

$$Y_{v,i}^{\ l} = \frac{[A_i^l - V_i]}{V_i^d} \quad ; if\ V_i < A_i^l$$

$$Y_{v,i}^{\ l} = 0 \quad ; if\ V_i \ge A_i^l \qquad (1)$$

Where V_i is the voltage magnitude at bus i. For all upper and lower limit of bus voltages, the normalization factor $D_{v,i}$ is given in (2):

$$Z_{v,i}^{\ u} = \frac{[V_i^u - A_i^u]}{V_i^d}$$

$$Z_{v,i}^{\ l} = \frac{[A_i^l - V_i^l]}{V_i^d} \qquad (2)$$

From equation (1) and (2), the value of the ratio (Y/Z) will give a value of "0" if the value of the bus voltage is between lower and upper alarm limit. It is classified as the secure state. If the value of the bus voltage is greater than the upper alarm limit or less than the lower alarm limit, it gives a value (Y/Z) greater than "0". It is classified as the alarm state. If the value of the bus voltage is greater than the upper-security limit or less than the lower security limit, it gives a value (Y/Z) greater than “1”. It is classified as the insecure state.

For line flows, the limit violation vectors and the normalization factor are defined similarly. Since only the maximum limits are necessary to be stated for the power flow through each line, two types of upper limits are given for each line: the alarm limit and the security limit. The security limit is the maximum limit of the power flowthrough the line. The normalized violation vectors for each line j are given in (3):

$$X_{p,j} = \frac{[\,|P_j| - P_{A,j}\,]}{Base\ MVA} \quad ; if\ |P_j| > P_{(A,j)}$$

$$X_{p,j} = 0 \quad ; if\ |P_j| \le P_{(A,j)} \qquad (3)$$

Where $_jJ$ is the absolute value of the power flow through the line and $P_{A,j}$ is the alarm limit for power flow. The normalization factor for each line is given in (4):

$$Z_{P,j} = \frac{[\,P_{P,j} - P_{A,j}\,]}{Base\ MVA} \qquad (4)$$

Where $P_{P,j}$ is the security limit of the j^{th} transmission line. Here also, the system can be classified with respect to the power flow through the line viz. secure, alarm and insecure based on the value of (Y/Z) vector.

The concept of hyper-ellipse inscribed within the hyper-box is used for constructing the scalar valued composite security index PI_{com} from the violation vectors are given in equation 1, 2, 3 and 4 it is given in (5) as

$$PI_{com} = \left[\sum_i \left(\frac{Y_{v,i}^{\ u}}{Z_{v,i}^{\ u}} \right)^{2n} + \sum_i \left(\frac{Y_{v,i}^{\ l}}{Z_{v,i}^{\ l}} \right)^{2n} + \sum_j \left(\frac{Y_{p,j}}{Z_{p,j}} \right)^{2n} \right]^{\frac{1}{2n}} \qquad (5)$$

Where "n" is the exponent used in the hyper ellipse equation. The value of "n" is chosen as "2", because the approximation of hyper-box to the hyper-ellipse has not improved beyond "n" = 2 (Sunitha et al., 2011). From the value of the composite security index, the system is classified to be in one of the two states as given in Table 1.

Composite Security Index (CSI)	Class Category
$PI_{com} \le 1$	Secure
$PI_{com} > 1$	Insecure

TABLE 1. Class Categories for Security Assessment

3. CALCULATIONS OF THERMAL LIMIT OF THE TRANSMISSION LINES

In most of the work presented in the literature thermal limit or security limit of the transmission lines are assumed, the thermal limit of the transmission lines is provided by the manufacturer of the transmission line. Thermal limits of the IEEE standard bus systems are not available in the available kinds of literature. Most of the researchers have assumed thermal limits on the base of the experience. Kalyani et al., (2011) assumed thermal limit or MVA limit of system branches as 130% of the base case. Kalyani&Swarup, (2009) and Sekhar et al., (2016) assumed allowable maximum power flow through the transmission line using maximum power transfer equation in which δ is taken as 90^0 (Shekhar&Mohanty, 2016), but according to steady state stability, we can allow the value of δ in between 40^0 to 45^0.

In this work, the thermal limits of the IEEE standard test systems are considered based on loadability limit of the transmission line. The transmission lines of the IEEE standard test systems are classified as short, medium and long lines based on X/R ratio. The loadability limit of the short transmission line is equal to the thermal limits of the line and that is decided on the base of surge impedance loading. The voltage drop limit determines the loadability limit of the medium line. The ratio VR/VS ≥ 0.95 is taken to decide the loadability limit of the medium line. The steady state stability is a limiting factor for the loadability limit for the long transmission line (Duncan&Sharma, 2012). For calculation of loadability limit of the long transmission line, the angle δ is taken as 45^0 in equation 6.

$$P_{max} = \frac{V_i V_j}{X_{ij}} \sin \delta \qquad (6)$$

4. DESIGN OF STATIC SECURITY CLASSIFIER USING PATTERN RECOGNITION APPROACH

A pattern is a pair consists of information or observation and the meaning of the observation. Pattern recognition interprets meaning from observation or information. Pattern recognition is defined as the operation of taking raw data and taking action based on the class of data. Classifying the patterns based on either past knowledge about the system or statistical information is obtained from the patterns. The main aim of applying pattern recognition approach to security assessment is to reduce the online computation time (Kalyani&Swarup, 2011). It can be done at the cost of an extended offline computation. The progression of steps carried out in the design of static security classifier is represented in the form of the flow chart in Figure 1.

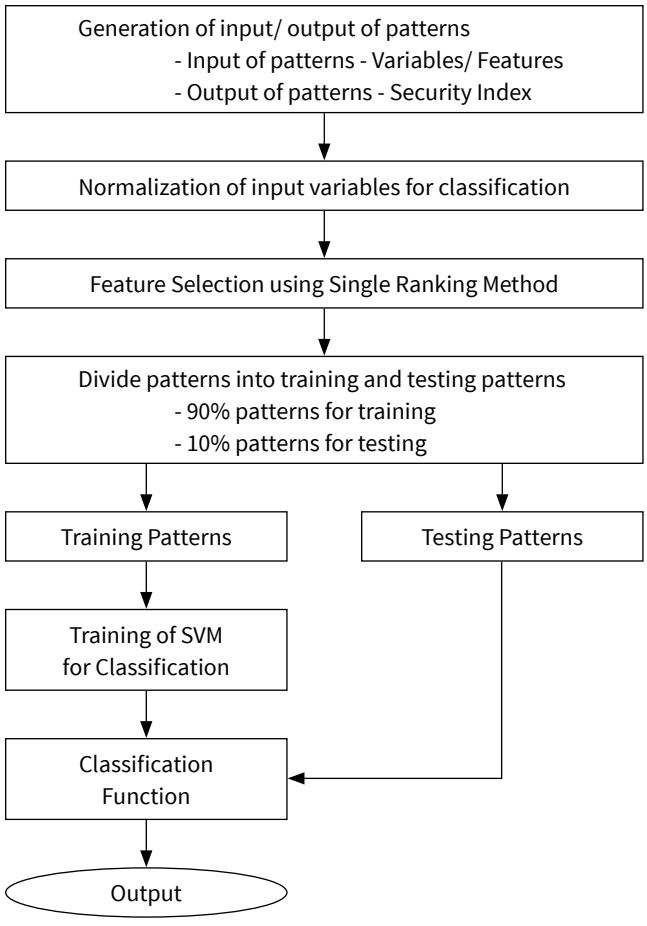

FIGURE 1. Main steps in design of static security classifier

As shown in Figure 1, the design of static security classifier using SVM goes through a series of sequential steps. In upcoming sections, explain the steps and Support Vector Machine used in the classification scheme. The main stages are data generation, normalization, feature selection, classifier design and performance evaluation.

4.1. DATA OR PATTERN GENERATION

The success of any classifier depends on good and wide ranges of the training sets. The training set must represent entire operating states of the power system (Kalyani & Swarup, 2009). This training set can be formed either by collecting past real measurements or by offline studies of the power system. A large number of operating scenarios are generated through offline simulations. Each operating scenario is considered as a pattern. Each pattern consists of power system variables such as bus voltages (V_i), bus angles (δ_i), active and reactive bus loads (P_i and Q_i), active and reactive generations (P_{Gi} and ${}_GQ$), active and reactive power flows (P_{ij} and Q_{ij}) through the transmission line. Patterns are generated by changing the load on the bunch of the buses from 50% to 150% of the original load arbitrary. Single line contingency is considered for this work.

4.2. NORMALIZATION OF DATA

Normalization of pattern variables is done to improve the performance of the algorithm. The main advantage of normalization in Support Vector Machine is helpful to reduce the effect of the attributes in greater numeric ranges on the attributes of the smaller numeric ranges, and it also reduces numerical difficulties during the calculation. Because kernel values usually depend on the inner products of feature vectors, e.g. the linear kernel and the polynomial kernel, large attribute values might cause numerical problems. The variables in the feature vector are normalized in the range (Wood&Wollenberg, 2012) using the min-max normalization method. It is one of the widely used techniques by most of the researchers for the data scaling process (Kalyani&Swarup, 2011).

4.3. FEATURE SELECTION

The success of any classifier depends on the selected features for the classification. To get complete information about the nature of the power system, the features are selected in high numbers. Therefore, it is important to decide the relatively small number of features unique for classification (Weerasooriya&Sharkawi, 1992). Feature selection is a process of selecting important features from a total number of features. Selected feature will give more useful information than not selected features. Engineering judgments may select features, but occasionally it may lead to rejection of important features.

Single ranking and Correlation Coefficient Method is used for feature selection. The heuristic notion of interclass distance is used to select the important features. The average pair wise distance between the patterns is useful information for the measure of class separability in the region concerning the particular variable. The index F_i provides a measure of this class separation concerning the i^{th} variables.

$$F_i = \left| \frac{m_i^{(s)} - m_i^{(l)}}{\sigma_i^{(S)^2} - \sigma_i^{(l)^2}} \right| 1 \le i \le 1 \qquad (3)$$

Where,

$$m_i^{(S)} = \frac{1}{N^{(S)}} \sum_{j=1}^{N(S)} X_{ij}^{(S)}$$

$$m_i^{(S)} = \frac{1}{N^{(S)}} \sum_{j=1}^{N(S)} X_{ij}^{(S)}$$

$$\sigma_i^{(S)\,2} = \frac{1}{N^{(S)}} \sum_{j=1}^{N(S)} \{ X_{ij}^{(S)} - m_i^{(S)} \}^2$$

$$\sigma_i^{(l)} = \frac{1}{N^{(l)}} \sum_{j=1}^{N(l)} \{ X_{ij}^{(l)} - m_i^{(l)} \}^2$$

Where, $m_i^{(.)}$ and $\sigma_i^{(.)^2}$ are mean and variance if variable corresponding to class (.). The superscript (S) stands for 'secure' while (I) stands for 'insecure'. $N^{(S)}$ and $N^{(I)}$ indicate the number of secure and insecure patterns that form the training set {$N = N^{(S)} + N^{(I)}$}. Variables with higher values of F suggest more information about class separability than others. Therefore classification can be based on selected variables which will be referred to as features.

The correlation coefficient between the i^{th} and the j^{th} variable is defined as:

$$C_{Cij} = \frac{E\{y_i y_j\} - E\{y_i\}E\{y_j\}}{\sigma_i \sigma_j} \; i,j = 1,2,\ldots,n$$

Where,

$$E\{y_i y_j\} = \frac{1}{N} \sum_{k=1}^{N} y_{ik} y_{jk}$$

$$E\{y_j\} = \frac{1}{N} \sum_{k=1}^{N} y_{ik}$$

$$\sigma_i^2 = \frac{1}{N} \sum_{k=1}^{N} (y_{ik} - E\{y_i\})^2$$

The following steps for feature selection:

1. Calculate F_i for all i such that $0 \le i \le n$.
2. Arrange variables according to the descending order of F_i.
3. Go to the first variable with highest F_i value.
4. Calculate correlation coefficients if all remaining variables with respect to this variable.
5. Eliminate all variables which have the value greater than 0.9 values.
6. Go to the next highest ranked variables and go to step 4.

4.4. CLASSIFIER DESIGN USING BINARY CLASS SUPPORT VECTOR MACHINE

The classifier gives the boundary between separating classes. The accuracy of the classifier depends on the data provided for training purpose. The training algorithms available are least squares, back propagation, linear programming, etc., to design the classifier (Mohammad&Yaoyu, 2003). These existing algorithms consume less time, but have certain limitations such as poor classification accuracy and high misclassification rate, specifically when the size of the problem increases. So, Support Vector Machine is used for efficient training procedure. The static security assessment problem is treated as binary class pattern classification problem in this work.

SVM classifier reduces the generalization error by optimizing the trade-off between the number of training errors. SVMs in most of the cases are found to provide better classification results than other widely used pattern recognition classifiers. SVMs carry out the task of the binary classification by mapping the input data to a multidimensional feature space, and then it will construct an optimal hyper plane classifier separating the two classes with maximum margin. For minimization of the error optimal hyper plane is built by an iterative training algorithm in the SVM. Consider a training set $T = \{x_i, y_i\}$, where x_i is a real-valued n-dimensional input vector and $y_i \epsilon \{0, 1\}$ is a label that determines the class of data instance, x_i. For the construction of optimal separating hyper plane, the SVM classifier solves the following optimization problem.

$$\min_{w,b,\xi} \frac{1}{2} w^T w + C \sum_{i=1}^{l} \xi_i$$

Subject to

$$y_i (w^T \emptyset(x_i) + b \ge 1 - \xi_i; \quad \xi_i \ge 0, \quad i = 1,2,\ldots..,l$$

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, $\emptyset$ (.) is a mapping function called 'kernel' function and b is the threshold. The kernel function maps the data into the feature space from the input space where they are linearly separable. The concept of kernel mapping let on the SVM models to perform separations even with very complex boundaries. In this paper, Radial Basis Function kernel is used in the design of Binary class Support Vector Machine model.

4.4.1 CHOICE OF KERNEL

The Radial Basis Function (RBF) is used as the Kernel mapping function because of its widely known accuracy, and it is capable of handling non-linear relations between the class labels and input features.

4.4.2. ADJUSTING THE KERNEL PARAMETERS

Two parameters associated with RBF functions are to be selected (1) penalty parameter C and (2) RBF kernel parameter γ. The main aim is to identify optimal (C,γ) for the classifier to accurately predict unknown data. The grid search technique is used for selection of parameters because it is the most common method used to determine SVM parameters. In v cross-validation, the whole training set is equally divided into v subsets, v-1 subsets are used for training purpose, and one remaining subset is used for testing of trained classifier. This procedure is repeated for the various set of subsets. The cross-validation accuracy is calculated by the percentage of data samples correctly classified. Here Grid search is used on C and γ using 5-cross-validation. All pairs of C and γ were tried, and the one pair is selected which will give highest cross-validation accuracy. The sequence was used $C = \{2^{-5}, 2^{-4}, 2^{-3} \ldots 2^{15}\}$ and $\gamma = \{2^{-15}, 2^{-14}, 2^{-13} \ldots 2^{5}\}$.

4.4.3. TRAINING AND TESTING OF SVM CLASSIFIER

Once kernel parameters are selected SVM classifier is trained with the normalized input-output training data samples. On the satisfactory performance of the SVM classifier in the training phase, it is validated with test data samples to check its overall performance.

5. PERFORMANCE EVALUATION OF CLASSIFIER

The performance evaluation of trained classifier is validated using following performance measures:

1. Classification Accuracy (CA)

$$\text{Classification Accuracy (\%)} = \frac{\text{(No. of samples classified correctly)}}{\text{(Total no. of samples in data set)}} \times 100$$

2. Secure Misclassification Rate (SMCR)

$$\text{Secure Misclassification Rate (\%)} = \frac{\text{(No. of 0's classified as 1)}}{\text{(Total no. of insecure states)}} \times 100$$

3. Insecure Misclassification Rate (ISMCR)

$$\text{Insecure Misclassification Rate (\%)} = \frac{\text{(No. of 1's classified as 0)}}{\text{(Total no. of secure states)}} \times 100$$

In the static security assessment, it is necessary to make sure that the misclassification rate is as small as possible. Especially, the chances of an insecure state being wrongly predicted as secure states need to be reduced. So, the Classifier for the static security assessment must be designed to have high classification accuracy and less misclassification rate.

6. RESULTS AND DISCUSSIONS

The proposed work aims to develop a static security assessment Binary-classifier using Support Vector Machine. The proposed binary class SVM classifier is implemented in IEEE 14 and 30 bus test systems (Zimmerman&Gan, 1997). Data are generated by varying loads in the bunch of buses between 50% to 150% of their base case values arbitrary. Single line contingency is considered for each operating scenario. A load flow solution is done using Newton-Raphson method. Data generation is done with the help of MATPOWER toolbox (Zimmerman&Gan, 1997). LIBSVM software developed by C. C. Chang and C. J. Lin is used for SVM binary-classifier design (Chang&Lin, 2001). For calculation of the composite security index, we have to choose both alarm and security limits for bus voltages and line flows. ± 5% and ± 7% of the desired bus voltage values are taken as alarm and security limits for bus voltages. Security limit for the transmission line is calculated as explained in section 3. Alarm limit is taken as the 80% of security limit. For PV buses the specified bus voltage is taken as desired bus voltage and for PQ buses "1 p.u." is taken as the desired bus voltage. Approximately, 90% of data used for training and 10% of data used for testing. Feature selection is done by Single Ranking and Correlation Coefficient method. Results of feature selection and data generation for static security assessment are given in Table 2, Table 3 and Table 4. Table 2 gives the dimensionality reduction achieved by the Single Ranking and Correlation Coefficient method. The complexity of the classifier is reduced due to fewer numbers of feature used, it leads to reduction of training and testing time in the implementation of SVM. Results of the parameter selected by the Grid Search using 5-cross-validation are given in Table 5. Performances of the SVM-based binary-classifier on the IEEE standard test systems are given in Table 6.

	IEEE 14 Bus System	IEEE 30 Bus System
No. of Variables	106	214
No. of Feature Selected By Single Ranking Method	10	24
Dimensionality Reduction	9.43%	11.21%

TABLE 2. Dimensionality reduction due to single ranking feature selection method

IEEE 14 Bus System	V_9, V_{11}, V_{14}, V_{12}, V_{10}, $P_{5\text{-}6}$, P_{G1}, $Q_{5\text{-}6}$, $P_{2\text{-}3}$, $P_{6\text{-}13}$
IEEE 30 Bus System	Q_{G1}, Q_{G5}, Q_{G2}, P_{G1}, V_7, V_{28}, Q_{G8}, $Q_{2\text{-}5}$, V_{20}, $P_{4\text{-}12}$, $P_{12\text{-}14}$, $Q_{6\text{-}7}$, V_{14}, V_{15}, $P_{15\text{-}18}$, $Q_{6\text{-}28}$, $P_{12\text{-}15}$, $Q_{9\text{-}10}$, $Q_{24\text{-}25}$, V_{24}, $P_{9\text{-}11}$, V_{23}, $Q_{28\text{-}27}$, $P_{15\text{-}23}$

TABLE 3. Features selected by single ranking and correlation method

	IEEE 14 Bus System	IEEE 30 Bus System
Total Operating Scenarios	500	975
Total Operating Scenarios	312	743
Total Insecure Cases	188	232
Training Set		
Operating Scenarios	440	819
Secure Cases	281	614
Insecure Cases	159	205
Testing Set		
Operating Scenarios	60	156
Secure Cases	31	129
Insecure Cases	29	27

TABLE 4. Data generation for static security assessment

System	Selected parameters value (Parameter Ranges $C = (2^{-5}, 2^{15}$ in step of $2^{1})$ and $\gamma = (2^{-15}, 2^{5}$ in step of $2^{1})$)
IEEE 14 Bus System	C = 128.0 γ = 1.0
IEEE 30 Bus System	C = 16384.0 γ = 0.0625

TABLE 5. Result of parameter selection of radial basis function using grid search and 5-cross validation

	IEEE 14 Bus System	IEEE 30 Bus System
Train Set		
5-Cross Validation CA (%)	99.091%	98.53%
Samples CA (%)	99.55% (438/440)	99.88% (818/819)
SMC (%)	0.629% (1/159)	0% (0/205)
ISMC (%)	0.356% (1/281)	0.1628% (1/614)
Test Set		
Samples CA (%)	93.33% (56/60)	98.07% (153/156)
SMC (%)	10.34% (3/29)	7.41% (2/27)
ISMC (%)	3.23% (1/31)	0.775% (1/129)
Overall CA (%) (Training and Testing)	98.80% (494/500)	99.59% (971/975)

TABLE 6. Performance evaluation of SVM classifiers on train set and test set

The performance of the SVM-based binary-classifiers on the test system is found quite satisfactory regarding the high classification accuracy and less misclassification rate. Secure Misclassification is not dangerous to the system because it is giving the false alarm. However Insecure Misclassifications are dangerous because here the insecure state is classified as the secure state and it is also called as the false dismissal. In IEEE 14 bus system, total four misclassifications occur in testing, in which three secure states classified as the insecure state, one insecure state is classified as the secure state. So, only one misclassification is dangerous. In the results of the IEEE 30 bus system, two secure states are classified as the insecure states; one insecure state is classified as the secure states. Less misclassification rate for insecure cases represents the effectiveness of the classifier.

7. CONCLUSION & POLICY IMPROVEMENT

This paper has proposed a binary-classifier based on the Support Vector Machine for the static security assessment of the power system. Selection of the weighting factor is eliminated due to the use of CSI instead of other performance indices. Thermal limit of the transmission lines is selected based on the loadability of the transmission line. The loadability of the transmission line is calculated by classifying transmission line into the short, medium and long transmission line. The classification of the power system indicates the security states to the operator, as the trained Support Vector Machine based classifier predicts the security state of the power system in the fraction of second; it helps to initiate control action as early as possible. So, Cascade tripping of the power system is avoided. The proposed binary-classifier was tested on IEEE standard test systems. Simulation results have proven high classification accuracy and fewer misclassification rates of the binary-classifier, Especially Insecure misclassifications are very less. Due to less time in the prediction of the security state and less insecure misclassification rate making it suitable for online implementation. The prediction of the security state in the small possible time for the present operating scenario will help utility to give reliable power to the society. Future work is the implementation of the Binary Class SVM to the larger systems.

REFERENCES

Chang, C. (2001). LIVSVM-A Livrary for Support Vector Machines. http://www. csie. ntu. edu. tw/~ cjlin/libsvm/.

Costa, Munro&Nattern (1984). Recognition in power-system security,International Journal of Electrical Power & Energy Systems, 6(1), 31–36.

Jain, T., Srivastava, L., & Singh, S. N. (2003). Fast voltage contingency screening using radial basis function neural network. IEEE Transactions on Power Systems, 18(4), 1359-1366.

Kalyani, S., &Swarup, K. S. (2013). Static security assessment in power systems using multi-class svm with parameter selection methods. International Journal of Computer Theory and Engineering, 5(3), 465

Kalyani, S., &Swarup, K. S. (2011). Classification and assessment of power system security using multiclass SVM. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(5), 753-758.

Kalyani, S., &Swarup, K. S. (2009). Binary svm approach for security assessment and classification in power systems. In India Conference (INDICON), 2009 Annual IEEE (pp. 1-4). IEEE.

Kalyani, S., &Swarup, K. S. (2009). Power system security assessment using binary SVM based pattern recognition. World Academy of Science, Engineering and Technology, 52, 725-731

Kalyani, S., &Swarup, K. S. (2012). Design of pattern recognition system for static security assessment and classification. Pattern Analysis and Applications, 15(3), 299-311.

Mohamed, Sheikh Maniruzzaman, AiniHussain, A. (2001). Static security assessment of a power system using genetic-based neural network. Electric Power Components and Systems, 29(12), 1111-1121.

Niazi, K. R., Arora, C. M., &Surana, S. L. (2004). Power system security evaluation using ANN: feature selection using divergence. Electric Power Systems Research, 69(2), 161-167.

Niebur, D., &Germond, A. J. (1992). Power system static security assessment using the Kohonen neural network classifier. IEEE Transactions on Power Systems, 7(2), 865-872.

Refaee, J. A., Mohandes, M., &Maghrabi, H. (1999). Radial basis function networks for contingency analysis of bulk power systems. IEEE Transactions on Power Systems, 14(2), 772-778.

Pang, C. K., Koivo, A. J., & El-Abiad, A. H. (1973). Application of pattern recognition to steady-state security evaluation in a power system. IEEE Transactions on Systems, Man, and Cybernetics, 3(6), 622-631.

Saeh, I. S., &Khairuddin, A. (2008, December). Static security assessment using an artificial neural network. In Power and Energy Conference, 2008.PECon 2008. IEEE 2nd International (pp. 1172-1178). IEEE.

Sekhar, P., &Mohanty, S. (2016). An online power system static security assessment module using multi-layer perceptron and radial basis function network. International Journal of Electrical Power & Energy Systems, 76, 165-173.

Shahidehpour, M., & Wang, Y. (2004). Communication and control in electric power systems: applications of parallel and distributed processing. John Wiley & Sons.

Sidhu, T. S., & Cui, L. (2000). Contingency screening for steady-state security analysis by using FFT and artificial neural networks. IEEE Transactions on Power Systems, 15(1), 421-426.

Sunitha, R., Sreerama, R. K., & Mathew, A. T. (2011). A composite security index for on-line steady-state security evaluation. Electric Power Components and Systems, 39(1), 1-14.

Swarup, K. S. (2008).Artificial neural network using pattern recognition for security assessment and analysis. Neurocomputing, 71(4), 983-998.

Swarup, K. S., &Corthis, P. B. (2002). ANN approach assesses system security. IEEE Computer Applications in Power, 15(3), 32-38.

Weerasooriya, S., & El-Sharkawi, M. A. (1992, May). Feature selection for static security assessment using neural networks.In Circuits and Systems, 1992. ISCAS'92. Proceedings., 1992 IEEE International Symposium on (Vol. 4, pp. 1693-1696). IEEE.

Glover, J. D., Sarma, M. S., &Overbye, T. (2012). Power System Analysis & Design, SI Version. Cengage Learning.

Wood, A. J., &Wollenberg, B. F. (2012). Power generation, operation, and control. John Wiley & Sons.

Zimmerman, R. D., Murillo-Sánchez, C. E., &Gan, D. (1997). MATPOWER: A MATLAB power system simulation package. Manual, Power Systems Engineering Research Center, Ithaca NY, 1.

Mr. Astik Dhandhia
Research Scholar and Lecturer,
Department of Electrical Engineering,
Pandit Deendayal Petroleum University,
Raysan, Gandhinagar, India.

Dr. Vivek Pandya
Head and Professor,
Department of Electrical Engineering,
Pandit Deendayal Petroleum University,
Raysan, Gandhinagar, India.

Mr. Siddharth Joshi
Lecturer,
Department of Electrical Engineering,
Pandit Deendayal Petroleum University,
Raysan, Gandhinagar, India.

E-mail: *astikdhandhia@gmail.com*