MultiCraft

International Journal of Engineering, Science and Technology
Vol. 2, No. 3, 2010, pp. 175-185

INTERNATIONAL JOURNAL OF ENGINEERING, SCIENCE AND TECHNOLOGY

www.ijest-ng.com

Supervised fuzzy C-means clustering technique for security assessment and classification in power systems

S. Kalyani[1]*, K.S. Swarup[1]

[1]*Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai - 600036, INDIA*
[*]*Corresponding Author: e-mail:kal_yani_79@yahoo.co.in, Tel +91-044 -22575461, Fax.+91-044 -22574402*

Abstract

Security assessment is an important concern in planning and operation studies of an electric power system. Conventional method of security evaluation is performed by simulation consisting of load flow program and transient stability analysis, consuming long computer time and generating voluminous results. This paper presents a practical Pattern Recognition (PR) approach for security assessment in power systems. The problem of security assessment is focused in two modes, viz., static and transient. Static security pertains to the study of violation of system components when subjected to contingencies like line/generator outages. Transient Security study deals with system dynamic behavior when subjected to severe perturbations like three phase faults. A Supervised Fuzzy C-Means (SFCM) algorithm is proposed in the classification phase of PR system for security assessment. The proposed algorithm is tested on 39 Bus New England and IEEE 57 Bus systems. The classification results of the proposed SFCM classifier is compared with the Method of Least Squares (MLS) and Multilayer Perceptron (MLP) classifiers. The results prove that the former gives high classification accuracy and less misclassification rate compared to the latter, enhancing the feasibility and applicability of SFCM algorithm for on-line security evaluation.

Keywords: Security Assessment, Static Security, Transient Security, Pattern Recognition, Fuzzy C-Means.

1. Introduction

Nowadays, power systems are forced to operate under stressed operating conditions closer to their security limits. Under such fragile conditions, any small disturbance could endanger system security and may lead to system collapse (Niazi *et al*, 2004). Fast and accurate security monitoring method, therefore, has become a key issue to ensure secure operation of the system and forewarn the system operators to take necessary preventive actions in case need arises. Power system security is defined as the ability of the system to withstand unforeseen contingencies without violating normal operating limits.

Security assessment (SA) refers to the analysis performed to determine whether or not a power system can meet specified reliability and security criteria in both steady-state and transient time frames for all credible contingencies. Security analysis may be broadly classified as (i) Static Security and (ii) Transient Security (Shahidehpour *et al*, 2003). Static security evaluation detects any potential overload of a system branch or an out-of limit voltage following a given list of contingencies (Matos *et al*, 2000). Transient security evaluation pertains to system dynamic behavior in terms of rotor angle stability, when subjected to perturbations. Traditional security assessment involves numerical solution of non-linear load flow equations and transient stability analysis for all credible contingencies (Luan *et al*, 2000). Because of the combinatorial nature of problem, this approach requires a huge amount of computation time and hence found infeasible for real time security analysis of practical power system networks.

Pattern Recognition (PR) techniques have shown great importance as a means of predicting the security of large electric power systems, overcoming the drawbacks of traditional approaches (Luan *et al*, 2000; Pang *et al*, 1973). The first step in applying PR technique to the security assessment problem is the creation of an appropriate data set for training and testing purposes. The required data samples called patterns are generated by off-line simulations or obtained from real time occurrences (Pang *et al*, 1973). The next important aspect in achieving good performance is the selection of input features, a subset of pattern variables. Many feature selection algorithms are reported in the literature such as Principal Component Analysis, Entropy Maximization, and

Fisher Discrimination (Jensen *et al*, 2001). In this paper, a forward sequential method is adopted for feature selection process. Using the input features selected, a classification function is designed for accessing system security status.

The design of a suitable classifier in the pattern recognition system is an important concern for on-line security evaluation. Literatures have reported the use of conventional algorithms like linear programming, least squares (Pang *et al*, 1974) and use of expert systems like neural networks, decision trees (Luan *et al*, 2000) for designing the classifier. These existing algorithms seem to work well with linearly separable classes, but not well established on non-linearly separable classes. This led to the idea of applying clustering algorithm for power system security evaluation to handle the problem of non-linear separability between classes. The fuzzy clustering technique of steady state security evaluation proposed by Matos (Matos *et al*, 2000) uses an unsupervised learning, making it infeasible for on-line implementation. This paper presents the application of an active Supervised Fuzzy C-Means (SFCM) clustering algorithm for real time security assessment. A given system operating state is grouped in one of two clusters - Secure/Insecure, according to its membership value. The proposed SFCM algorithm is implemented in New England 39 bus and IEEE 57 bus standard test systems and its performance is compared with Method of Least Squares (MLS) and Multilayer Perceptron (MLP) classifiers. The simulation results prove that the SFCM trained classifier gives high classification accuracy and less false dismissals, enhancing its feasibility for on-line implementation of security evaluation.

2. Security Assessment (SA)

Security Assessment is the process of determining whether and to what extent, a system is 'reasonably' safe from serious interference to its operation (Luan *et al*, 2000). It evaluates the robustness of the system (security level) to a set of contingencies in its present state or future state. This section describes in brief the process of static security assessment and transient security assessment carried out in power system networks.

2.1 Static Security Assessment (SSA):

Static security of a power system addresses whether, after a disturbance, the system reaches a steady state operating point without violating system operating constraints called 'Security Constraints' (Shahidehpour *et al*, 2003; Pang *et al*, 1973; Pang *et al*, 1974). These constraints ensure the power in the network is properly balanced as given by Eq. (1), magnitude of all bus voltage and the MVA flow in the transmission line is within acceptable limits as given by Eq. (2). If any one constraint violates, the system may experience disruption that could result in a 'black-out'.

$$\sum_{i=1}^{N_g} P_{Gi} = P_D + P_{loss} \quad ; \quad P_{Gi}^{\min} \le P_{Gi} \le P_{Gi}^{\max} \tag{1}$$

$$\left|V_k^{\min}\right| \le \left|V_k\right| \le \left|V_k^{\max}\right| \quad ; \quad S_{km} \le S_{km}^{\max} \tag{2}$$

In static security assessment process, the status of the power system is evaluated for various probable contingencies by solving non-linear load flow equations. The contingencies may include outage of a transmission line or a transformer or a generating unit. The load flow is solved for various disturbances and the results are compared with system constraints. The system operating state is labeled as '*Static Secure*' (SS: Binary 1) if all the constraints (1)-(2) are satisfied for a specified contingency. If any one constraint violation is identified, the system state is labeled as '*Static Insecure*' (SI: Binary 0).

2.2 Transient Security Assessment (TSA):

Transient security of a power system addresses whether, after a perturbation, the system proceeds to operate consistently within the limits imposed by the system stability phenomena (Shahidehpour *et al*, 2003; Pang *et al*, 1973; Pang *et al*, 1974). 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 (Hakim, 1992). TSA is a subset of transient stability analysis. Transient stability pertains to rotor angle stability, wherein the stability phenomena are characterized by rotor dynamics under a severe perturbation. The system state is classified as '*Transient Secure*' (TS: Binary 1) if the rotor angle of any generator does not exceed $180^0 - \delta_0$, δ_0 being the rotor angle of slack (reference) generator, after fault clearing instant, under specified transient disturbance. On the contrary, if the rotor angle exceeds $180^0 - \delta_0$, the system state is classified as '*Transient Insecure*' (TI: Binary 0).

3. Application of Pattern Recognition Technique to Security Assessment

Pattern Recognition is an integral part in machine intelligence systems built for decision making. It deals with classification of data objects, referred as '*Patterns*', into a number of categories or classes (Theodoridis *et al*, 1992). The main objective of applying pattern recognition approach to security assessment problem is to reduce on-line computational requirements. This is done at the expense of an extensive off-line simulation, generating sufficient data points. If the separating surface between the distinguishing classes is evaluated as a security function, the system security can be accessed at any point of time. This is the basic

idea of PR approach. The sequence of steps carried out in off-line in applying PR approach to security assessment is shown in the form of a flowchart in Figure 1.

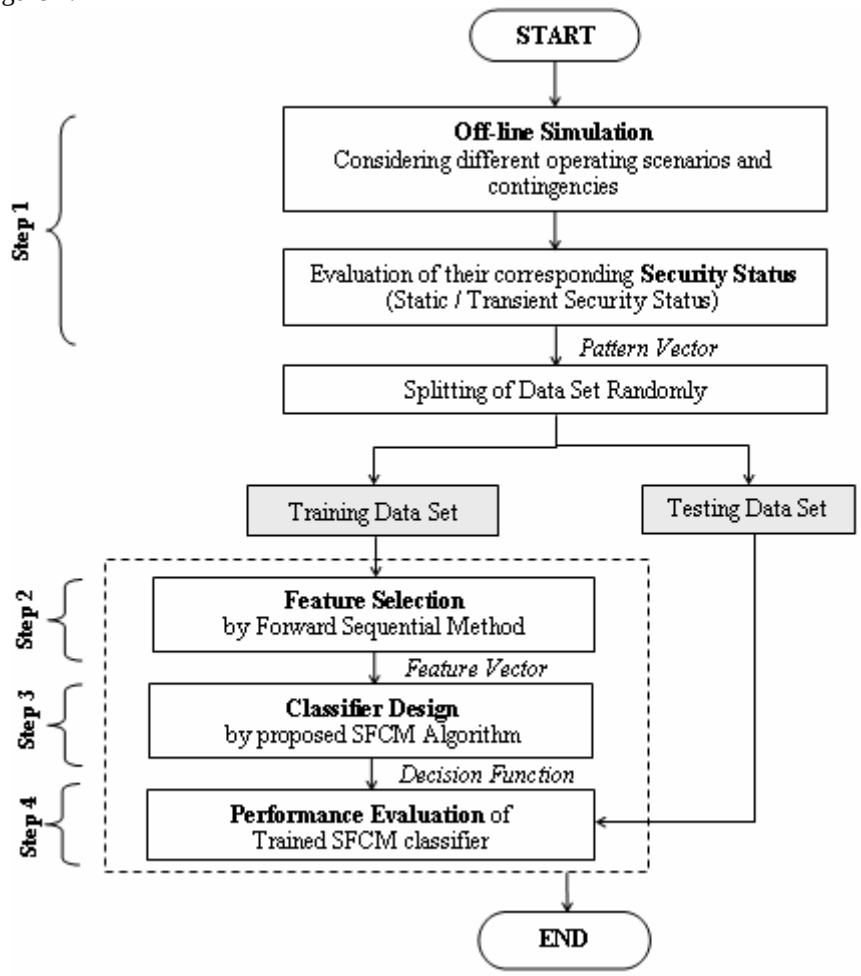

Figure 1. Stages in Design of Pattern Recognition (PR) System for Security Evaluation

As shown in Figure 1, the design of pattern recognition system using the proposed Supervised Fuzzy C-Means (SFCM) algorithm undergoes a series of sequential steps. In this section, we briefly outline the main steps and algorithm of the fuzzy classification scheme. The main stages are as follows:

Step 1: Data Generation (consists of generating pattern vector)
Step 2: Feature Selection (selecting a subset of pattern attributes called features)
Step 3: Classifier Design (devising a decision function called Security Function)
Step 4: Performance Evaluation (Validating and testing the designed classifier)

This section gives a brief description of each of the above stages involved in the design of pattern recognition system for the problem of security assessment.

3.1 Step 1: Pattern (Data) Generation:

The success of pattern recognition relies on a good training set. This set must adequately represent the entire range of system operating states. A large number of characteristic operating points are generated through off-line simulation and the security status is evaluated for each contingency under study. Each operating point is termed as a pattern (Se-Young oh, 1986). Each pattern is characterized by a number of attributes such as load level, voltages, power generation, etc. These attributes form the components of a vector called '*pattern vector*'. Evaluating the security status, each pattern is labeled as belonging to secure/insecure class. The data samples generated in this phase are randomly split into train set and test set.

3.2 Step 2: Feature Selection:

Feature selection reduces the dimensionality of data by selecting only a subset of measured features (predictor variables) to create a model (Weerasooriya *et al*, 1986). The selected features must be capable of giving more useful information to build the classification function. The features form the components of a vector called feature vector Z. Features may be selected by engineering judgment. But such selections will be subjective with the possibility of important variables getting rejected. A common method of feature selection is sequential feature selection, consisting of two components - an objective function called criterion and a sequential search algorithm. In this paper, we use a '*Sequential Forward Selection (SFS)*' method (Theodoridis *et al*, 1992). The criterion which this method seeks to minimize is misclassification for classification models. The SFS method starts with an empty candidate set and adds feature variables sequentially until addition of further variables does not decrease the criterion (minimization of misclassification).

3.3 Step 3: Classifier Design:

Having selected the desired feature subset, the next step in the PR system is to design an efficient classifier for the security assessment problem. There are many training algorithms reported in literature for classifier design. Few of them include least squares, linear programming, back propagation, etc. These algorithms, although less time consuming, were found to give poor classification accuracy. The main requirements of a good classifier are '*high accuracy*' and '*less misclassification*'. This led to the thought of finding a more efficient learning algorithm for classifier design. In this paper, the Supervised Fuzzy C-Means (SFCM) clustering algorithm is identified as a suitable tool for design of classifier in the PR system. This section gives a brief outline of fuzzy clustering and algorithm of SFCM for classification task.

3.3.1 Fuzzy Clustering:

Clustering is a process of partitioning or grouping a set of data objects into a number of clusters such that similar patterns are assigned to one cluster. The measure of similarity or distance between respective patterns is fundamental for any clustering technique (Ross, 2004). Depending on the data and application, different types of similarity measures like distance, connectivity and intensity can be used. These measures control the method of cluster formation. In this paper, Euclidean distance based similarity measure is used for class identification. Fuzzy clustering is a class of algorithm in cluster analysis wherein the allocation of data points to clusters is not 'hard' but 'fuzzy' in the same sense as fuzzy logic. Fuzzy logic is a multi-valued logic derived from fuzzy set theory, proposed by Lofti Zadeh to deal with reasoning that is approximate rather than precise (Ross, 2004).

Fuzzy C Means (FCM) is one of the widely used fuzzy partitioning scheme, originally introduced by Bezdec, as an improvement on earlier clustering methods (Wei-Che Chen *et al*, 2009). FCM is an overlapping data clustering technique wherein each data point, X_k, belongs to a cluster i to some degree specified by a membership grade, u_{ik}. The detailed algorithm of fuzzy c-means clustering is available in Ref (Wei-Che Chen *et al*, 2009). The FCM algorithm outputs a list of cluster centers and membership grades for each point. This information can be used to build a fuzzy inference system by creating appropriate membership functions to represent the fuzzy qualities of each cluster. FCM is an unsupervised learning algorithm, which performs the classification of data samples without utilizing the class label information. A common problem with FCM is that the cluster structure does not necessarily correspond to the classes in the dataset, reducing its classification accuracy and efficiency. Hence, FCM is preferred only when there is no prior information regarding class labels.

3.3.2 Supervised Fuzzy C-Means (SFCM) Clustering:

Class labels always provide a useful guidance during training process, as being done in all the learning methods. Hence, it becomes necessary to use the labeled samples in training phase and unlabeled samples in testing phase to improve the performance of FCM. This idea led to the development of a new algorithm called '*Supervised Fuzzy C-Means (SFCM)*' algorithm, a slight modification of FCM (Hong-Bin *et al*, 2005). The SFCM clustering technique aims to develop classifiers that can utilize both labeled and unlabeled samples. In this method of classification, a known fixed set of categories and category-labeled training data are used to induce a classification function (Li *et al*, 2008). The supervised clustering can group data using the categories in the initial labeled data, as well as extend and modify the existing set of categories to reflect other irregularities in the dataset.

The determination of fuzzy partition matrix U (dividing n data sets into c classes) using Supervised Fuzzy C Means clustering is an iterative optimization procedure. The core of SFCM is to use the labeled data samples to guide the iterative optimization procedure. The objective function of the SFCM optimization problem is defined as:

$$J_m(U,v) = \sum_{i=1}^{c}\sum_{k=1}^{n}\left(u_{ik}\right)^m d_{ik}{}^2 + a\sum_{i=1}^{c}\sum_{k=1}^{n}\left(u_{ik} - f_{ik}\right)^m d_{ik}{}^2 \tag{3}$$

where

U Fuzzy Partition Matrix

v Cluster Center

u_{ik} Membership degree of k^{th} data point belonging to the i^{th} cluster (value between 0 and 1)

d_{ik} Distance measure of k[th] data point from i[th] cluster center

f_{ik} Membership degree of k[th] labeled sample belonging to the i[th] cluster (value is either 0 or 1)

The coefficient 'a' denotes scaling factor and 'm' denotes the fuzzy coefficient. The role of 'a' is to maintain a balance between supervised and unsupervised component within the optimization mechanism and parameter 'm' controls the amount of fuzziness in the classification. The typical value of m is 2 and a=L/n, L denoting the size of labeled samples *(*Li *et al, 2008)*. The function J_m can take a large number of values, the smallest one being associated with best clustering.

Algorithm for SFCM

An effective algorithm for fuzzy classification called iterative optimization procedure is discussed herein. The steps in this algorithm are as follows:

1. Fix the number of clusters c. Initialize membership values of matrix F of size c x n with 0 or 1 in accordance with class labels. Initialize fuzzy partition matrix $U^{(0)}$ with random values between 0 and 1, where U ε M_{fc}.

$$M_{fc} = \left\{ U\big|_{u_{ik}} \in [0,1]; \sum_{i=1}^{c} u_{ik} = 1; 0 < \sum_{k=1}^{n} u_{ik} < n \right\} \tag{4}$$

2. Start the iterative procedure and set the iteration count, t = 1.
3. Calculate the centers (prototypes) of the clusters using the equation (5) given below

$$v_{ij}^{(t)} = \frac{\sum_{k=1}^{n} \left(U_{ik}^{(t-1)}\right)^m Z_{kj}^{(train)}}{\sum_{k=1}^{n} \left(U_{ik}^{(t-1)}\right)^m} \quad ; \quad j = 1, 2.....m \tag{5}$$

$v_i^{(t)}$ is the i[th] cluster center described by m features (m coordinates) and arranged in the vector form represented as $v_i^{(t)} = \left\{ v_{i1}^{(t)}, v_{i2}^{(t)}, \ldots, v_{im}^{(t)} \right\}$. $Z_{kj}^{(train)}$ represents the k[th] data instance corresponding to the m[th] selected feature variable. The data matrix, Z, is the input train feature vector set obtained for SSA / TSA classification process.

4. Calculate the distance, $d_{ik}^{(t)}$, between the i[th] cluster center and k[th] data set (data point in m-space). The distance measure used is *Euclidean Distance* as given by equation (6).

$$d_{ik}^{(t)} = \left\| Z_k - v_i^{(t)} \right\| = \sqrt{\sum_{j=1}^{m} \left(Z_{kj}^{(train)} - v_{ij}^{(t)} \right)^2} \tag{6}$$

5. Update the fuzzy partition matrix, $U^{(t+1)}$, for the next iteration as follows:

$$u_{ik}^{(t+1)} = (1-a) \left[\sum_{j=1}^{c} \left(\frac{d_{ik}^{(t)}}{d_{jk}^{(t)}} \right)^{\frac{2}{m-1}} \right]^{-1} + a\, f_{ik} \quad \forall\, I_k = \phi$$

$$(or)\ \ u_{ik}^{(t+1)} = 0 \quad \forall\ classes\ i\ where\ i \in \tilde{I}_k \tag{7}$$

where

$$I_k = \left\{ i\big|_{2<c<n} ;\ d_{ik}^{(t)} = 0 \right\};\ \tilde{I}_k = \{1, 2, \ldots, c\} - I_k ;\ \sum_{i \in I_k} u_{ik}^{(t+1)} = 1 \tag{8}$$

6. If $\left\| U^{(t+1)} - U^{(t)} \right\| \le \varepsilon$ (ε being iterative accuracy), stop the iteration and output v (cluster center), U (fuzzy matrix); else increment the iteration count, t = t+1 and return to Step 3.

Note: For test set samples, whose class labels are unknown, the fuzzy matrix is updated as follows:

$$u_{ik} = \left[\sum_{j=1}^{c} \left(\frac{\left\| Z_k^{(test)} - v_i \right\|}{\left\| Z_k^{(test)} - v_j \right\|} \right)^{\frac{2}{m-1}} \right]^{-1} \tag{9}$$

where v_i and v_j are values obtained from final cluster center v of the SFCM iterative training algorithm described above.

3.4 Step 4: Performance Evaluation:

The performance of the classifier designed using SFCM training algorithm is rated by evaluating the following measures for train set, test set and combined data set.

(a) Mean Squared Error (MSE)

$$MSE = \frac{1}{n} \sum_{k=1}^{n} \left(E_k \right)^2 \quad ; \quad E_k = \left| DO_k - AO_k \right| \tag{10}$$

where

DO_k Desired output obtained from off-line simulation (data generation)

AO_k *Actual* output obtained from the classifier algorithm designed in PR system

(b) Classification Accuracy (CA)

$$CA(\%) = \frac{No.of\ samples\ classified\ correctly}{Total\ No.of\ samples\ in\ data\ set} \times 100 \tag{11}$$

(c) Misclassification (MC) Rate

(i) Secure Misclassification (SMC) or False Dismissal

$$SMC(\%) = \frac{No.of\ 0's\ classified\ as\ 1}{Total\ No.of\ Insecure\ (0)\ States} \times 100 \tag{12}$$

(ii) Insecure Misclassification (ISMC) or False Alarm

$$ISMC(\%) = \frac{No.of\ 1's\ classified\ as\ 0}{Total\ No.of\ Secure\ (1)\ States} \times 100 \tag{13}$$

In power system security evaluation, the false alarms are not much harmful. In case of false dismissals, failure of control actions may lead to a severe blackout. It is, therefore, important to ensure that false dismissals are kept at minimal. The classification system must be efficiently designed to meet this requirement.

4. Results and Discussion

The proposed SFCM based design of classifier for security assessment is implemented in 39 Bus New England (Pai, *1989*) and IEEE 57 Bus systems (PSTCA). The bus voltage magnitude is limited to the range of 0.90pu - 1.10pu. The generator data and their limits are given in Appendix. The data set required for training and testing are generated by off-line simulation with programs developed in Matlab 7.0 package. We have considered different operating scenarios by varying generation and load from 50% to 200% of their base case value. The variation in generation is limited to their minimum and maximum limits.

4.1. Results of Static Security Assessment:

In Static Security Assessment, single line outages are simulated for each operating condition. For a given operating condition and specified contingency, load flow solution by Fast Decoupled Load Flow method is obtained. The static security status (secure/insecure) is determined for feasible solutions by evaluating the security constraints given by equation (1)-(2). The steady state variables of the load flow solution are recorded as pattern variables X, which includes bus voltage magnitude, bus voltage angle, complex power generation at generator buses, complex power load at load buses and MVA flow in all branches. An optimal subset of pattern vector called '*feature vector (Z)*' is identified by SFS feature selection method. The results of data generation and feature selection phases for static security assessment are shown in Table 1.

The data samples of m features are randomly split into train and test set. The classifier is designed by SFCM algorithm based on train set. Using the resultant cluster centers, the fuzzy partition matrix of test set is determined. The class labels of the test samples are predicted by the maximal membership function value in the fuzzy matrix, U. The fuzzy coefficient 'm' in SFCM algorithm is assumed as 2. The performance of SFCM classifier is shown in Table 2. The results of SFCM classifier is compared with the Method of Least Squares (MLS) and Multilayer Perceptron (MLP) classifiers. The MLS classifier is designed by Multiple Linear Regression technique using the selected input feature set. The MLP classifier, designed using Neural Network toolbox in Matlab

7.0, consists of a hidden layer with 30 neurons of 'tansig' function. The MLP network is trained with Levenberg Marquardt algorithm (Learning rate=0.05, Goal=0.001, Epochs=600).

Table 1. Data Generation and Features of Static Security Assessment

Test Case Studied →	**New England 39 Bus System**	**IEEE 57 Bus System**
Operating Scenarios	531	1378
Static Secure (SS) Classes	330	719
Static Insecure (SI) Classes	201	659
No. of Pattern Variables	153	243
No. of Features Selected	20	22
Dimensionality Reduction	**13.072 %**	**9.054 %**

The classification results of various classifiers show that the SFCM trained classifier gives a fairly high classification accuracy and less secure misclassification rate, compared to MLP or MLS classifiers, as evident from Table 2. The SFCM algorithm is capable of classifying unlabeled class samples (test set) with high accuracy and less SMC rate, as shown highlighted (boldface) in Table 2. This feature is highly important for power system operation, where it is unrealistic to expect that all possible cases will be encountered through off-line simulation. Figure 2 shows the comparison of the performance of classifiers for entire data set, as a bar plot for the test cases studied. As seen from Figure 2, the results of SFCM prove to more encouraging than other classifier algorithms, making it suitable for on-line implementation.

Table 2. Comparative Performance of Classifiers for Static Security Assessment

	Test Case Studied →	**New England 39 Bus System**			**IEEE 57 Bus System**		
	Classifier Type →	**SFCM**	**MLS**	**MLP**	**SFCM**	**MLS**	**MLP**
TRAIN SET	*No. of Samples*	434	434	434	1213	1213	1213
	Classification Accuracy (%)	100.0	70.97	70.27	100.0	63.48	75.43
	Mean Squared Error	0.000	0.291	0.297	0.000	0.365	0.246
	Secure Misclassification (%)	0.000	79.75	81.65	0.000	76.25	51.29
	Insecure Misclassification (%)	0.000	0.000	0.000	0.000	0.000	0.000
	CPU Time (s)	0.340	1.274	3.719	0.420	0.883	17.96
TEST SET	*No. of Samples*	97	97	97	165	165	165
	Classification Accuracy (%)	**87.63**	68.04	83.51	**91.52**	63.03	67.27
	Mean Squared Error	0.124	0.319	0.165	0.085	0.369	0.327
	Secure Misclassification (%)	**20.93**	72.09	37.21	**15.38**	78.21	50.00
	Insecure Misclassification (%)	5.556	0.000	0.000	2.298	0.000	17.24
	CPU Time (s)	0.042	0.013	0.023	0.124	0.002	0.024

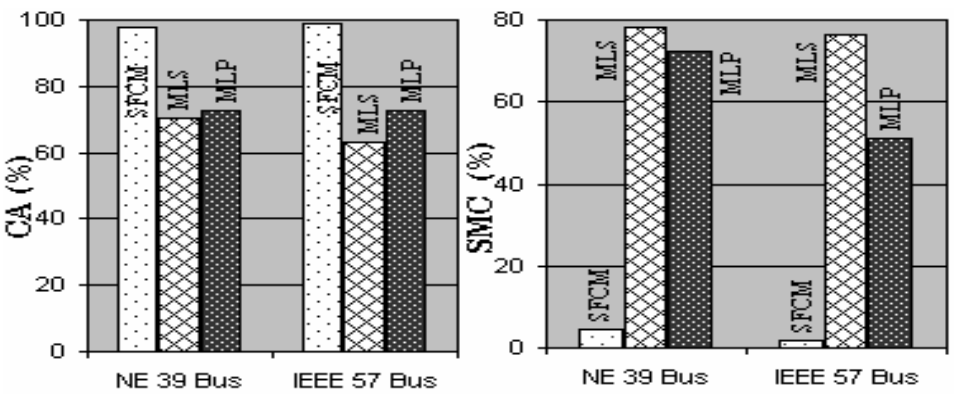

Figure 2. Overall Performance of Classifiers for Static Security Assessment

4.2. Results of Transient Security Assessment:

In transient security assessment process, the static security status of all the operating scenarios is first identified by running load flow program. The operating scenarios which are static insecure (violating one or more of the constraints (1)-(2)) are ignored. Each static secure case is subjected to transient security analysis by simulating transient disturbances (three phase faults) on all lines, one at a time, both near sending and ending buses. The faults are applied at 0 sec and cleared at 0.25 sec (freq. being 60Hz) by tripping the faulted line. The system dynamic equations are solved by numerical integration technique, viz., fourth-order Runge Kutta method and the transient security status is evaluated for each disturbance. If the relative rotor angle of any generator with respect to reference generator exceeds $180^0 - \delta_0$ after fault clearing instant, the corresponding data pattern is labeled as Transient Insecure (0), else classified as Transient Secure (1). A simple classical model with each generator represented by constant voltage behind transient reactance is used in the transient stability simulation.

The steady state variables from static security assessment and the variables pertaining to system dynamic behavior obtained from transient security assessment form the components of pattern vector. The pattern variables are bus voltage magnitude and angle, power generation and load, mechanical input power, electrical output power and relative rotor angle of generators at fault application time and fault clearing time. The size of the pattern vector being large, we identify those variables having higher information content by SFS feature selection method. This, in turn, yields the feature vector (Z) for classifier design. The result of data generation and feature selection phases for transient security assessment is shown in Table 3.

Table 3. Data Generation and Features of Transient Security Assessment

Test Case Studied →		**New England 39 Bus System**	**IEEE 57 Bus System**
SSA	*Operating Scenarios*	31	25
	Static Secure (SS) Classes	**15**	**14**
	Static Insecure (SI) Classes	16	11
TSA	*Operating Scenarios*	1020	1764
	Transient Secure Classes	614	1072
	Insecure Classes	406	692
No. of Pattern Variables		153	198
No. of Features Selected		23	7
Dimensionality Reduction		**15.032 %**	**3.535 %**

Table 4. Comparative Performance of Classifiers for Transient Security Assessment

	Test Case Studied →	**New England 39 Bus System**			**IEEE 57 Bus System**		
	Classifier Type →	**SFCM**	**MLS**	**MLP**	**SFCM**	**MLS**	**MLP**
TRAIN SET	*No. of Samples*	910	910	910	1589	1589	1589
	Classification Accuracy (%)	100.0	68.24	75.27	100.0	71.55	79.55
	Mean Squared Error	0.000	0.318	0.247	0.000	0.285	0.205
	Secure Misclassification (%)	0.000	78.86	59.84	0.000	69.22	49.77
	Insecure Misclassification (%)	0.000	0.000	0.000	0.000	0.000	0.000
	CPU Time (s)	0.348	0.609	10.93	0.359	0.369	8.992
TEST SET	*No. of Samples*	110	110	110	175	175	175
	Classification Accuracy (%)	**90.91**	85.45	81.82	**86.86**	77.21	70.28
	Mean Squared Error	0.091	0.146	0.182	0.131	0.223	0.297
	Secure Misclassification (%)	**33.33**	53.33	66.67	**25.64**	100.0	58.98
	Insecure Misclassification (%)	0.000	0.000	0.000	9.558	0.000	21.32
	CPU Time (s)	0.098	0.002	0.015	0.044	0.002	0.015

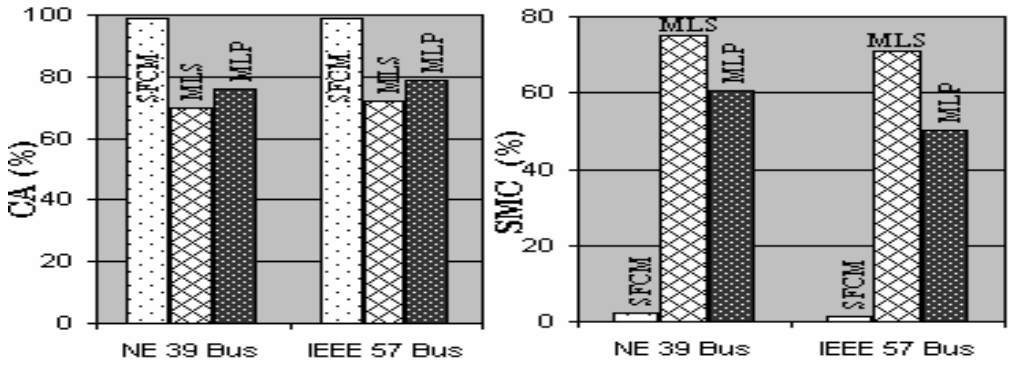

Figure 3. Overall Performance of Classifiers for Transient Security Assessment

The classification function is designed based on the train set of the feature vector. The results of classifiers obtained during training and testing phases for transient security assessment is shown in Table 4. The SFCM results are compared with MLP and MLS classifiers. The MLP and MLS classifier are designed and trained as discussed in previous section. Figure 3 shows the performance comparison of the classifiers as a bar plot for the test cases studied. It can be seen from Table 4 and Figure 3 that the SFCM classifier gives a better result in terms of high classification accuracy and less misclassification rate than the other classifiers. Furthermore, the time taken by SFCM classifier is quite acceptable, making it feasible for on-line security monitoring system. Data robustness, overload detection, voltage monitoring and contingency analysis are widely studied in security assessment. The proposed classifier is useful for all these analysis.

5. On-line Implementation

The security system developed based on PR approach using SFCM algorithm is feasible for on-line implementation. In on-line mode, real time system data of the selected feature variables are measured and system static / transient security status is accessed as shown in Figure 4. The implementation procedure shown in Figure 4 is a general idea and applicable for both SSA and TSA. When applied for SSA, real time power flow data measurements are used as input to SFCM classifier. In case of TSA application, real time dynamic variables like machine angle, electrical power are fed as input to classifier algorithm. For any new operating point, use of equation (9) gives the degrees of membership to each class. The new point is assigned to the class corresponding to maximal membership function value. This process involves very little computation effort, i.e., only manipulation of equation (9) and hence suitable for on-line security evaluation process. Moreover, the classification of operating points among all classes with degrees of membership helps the operator to take appropriate control decisions, especially in case of critical operating points.

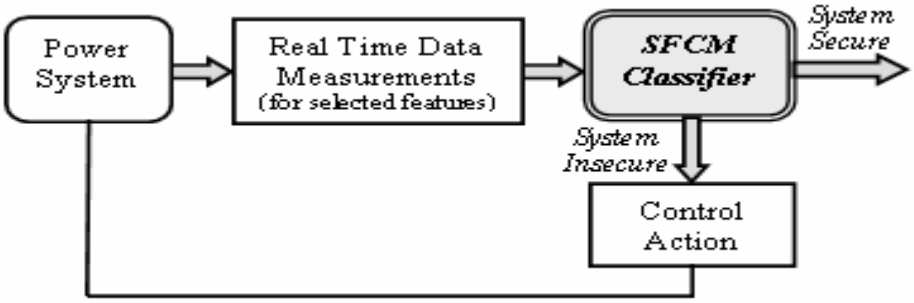

Figure 4. On-line Implementation of Security Assessment Process

6. Conclusions

The application of pattern recognition approach for classifying the input feature vector representing the power system states is presented. The classifier in the PR system is developed by a fuzzy clustering algorithm called '*Supervised Fuzzy C-Means* (SFCM)'. Training set vectors generated from off-line simulations are presented as inputs to SFCM algorithm, which uses active supervised learning to adapt its weight vectors (cluster centers). The proposed SFCM-PR model was tested on New England 39 Bus and IEEE 57 Bus test systems for both static and transient security assessment. Simulation results show that high accuracy classifiers with less false dismissal rate are realizable with the SFCM algorithm. Further, the SFCM algorithm involves less computation effort, making it suitable for real time security evaluation. Future work will focus on further improving the successful classification level by combining SFCM with machine learning algorithms like Support Vector Machines.

Appendix

Generator Data:

New England 39 Bus System

Gen No.	Bus No.	P_{min} (MW)	P_{max} (MW)	R_a (pu)	X_d' (pu)	H (s)
1	30	0	350.00	0.00	0.0310	42.00
2	31	0	1150.00	0.00	0.0697	30.30
3	32	0	750.00	0.00	0.0531	35.80
4	33	0	732.00	0.00	0.0436	28.60
5	34	0	608.00	0.00	0.1320	26.00
6	35	0	750.00	0.00	0.0500	34.80
7	36	0	660.00	0.00	0.0490	26.40
8	37	0	640.00	0.00	0.0570	24.30
9	38	0	930.00	0.00	0.0570	34.50
10	39	0	1100.00	0.00	0.0060	500.00

IEEE 57 Bus System

Gen No.	Bus No.	P_{min} (MW)	P_{max} (MW)	R_a (pu)	X_d' (pu)	H (s)
1	1	0	575.88	0.00	0.2500	4.000
2	2	0	100.00	0.00	0.2000	3.000
3	3	0	140.00	0.00	0.2000	3.000
4	6	0	100.00	0.00	0.2500	5.000
5	8	0	550.00	0.00	0.2000	2.500
6	9	0	100.00	0.00	0.2000	3.000
7	12	0	410.00	0.00	0.2500	5.000

Acknowledgement

The first author likes to thank the Management and Principal of KLN College of Engineering, Madurai for giving an opportunity to undergo Doctoral programme at IIT Madras under Quality Improvement Programme (QIP) scheme. The authors also thank Indian Institute of Technology Madras for providing necessary facilities and resources to carry out this research work.

References

Hakim, H., 1992. Application of Pattern Recognition in Transient Security Assessment, *Electric Power Components and Systems*, Vol.20, Issue 1, pp.1-15.

Hong-Bin, Jie Yang, Xiao-Jun Liu and Kuo-Chen Chou, 2005. Using Supervised Fuzzy Clustering to Predict Protein Structural Classes, *Biochemical and Biophysical Research Communication*, Vol. 334, pp. 577-581.

Jensen, Craig A., Sharkawi, El-Mohamed A., and Marks, Robert J., 2001. Power System Security Assessment using Neural Networks: Feature Selection using Fisher Discrimination, *IEEE Transactions on Power Systems*, Vol.16, No.4, pp.757-763.

Li, C., Liu, L. and Jiang, W., 2008. Objective Function of Semi-Supervised Fuzzy C-Means Clustering Algorithm, *IEEE International Conference on Industrial Informatics*, Daejeon, Korea, July 13-16, pp. 737-742.

Luan, W.P., Lo, K.L., and Yu, Y.X., 2000. ANN Based Pattern Recognition Technique for Power System Security Assessment, *IEEE International Conference on Electric Utility Deregulation and Restructuring and Power Technologies 2000*, City University, London, pp. 197-202.

Matos, M.A., Hatziargyriou, N.D. and Pecas Lopes, J.A., 2000. Multi-contingency Steady State Security Evaluation using Fuzzy Clustering Techniques, *IEEE Transactions on Power Systems*, Vol.15, No.1, pp.177-182.

Niazi, K.R., Arora, C.M., and Surana, S.L., 2004. Power System Security Evaluation using ANN: Feature Selection using Divergence, *Electric Power Systems Research*, Vol.69, No. 2-3, pp.161-167.

Pai, M.A., 1989. Energy Function Analysis of Power System Stability, *Kluwer Academic Publishers*.

Pang, C.K., Kovio, A.J., and El-Abiad, A.H., 1973. Application of Pattern Recognition to Steady State Security Evaluation in a Power System, *IEEE Trans. on Systems, Mans & Cybernetics*, Vol. SMC-3, No.6, pp.622-631.

Pang, C.K., Prabhakara, F.S., El-Abiad, A.H., and Kovio, A.J., 1974. Security Evaluation in Power Systems using Pattern Recognition, *IEEE Transactions on Power Apparatus & Systems*, Vol. PAS-93, pp.969-976.

Power System Test Case Archive. Available at http://www.ee.washington.edu/research/pstca/

Ross, Timothy J., 2004. Fuzzy Logic with Engineering Applications, *John Wiley & Sons*, Second Edition.

Se-Young Oh, 1986. Pattern Recognition and Associative Memory Approach to Power System Security Assessment, *IEEE Transactions on Systems, Mans & Cybernetics*, Vol. SMC-16, No. 1, pp. 62-72.

Shahidehpour, S.M. and Wang, Y., 2003. Communication and Control in Electric Systems: Applications of Parallel and Distributed Processing, *Wiley-IEEE*, John Wiley & Sons.

Theodoridis, S. and Koutroumbas, Konstantinos., 2003. Pattern Recognition, *John Wiley & Sons*, Prentice Hall, Third Edition.

Weerasooriya, S., and El-Sharkawi, M.A., 1992. Feature Selection for Static Security Assessment using Neural Networks, *IEEE International Symposium on Circuits & Systems*, California, May 10-13, pp. 1693-1696.

Wei-Che Chen, and Ming-Shi Wang, 2009. A Fuzzy C-Means Clustering-Based Fragile Watermarking Scheme for Image Authentication, *Expert Systems with Applications*, Vol. 36, pp. 1300-1307.

Biographical notes:

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 Electrical 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. He received his Bachelors Degree in Electrical Engineering from Jawaharlal Nehru Technological University, Kakinada Andhra Pradesh and Masters Degree in Power Systems Engineering from Regional Engineering College, Warangal. He received his PhD degree from Indian Institute of Science, Bangalore. His areas of research are artificial intelligence, knowledge-based systems, computational intelligence, soft computing, and object modeling and design of power systems. He is a Senior Member of IEEE since 2003.

Received January, 2010
Accepted March 2010
Final acceptance in revised form March 2010