Selection of Power System Variables for Binary-Class Support Vector Machine in Static Security Assessment of Power System

Jignesh Borisagar
Gujarat Power Research and Development Cell,
Urja Vikas Nigam Limited,
Gandhinagar, India
jigneshborisagar05@gmail.com

Astik Dhandhia
Electrical Department,
Shantilal Shah Engineering College,
Bhavnagar, India
astikdhandhia@gmail.com

***Abstract*— determining the correct decision for the current power system operating scenario is crucial for the operator to ensure a reliable and secure power system. The limitations of traditional power flow frameworks include higher memory requirements and lengthier computation times. Therefore, it is not a practical solution for applications require static security assessments in real time. Additionally, the composite security index was developed to prevent the masking issue resulting from performance indexes based on line loadings and bus voltage deviations for security assessment. As a result, the composite security index has a stronger ability to distinguish between contingency cases involving closer violations. Support vector machines have been used in the solution of the power system static security binary-class classification problem. The performance of the binary-class support vector machine classifier has been shown to be subject to several sets of power system variables. In order to achieve the best feature selections and the lowest rate of misclassification, sequential forward selection has been employed. Two IEEE standard test systems are used to validate the outcomes of the suggested methodology.**

Keywords*— *Composite Security Index, Feature Selection, Static Security Assessment, Support Vector Machine

I. INTRODUCTION

The main three parts of the power system are the distribution, transmission, and generation of power. Ensuring that consumers receive consistent and sufficient electricity throughout power system operation is of the utmost significance. The deregulation of the electrical grid has made continuous power more important than ever. A security of power system means the ability to survive without loss of power to consumers during critical contingencies [1]. It can be defined as a secure system if it works within its acceptable operating zone during normal operation as well as in case of emergency. The process of evaluating a system's steady state behavior by the solution of a series of algebraic equations is known as steady state security assessment. This article only discusses static security assessments. The three primary elements of the security process are power system control for secure operation, contingency analysis, and monitoring of the power system [2]. Contingency analysis is the most concerning of these three portions since it requires a lot of time-consuming simulations, one after the other. Power flow simulations are used in the time-consuming contingency analysis process to ascertain the security of the power system. Accordingly, it may not be suitable for real-time applications in some circumstances [3]. Therefore, new and very effective techniques for the safe operation and control of gigantic power systems have to be developed. The shortcomings of the traditional approach used for security evaluation can be addressed by the pattern recognition (PR) method. The pattern recognition method's quick power system security evaluation is made possible by the majority of calculations being completed offline. The classification function will be used to quickly assess the security of the system and was designed using training data sets that were generated offline. Static security assessment has been addressed by artificial intelligence techniques such as the Radial Basis Function Neural Network [4], Multi-layered feed forward network [5], Self-Organization feature map [6]. Random forest model [7], Convolutional Neural Networks [8]. The results of the aforementioned approaches primarily depend on the specific problem at hand, and they are also unable to predict future insecure states. The classification function in this case is designed using Support Vector Machines (SVM). Using the hyper-ellipse concepts inside the hyper-box, the Composite Security Index (CSI) is used to have a lower misclassification rate during security assessments. The masking issue will be resolved by using CSI. The power system variables that are used to generate the patterns determine how well the intended function performs throughout the training and testing phases when employing the pattern recognition approach. In the last forty years, various researchers have used varying sets of variables—such as bus voltages and angles, active and reactive power loads at buses, active and reactive generation at buses, active and reactive power flow in transmission lines, and so forth—to form the input patterns to design the security function. To create the patterns, researchers have taken a subset of the aforementioned variables. It is therefore crucial to investigate how various sets of variables affect the way static security assessments are performed when creating patterns. The Sequential Forward Selection approach has been used to minimize the pattern's dimension.

Keeping in mind the work mentioned above in the context of static security evaluation of power systems, the following objectives have been set during this work.

- To use an SVM-based binary class classifier to classify static security assessment problems into secure and insecure levels based on pattern recognition techniques.
- Formulating a composite security index to identify patterns as secure or insecure.
- Radial Basis Function (RBF) is used for binary class support vector machines, and sequential forward selection is used for optimal feature extraction.

2024 IEEE International Conference on Industrial Technology (ICIT) | 979-8-3503-4026-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICIT58233.2024.10540835

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.

- To evaluate the impact of various power system variables on the performance of a binary classifier built using a support vector machine as a pattern vector.

The proposed methodology has been applied in IEEE 30 bus and IEEE 118 bus test systems.

II. Static Security Assessment Using Composite Security Index

Static security refers to a system's capacity to continue operating inside a predetermined area where no constraints should be violated. In addition, even in the unlikely scenario of a system line or generator failure, the violations of boundaries must be limited to the specified limit [2], [9-10]. The definition of a contingency is a failure of any generator or transmission line. When a contingency occurs in the power system, a static security assessment analyzes any significant overload on any lines or bus voltage limit violation. The critical contingencies are then ranked and classified by SSA in descending order based on their main negative impact on static security. Calculating the performance index (PI) using load flow solutions is the standard procedure for this kind of ranking and classification. The masking problem has a significant impact on the contingency classifying and ranking approach [2], [11]. In [12], an improved methodology for computing the Composite Security Index (CSI) is presented. This approach uses a hyper-ellipse enclosed within a hyper-box, which completely eliminates the masking problem of conventional PI.

Formulation of Composite Security Index

The criteria given in (1) and (2) must be met for power systems to function normally.

$$\sum_{a=1}^{N_{Gen}} P_{Ga} = P_{TL} + P_l \tag{1}$$

$$\left.\begin{array}{c} P_{Ga}^{min} \le P_{Ga} \le P_{Ga}^{max}, a = 1,2,\dots,N_{Gen} \\ \left|V_a^{min} \le |V_a| \le |V_a^{max}|\right|, i = 1,2,\dots,N_{Bus} \\ P_{jk} \le P_{jk}^{max}\ for\ every\ branch, j-k \end{array}\right\} \tag{2}$$

After any outage, the degree to which the constraints in (1) and (2) are satisfied can verify the "secure state" of the power system. Conversely, in the event that any of the constraints in (1) and (2) are violated, the system state is considered to be in an "insecure state." For the purpose of determining the secure and unsecure states of bus voltages, both upper and lower limit violations are taken into consideration; however, only upper limit violations are taken into consideration for transmission line loading. The system state is classified as either secure or insecure based on the composite security index value, according to the requirements listed in the following section.

A. Bus Voltage Security Index

Set $V_a^d, A_{V,a}^u, A_{V,a}^l, S_{V,a}^u$ and $S_{V,a}^l$ at bus a. And calculate $a_{(V,a)}^u, b_{(V,a)}^u, a_{(V,a)}^l$ and $b_{(V,a)}^l$.

$$\left.\begin{array}{c} a_{(v,a)}^u = \left[V_a - A_{V,a}^u\right]/(V_a^d); if\ V_a > A_{V,a}^u \\ a_{(V,a)}^l = \left[A_{V,a}^l - V_a\right]/(V_a^d); if\ V_a < A_{V,a}^l; \\ a_{(v,a)}^u = 0; if\ A_{v,a}^l \le V_a \le A_{v,a}^u \\ and\ a = 1,2,\dots,N_{Bus} \end{array}\right\} \tag{3}$$

$$\left.\begin{array}{c} b_{(v,a)}^u = \left[S_{V,a}^u - A_{V,a}^u\right]/(V_a^d) \\ b_{(V,a)}^l = \left[A_{V,a}^l - S_{V,a}^l\right]/(V_a^d) \\ and\ a = 1,2,\dots,N_{Bus} \end{array}\right\} \tag{4}$$

With the use of (3) and (4) in the hyper-ellipse equation as given in [12] and after setting $k = 1.0$, the security index for bus voltage can be given as per (5).

$$PI_V = \left[\sum_a \left(a_{(V,a)}^u / b_{(V,a)}^u\right)^{2k} + \sum_a \left(a_{(V,a)}^l / b_{(V,a)}^l\right)^{2k}\right]^{1/2k} \tag{5}$$

It is simple to classify the power system state which is related to bus voltage security using (5); it can be classified as (6) below.

$$\left.\begin{array}{c} PI_V = 0; Secure \\ PI_V \ge 1; Insecure \end{array}\right\} \tag{6}$$

B. Security Index for Transmission Line Power Flow

Only upper limitations are taken into account when calculating the line flow security index because of the maximum limit interest on line power flow. In (7) and (8), set $A_{MW,b}, S_{MW,b}$ through b^{th}line.

$$c_{MW,b} = \left[|MW_b| - A_{MW,b}\right]/Base\ MVA\ if\ |MW_b| > A_{MW,b}$$

$$c_{MW,b} = 0\ if\ \left|MW_b < A_{MW,b}\right|\ and\ b = 1,2,.,N_{line} \tag{7}$$

$$d_{MW,b} = \left[S_{MW,b} - A_{MW,b}\right]/Base\ MVA,\ b = 1,2,.,N_{line} \tag{8}$$

Calculate $c_{MW,b}$ and $d_{MW,b}$ for the b^{th}line. The state of the power system is determined by the Line Power Flow Security Index, which is derived from equations (7) and (8). Its value can be obtained in equation (10).

$$PI_P = \left[\sum_b \left(c_{MW,b}/d_{MW,b}\right)\right]^{1/2k} \tag{9}$$

$$\left.\begin{array}{c} PI_P = 0; Secure \\ PI_P \ge 1; Insecure \end{array}\right\} \tag{10}$$

The composite security index, as indicated in equation (11) can be created by combining equations (5) and (9) and applying the hyper ellipse methodology covered by the hyper box. Contingency situations can also be ranked in order of decreasing CSI value. CSI will be particularly useful in overcoming the problem of masking and violating. As stated in (12), the value of CSI can be used to categorize the overall security of the power system.

$$PI_C = \left[\sum_a \left(a_{(V,a)}^u / b_{(V,a)}^u\right)^{2k} + \sum_a \left(a_{(V,a)}^l / b_{(V,a)}^l\right)^{2k} + \sum_b \left(c_{MW,b}/d_{MW,b}\right)^{2k}\right]^{1/2k} \tag{11}$$

$$\left.\begin{array}{c} PI_C = 0; Secure \\ PI_C \ge 1; Insecure \end{array}\right\} \tag{12}$$

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.

III. Power System Static Security Assessment using Pattern Recognition

The system operator can make an accurate decision regarding the static security of the system by referring to the two classes—secure and insecure—that are described here for static security assessment. Because most simulation work is done offline, the pattern recognition (PR) technique used in this work has lessened the load on online computations. The purpose of the offline simulations is to generate a large number of operating situations that will serve as the basis for the creation of the static security classifier. For on-line applications, this classifier will be directly utilized to achieve faster call of power system static security. For the purpose of assessing power system static security, the data generation and pattern recognition methodology used in this work is described in detail in Fig. 1.

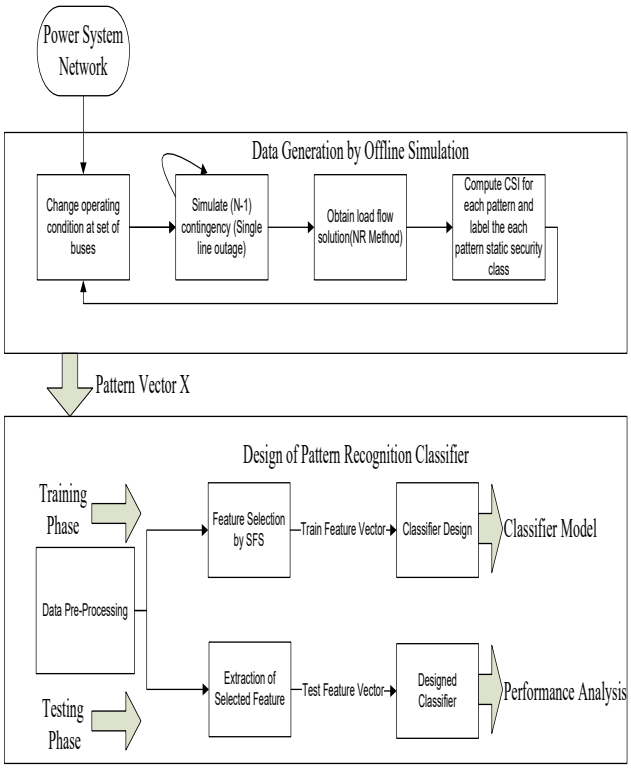

Fig.1 Steps followed in Data generation and PR approach for SSA

A. Pattern Generation for Static Security Assessment of Power System

The development of an adequate training set may be a crucial component in any pattern recognition approach's effectiveness. The training set should be chosen to adequately cover the entire spectrum of power system operating scenarios, as well as variations in the loads of active and reactive power at load buses and as contingency cases for transmission lines and generators that might compromise the security of the power system. These offline data obtained are considered to be a "pattern" [13]. For both active and reactive power on these specified bus groups, the load variation range is set at 50% to 150% of their base case loadings. Additionally, generator bus active power generation is adjusted appropriately to meet the criteria given in (1). Static security is greatly impacted by events like generator or transmission line outages in addition to fluctuations in load. Here, a single transmission line outage is implemented one at a time.

It is essential to choose variables that fully capture the characteristics of the power system. Therefore, it is necessary to investigate how various sets of factors affect the power system in the present scenario. Here, the impact of using various variable sets on the classifier's performance has been investigated. The five sets in all are regarded as presented in (13–17). Thus, load flow is achieved for each operating situation, and a pattern is created using the values given in (13–17). The CSI's decision, as stated in (12) will determine which state of power system is labeled as secure or unsecure.

$$X_1 = \{|V_a|, \delta_a\} \tag{13}$$

$$X_2 = \{|V_a|, \delta_a, Z\} \tag{14}$$

$$X_3 = \{|V_a|, \delta_a, P_{Ga}, Q_{Ga}, P_{Da}, Q_{Da}\} \tag{15}$$

$$X_4 = \{|V_a|, \delta_a, P_{Ga}, Q_{Ga}, P_{Da}, Q_{Da}, Z\} \tag{16}$$

$$X_5 = \{|V_a|, \delta_a, P_{Ga}, Q_{Ga}, P_{Da}, Q_{Da}, P_{jk}, Q_{jk}\} \tag{17}$$

A binary class problem involving the static security assessment of a power system with pattern recognition has been introduced. SVM is successfully used to create a binary classifier that divides a system into secure and unsecure states. The masking issue is avoided and reliable distinction between secure and insecure scenarios that fall within close region violations of power system limitations is made possible by the use of the composite security index. The sequential forward selection technique decreases pattern size while increasing classification accuracy. After comparing the performance of a binary classifier using various sets of power system variables as patterns, it was discovered that bus voltages, bus angles, and contingency number as the binary representation adequately covered information about the power system's static security state.

B. Feature Selection

Every pattern consists of an enormous number of variables. As stated in (13–17), the size of each pattern may further rise in proportion to the size of the system. Feature selection, which involves selecting a small number of variables known as "features" from (13–17), will be useful in reducing the original pattern vector's dimension. A set of variables like this is known as a feature vector, and it appears to be following: $Y = \{y_1, y_2, .., y_k\}$. The variables in the feature vector are much smaller than the variables in the pattern vector. There is a chance that some significant variables will be lost during the process of selecting a small, ideal collection of features from the large variable set. This could affect the accuracy of the classifier module and raise the rate of misclassification. Here, the feature selection process uses a sequential forward selection (SFS), which adds variables to the feature vector in a sequential manner. It operates by minimizing the objective function. The SFS approach begins with an empty set of features and adds them one at a time until the objective function is no longer maximized.

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.

C. Classifier Design using Multiclass Support Vector Machine

SFS is particularly helpful in extracting an ideal feature vector Y, which is then used as an input pattern to build a classifier. The classifier creates the borders that divide various classes into secure and insecure classes. Unknown testing patterns are used to validate the classifier, which is designed using the training patterns. In classifier design, various techniques are used, including neural networks with back propagation classifier, K-nearest neighbor (KNN), and least squares [13]. These techniques take extremely little time to compute, but their lower classification accuracy is found to be inappropriate for static security assessments.

SVMs are recently created learning algorithms that have demonstrated remarkable accuracy even in complicated systems when used to solve classification problems. Let $A = \{m_i, n_i\}$ is a training set, where m_i the input vector is valued having $n-$ dimension and $n_i \in \{+1, -1\}$ represents a label for class determination of data instance n_i. The locations closest to the generated hyper plane are known as Support Vectors (SVs). The maximum margin required to create SVs. By using an iterative training process to minimize the error function, SVM creates this ideal hyper plane.

In this work, two class categories for classifications—secure and insecure—are considered for the security assessment of the power system. For training of every binary classifier, the data are known solely from their corresponding classes. For i^{th} and j^{th} class from training data, the function is resolved as an optimization problem. The "Max-Wins voting" method is used in this instance for classification [14].

D. Selection of SVM Parameters

For support vector machines (SVMs), the Radial Basis function (RBF) is a highly recommended kernel mapping function [15] due to its lower misclassification rate, improved classification accuracy, and potential to capture non-linearity between selected features and class labeling.

The optimal values of (c, γ) are obtained using *v-fold* cross validation using Grid search. The best accuracy in cross validation may achieve by selecting optimal value (c, γ). The range $\{2^{-5}, 2^{-4}, \dots, 2^{14}, 2^{15}\}$ and $\{2^{-15}, 2^{-14}, \dots, 2^{4}, 2^{5}\}$ are chosen for c and γ, respectively. To accurately estimate the power system state in any PR problem, the classification accuracy of the classier, as given in (19), should be the highest, and the secure and insecure misclassification, as given in (20) and (21) should be the least.

E. Performance evaluation terms

Classification Accuracy (CA)

$$CA\ (\%) = \frac{Total\ correctly\ classified\ patterns}{Total\ patterns\ in\ data\ set} \times 100 \qquad (19)$$

Secure Misclassification (SMC)

$$SMC(\%) = \frac{No.of\ secure\ cases\ classified\ as\ insecure}{Total\ number\ of\ insecure\ cases} \times 100 \quad (20)$$

Insecure Misclassification (SMC)

$$ISMC(\%) = \frac{No.of\ insecure\ cases\ classified\ as\ secure}{Total\ number\ of\ secure\ cases} \times 100 (21)$$

IV. Results and Discussions

This work presents a static security assessment of the power system using a binary class support vector machine. IEEE standard test systems of 30 and 118 buses, which range both small and large system sizes, are utilized to validate the findings obtained with binary class SVM. On particular buses, the demands for active and reactive power are adjusted from 50% to 150% of their initial values. For every load modification scenario, a single line contingency case was also performed in order to produce more appropriate patterns for static security evaluation. PV buses' minimum and maximum reactive power generation capacities, as well as their active power generation, are all equally scaled according to changes in load demand.

However, security assessments that are based only on the constraints listed in (2) may occasionally experience masking issues [11], [16]. In order to address this issue, the composite security index, which is provided by (11) and discussed in Section 2 of this study, has been employed to evaluate static security. The security states in the SVM binary class problem are categorized as belonging to secure and insecure classes. For all load buses, the alarm and security limits are set at ± 5% and ± 7%, respectively, for voltages that are higher than the nominal value of 1 pu.

The transmission lines' alarm limit is set at 80% of the lines' security limits. The thermal limit of transmission line is considered as security limit for the transmission line. Table I provides specifics about the pattern created and how it was categorized into secure and insecure classes for the test systems under consideration.

TABLE I. Details Of Pattern Generated And its Classification in Secure and Insecure Classes

	IEEE 30 Bus System	**IEEE 118 Bus System**
Total operating Cases	975 (819+156)	9790 (8722+1068)
Total Static Secure Cases (Training + Testing cases)	743 (614+129)	9079 (8091 +988)
Total Static insecure Cases (Training + Testing)	232 (205+27)	711 (631+80)

The total patterns are split into two categories: approximately 10% are used for testing and rest of 90% are used for training. A better misclassification rate and increased classification accuracy result from careful feature selection. The approach of sequential forward selection is employed in this work since it yields the best feature selection outcomes [17]. The dimension reduction for test power systems under investigation using the SFS approach is displayed in Table II.

Tables III and IV present the SVM-based binary classifier performance for the IEEE 30 bus system and IEEE 118 bus system, respectively. Tables IV and IV show that training and testing can yield very strong accuracy levels for two test power systems with extremely low misclassification rates.

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.

TABLE II. REDUCTION IN DIMENSION FOR THE IEEE 30 AND 118 BUS TEST SYSTEMS.

	IEEE 30 bus test system	IEEE 118 Bus test System
Total No. of features	214	952
Features selected	09	60
% Dimension reduction achieved	4.21%	6.30%

It is seen that, for both test power systems, high classification accuracy is achieved in the all the selected patterns (13-17). It is also seen that in the chosen pattern X_2 as in (14) during testing is giving highest accuracy. Additionally, In IEEE 118 bus test power system that has achieved 99.72% accuracy in the chosen pattern X_2 provided in (14).

TABLE III. PERFORMANCE OF SVM-BASED BINARY CLASSIFIER FOR IEEE 30 BUS TEST SYSTEM

Selected Pattern Vector	Training sets	Testing sets			Overall CA (%) (Training and Testing) (%)
	Samples CA (%)	Samples CA (%)	SMC (%)	ISMC (%)	
X_1 as in equation (13)	99.76% (817/819)	98.72% (154/156)	0 % (0/27)	1.55% (2/129)	99.59 % (971/975)
X_2 as in equation (14)	98.90% (810/819)	98.72% (154/156)	3.70 % (1/27)	0.7752% (1/129)	98.87 % (964/975)
X_3 as in equation (15)	99.63% (816/819)	98.72% (154/156)	3.70 % (1/27)	0.7752% (1/129)	99.49 % (970/975)
X_4 as in equation (16)	98.78% (809/819)	98.08% (153/156)	3.70 % (1/27)	1.55% (2/129)	98.67 % (962/975)
X_5 as in equation (17)	99.76% (817/819)	98.72% (154/156)	3.70% (1/27)	0.7752 % (1/129)	99.59 % (971/975)

TABLE IV. PERFORMANCE OF SVM-BASED BINARY CLASSIFIER FOR IEEE 118 BUS TEST SYSTEM

Selected Pattern Vector	Training sets	Testing Sets			Overall CA (%) (Training andTesting) (%)
	Sample CA (%)	Sample CA (%)	SMC (%)	ISMC (%)	
X_1 as in equation (13)	99.85% (8709/8722)	99.53% (1063/1068)	1.25% (1/80)	0.405% (4/988)	99.82% (9772/9790)
X_2 as in equation (14)	99.91% (8714/8722)	99.72% (1065/1068)	2.5% (2/80)	0.101% (1/988)	99.89% (9779/9790)
X_3 as in equation (15)	99.79% (8704/8722)	99.53% (1063/1068)	2.5% (2/80)	0.304% (3/988)	99.77% (9767/9790)
X_4 as in equation (16)	99.89% (8712/8722)	99.62 % (1064/1068)	1.25% (1/80)	0.202% (2/988)	99.87% (9777/9790)
X_5 as in equation (17)	99.83% (8707/8722)	99.53% (1063/1068)	3.75% (3/80)	0.202% (2/988)	99.80% (9770/9790)

The findings also showed that testing in a chosen pattern X_2 presented in (14), for both test power systems, resulting in the maximum accuracy. The findings also showed that, in pattern X_2, the IEEE 30 and 118 test systems, respectively, are the only three misclassifications occur. In static security assessment, Insecure mis classifications are more critical as compare to Secure misclassification. From the results, it can see that only 1 insecure misclassification occurs in the both IEEE standard test system.

V. CONCLUSION

This paper presents a binary class static security assessment of a power system using pattern recognition. By employing the composite security index, the masking problem is eliminated and secure and insecure scenarios that come within the close region of constraints violations are accurately distinguished. SVM is effectively used to create a binary classifier that divides system state into secure and insecure categories. By effectively extracting features to increase classification accuracy and decrease the rate of misclassification, the sequential forward selection method significantly reduces the size of patterns. The classification accuracy achieved in the all variables set cases is around 98.72% in the testing phase for unknown pattern in the IEEE 30 bus test system. The classification accuracy achieved in the all variables set cases is around 99.53 % in the testing phase for unknown pattern in the IEEE 118 bus test system. It can see that binary classifier work even better for complex test system. The performance of the binary classifier has been examined in relation to several sets of power system variables, and it has been discovered that for selected pattern vector X_2 as in equation (14) gives highest accuracy for the both test system. So, we can say that bus voltage, bus angle, and contingency number in the binary form adequately cover information about the condition of the power system. In future, we can try number of combinations of variables to select the greater number of pattern vector to see the effect on binary classifier accuracy.

REFERENCES

[1] K. L. Morison, L.Wang, and P. Kundur, "Power system security assessment." IEEE Power Energy Magazine vol. 2, issue 5, pp. 30–39, 2004.

[2] A.J. Wood, B.F. Wollenberg, and G.B. Sheble, "Power generation, operation, and control", John Wiley & Sons, 2013.

[3] J. Srivani and K.S. Swarup, "Power system static security assessment and evaluation using external system equivalents", International Journal of Electrical Power & Energy Systems, Vol. 30, Issue 2, pp.83–92, 2008.

[4] R. K. Misra and S.P. Singh, "Efficient ANN method for post-contingency status evaluation", International Journal of Electrical Power & Energy Systems, Vol. 32, Issue 1, pp.54–62, 2010.

[5] L. Srivastava and S.N. Singh and J. Sharma, "A hybrid neural network model for fast voltage contingency screening and ranking", International Journal of Electrical Power & Energy Systems, Vol. 22, No. 1, pp.35-42, 2000.

[6] D. Niebur and A.J. Germond, "Unsupervised neural net classification of power system static security states", International Journal of Electrical Power & Energy Systems, Vol. 14, Issue 2-3, pp.233-242, 1992.

[7] N. Hariyanto et al, "Study of static security assessment accuracy results using random forest with various types of training and test datasets", International Journal on Electrical Engineering and Informatics, Vol. 1, pp. 119–133, 2023.

[8] M. Ramirez-Gonzalez, F.R. Segundo Sevilla, P. Korba and R. Castellanos-Bustamante, "Convolutional neural nets with hyperparameter optimization and feature importance for Power system static security assessment", Electric Power Systems Research, Vol. 211, 108203, (2022).

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.

[9] M. Shahidehpour and Y. Wang, "Communication and control in electric power systems: applications of parallel and distributed processing", Wiley-IEEE, New Jersey, 2003.

[10] G.C. Ejebe, H.P.VanMeeteren and B.F. Wollenberg, "Fast contingency screening and evaluation for voltage security analysis", IEEE Transaction on Power Systems, Vol. 3, Issue 4, pp. 1582–1590, 1988.

[11] K. Nara, K.Tanaka, H. Kodama, R.R. Shoults, M.S.Chen, P. V. Olinda, and D. Bertagnolli, "On-line contingency selection for voltage security analysis", IEEE Transaction on Power Apparatus System, Vol. PAS-104, Issue 4, pp. 847–856, 1985.

[12] R.Sunitha, R.K. Sreerama and A.T. Mathew, "A composite security index for on-line steady-state security evaluation", Electric Power Components and Systems, Vol. 39, Issue 1, pp. 1-14,2011.

[13] C.K.Pang, F.S. Prabhakara, A.H. El-Abiad and A.J. Koivo, "Security evaluation in power systems using pattern recognition", IEEE Transactions on Power Apparatus and Systems, pp. 969–976, 1974.

[14] C. Hsu and C. Lin, "A comparison of methods for multiclass support vector machines", IEEE Transaction on Neural Networks, Vol. 13, Issue 2, pp. 415–425, 2002.

[15] J. Min and Y.C. Lee, "Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters", Expert Systems with Applications, Vol. 28, Issue 4, pp. 603–614, 2005.

[16] R. Sunitha, R. Sreerama Kumar and A.T.Mathew "Online Static Security Assessment Module using Artificial Neural Network", IEEE transactions on power systems, Vol. 28, Issue 4, pp.4328-4335, 2013.

[17] S. Kalyani and K.S. Swarup, "Classification and Assessment of Power System Security Using Multiclass SVM" IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) Vol. 41, Issue 5, pp. 753–758, 2011a.

NOMENCLATURE

P_{Ga}	Active power generation at generator at bus a
P_{TL}	Total active load on buses
P_l	Total active loss in the transmission line
P_{Ga}^{min}	Minimum active power generation at bus a
P_{Ga}^{max}	Maximum active power generation at bus a
N_{Gen}	Number of generators
N_{Bus}	Number of buses
$\lvert V_a^{min} \rvert$	Minimum bus voltage limit at bus a
$\lvert V_a^{max} \rvert$	Maximum bus voltage limit at bus a
$\lvert V_a \rvert$	Bus voltage at bus a
P_{jk}	Active power flow in the transmission line $j-k$
P_{jk}^{max}	Maximum active power flow limit in the transmission line $j-k$
V_a^{Des}	Desired bus voltage at bus a
$A_{v,a}^{u}$	Upper alarm bus voltage limit at bus a
$A_{v,a}^{l}$	Lower alarm bus voltage limit at bus a
$S_{v,a}^{u}$	Upper security bus voltage limit at bus a
$S_{v,a}^{l}$	Lower security bus voltage limit at bus a
$A_{MW,b}$	Active power alarm limit in transmission line b
$S_{MW,b}$	Thermal limit in transmission line b
δ_a	Bus angle at bus b
Q_{Ga}	Reactive power generation at bus a
P_{Da}	Active power load at bus a
Q_{Da}	Reactive power load at bus a
Q_{jk}	Reactive power flow in the transmission line $j-k$
Z	Contingency no. in binary

Authorized licensed use limited to: Indian Institute of Technology Gandhinagar. Downloaded on November 05,2024 at 05:50:17 UTC from IEEE Xplore. Restrictions apply.