ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Fuzzy Logic Composite Criteria Based Power System Security Assessment Using ANN and SVM

P. Satyendra Kumar[1], S. Lalitha Kumari[2]

PG Student [PID], Dept. of EEE, G.M.R Institute of Technology, Rajam, Andhra Pradesh, India[1]

Assistant Professor, Dept. of EEE, G.M.R Institute of Technology, Rajam, Andhra Pradesh, India[2]

electrical.satyendra@gmail.com; lalliyuvaraj@gmail.com

ABSTRACT: Power is the basic necessity for the economic development of the country. Many functions necessary to present-day living grind to halt when the supply of energy stops. It is practically impossible to estimate the actual magnitude of the part that energy has played in the building up of present-day civilisation. There is need to maintain continuity of power. So assessment of power system security is important issue. Security Analysis is the process of testing power system safety limits, to determine up to what extent the system is safe. Here power system security is divided into three classes' viz.; secure, critically secure and insecure. In this paper, a multi class Support vector machine (SVM) classifier algorithm is used to classify the patterns. These patterns are generated for IEEE 30 bus by Fuzzy logic composite criteria at different generating and loading conditions. The simulation results of SVM classifier is compared with other artificial intelligence tools.

KEYWORDS: System Security, Patterns, Support Vector Machine, Artificial intelligence.

I.INTRODUCTION

Power system security Assessment is a major concern in real time planning and operation of an electrical power system [1].When severe penetration occurs, controlling and protecting of power system is important, which restores the system to normal state and preventing system collapse [2]. Power system security is defined as ability of system to withstand contingency when fault occurs. So, classifying and assessing power system security is important electrical issue. For classification and assessment of power system security a power full tool is required. There is need to generate patterns for assessing system security. Traditionally these patterns are generated by running load flow analysis. But this method is time consuming and less accurate [3].

In recent years, the use of artificial intelligence (AI) techniques has been proposed for security evaluation. A fuzzy logic composite criterion is an artificial intelligence tool used for generating patterns. From the generated patterns we can identify credible contingency from large list of contingencies and rank them based on severity. Based on system severity we can take necessary control action.

Many power system problems are solved by pattern classification approach. Classification is done by training the data set. From this we can assess system security in a short period of time. With the generated patterns we can cathorgize System security into secure, critically secure and insecure. By this we can determine system is in normal, alert and emergency condition [4]. So, for classification artificial intelligence tools like artificial neural network (ANN) and Support vector machine (SVM) are applied form which we can assess system security.

Artificial intelligence is the branch of computer science concerned with making computers behave like humans. The term was coined in 1956 by John Mc Carthy at the Massachusetts institute of technology. Artificial intelligence includes the following area of specifications such as pattern classification; speech recognition and robotics etc.... Therefore for pattern classification artificial intelligence tool like artificial neural network (ANN) and support vector machine (SVM) has been proposed. Artificial neural network (ANN) requires an extensive training process and a complicated design procedure. ANN is god in interpolation but not so good in extrapolation. Because of these

DOI: 10.15662/ijareeie.2015.0408013

drawbacks there is need to use a more efficient classifier algorithm for pattern classification for evaluating the system security. Therefore a multiclass support vector machine classifier is designed and implemented for security evaluation and classification [4].

Support vector machine is a supervised learning algorithm widely used in the field of machine learning and pattern classification. By linear or non-linear separation surface in the input space classification is achieved [5]. Based on the training set classification function is designed. To construct an optimal hyper plane SVM use iterative training algorithm which minimize error function? Here for assessing system security a multiclass support vector machine is used [6].

II.POWER SYSTEM SECURITY ASSESSMENT

The term ‘security’ as defined by NERC (1997) is the ability of the electric system to withstand sudden disturbance such as electric circuit or unanticipated loss of system element. Security assessment can be determined based on contingency ranking. A set of most probable contingencies is first specified for security assessment. This set may include outage of lines, sudden variation in loads/generation, and due to transformer tap setting [1]. Based on the value of security index power system security is divided into three classes secure, critically secure and insecure. The security level is defined based on the computation of term called Fuzzy logic composite criteria (FLCC). The system is said to be secure if the power generation and bus voltages are well within their limits [3]. The Fuzzy Logic Composite Criteria (FLCC) is computed by calculating the overall security index of line loadings, voltage profile, voltage stability indices, real/ reactive power outputs and transformer tapping’s [8].

III.PROPOSED SYSTEM

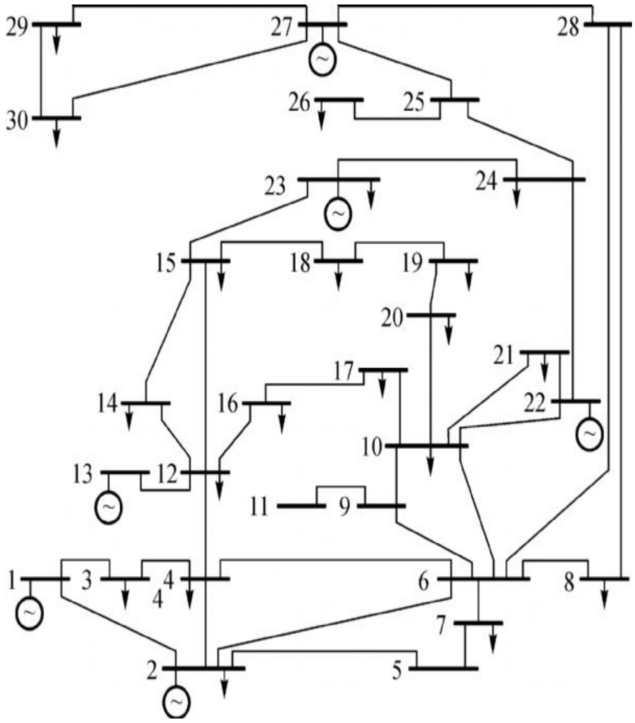

Fig. 1Single line diagram of IEEE-30 bus system

The proposed system consists of 30 buses out of which 6 are generation buses, 21 are load buses and 3 are SVC (static var compensator) buses and 37 transmission lines. For this proposed system operating conditions are changed to test the system. The violations of thermal limits of transmission lines and bus voltage limits are the main concerns of security analysis. System is said to be secure if the bus voltage magnitudes and real/reactive power generation of generator buses are well within their limits, with no occurrence of line overloads [2]. By making line outage there is possibility of occurring contingency. Number of contingency condition has been created, and each condition is applied to Fuzzy logic to obtain security index at each condition. Security index is computed by calculating the overall security index of line loadings (OSI$_{LL)}$, voltage profile (OSI$_{VP}$), voltage stability index (OSI$_{VSI}$), reactive power output (OSI$_{QG}$), real power outputs (OSI$_{PG}$) and transformer tap settings (OSI$_{TP}$) Based on index value obtained class labels' are been categorized [8].

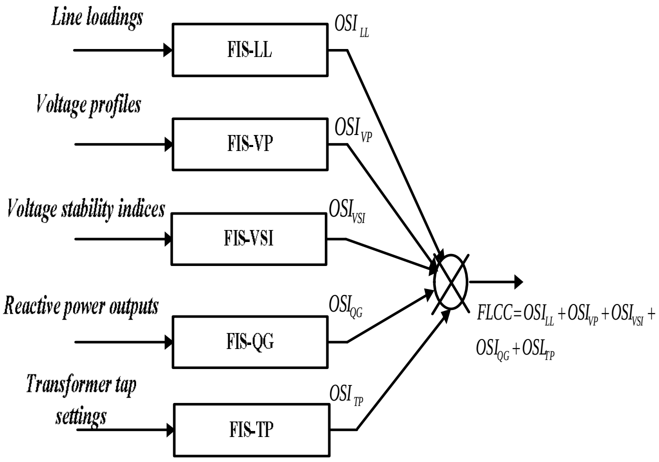

Fig. 2 Parallel operated fuzzy inference system

The Fuzzy logic composite criteria (FLCC) is computed by calculating the overall security index of line loading (OSI$_{LL}$), voltage profile (OSI$_{VP}$), voltage stability index (OSI$_{VSI}$), reactive power output (OSI$_{QG}$) and transformer tap settings (OSI$_{TP}$). The equations of OSI$_{LL}$, OSI$_{VP}$, OSI$_{VSI}$, OSI$_{QG}$ and OSI$_{TP}$ are shown below:

$$OSI_{LL} = \sum W_{LL}\ SI_{LL} \qquad (1)$$
$$OSI_{VP} = \sum W_{VP}\ SI_{VP} \qquad (2)$$
$$OSI_{\ VSI} = \sum W_{VSI}\ SI_{VSI} \qquad (3)$$
$$OSI_{TP} = \sum W_{TP}\ SI_{TP} \qquad (4)$$
$$OSI_{QG} = \sum W_{QG}\ SI_{QG} \qquad (5)$$

Where W= Weight coefficient for a severity index and SI= Severity index of a pre/post-contingent quantity.

$$FLCC= OSI_{LL}+OSI_{VP}+OSI_{VSI}+OSI_{QG}+OSI_{TP}$$

IV.CLASSFICATION OF POWER SYSTEM SECURITY

The severity of each system is tested under normal conditions by creating a line outage. The line that is mostly affected by line outage can be identified by creating this contingency. Contingency is known as an unpredictable condition in the power system. The impact of occurrence of contingencies should be evaluated. Contingency analysis means detecting post contingency operational limits violations. Primary purpose of maintaining power system security is to keep power system operation under stable conditions such that the single line failure does not lead to cascade tripping ad overall blackout. This purpose makes system to operate in a secure way [7]. Fuzzy logic is used for analysing contingencies. Patterns are generated by creating different line outages and changing generation for an IEEE 30 bus system and they are tabulated below. These patterns are generated by executing Mat lab programs for FLCC.

TYPE OF CLASS	OSILL	OSIVP	OSI VSI	OSI QG	OSI TP	FLCC
Class A	318.75	216	96	54	126	811.7
Class A	325	216	96	54	126	817.9
Class A	337.5	216	96	54	126	830.5
Class A	343.75	216	96	54	126	836.7
Class A	350	216	96	54	126	842.9
Class A	352.60	216	96	54	126	845.6
Class A	356.25	216	96	54	126	849.2
Class B	362.5	216	96	54	126	855.5
Class B	375	216	96	54	126	868.0
Class B	381.25	216	96	54	126	874.2
Class B	387.5	216	96	54	126	880.5
Class B	387.5	216	96	54	126	880.5
Class B	393.75	216	96	54	126	886.7
Class B	400	216	96	54	126	892.9
Class C	412.5	216	96	54	126	905.5
Class C	337.5	292.5	96	54	126	907.0
Class C	425	216	96	54	126	918.0
Class C	431.25	216	96	54	126	924.2
Class C	437.49	216	96	54	126	930.4
Class C	362.5	216	96	145	126	946.4
Class C	368.75	304.78	120	54	126	974.5

Table 1 Pattern for IEEE 30-Bus System for Line Outage

Based on FLCC values obtained, system security is ranked and classes are specified. System security is divided into three classes:-

Class Category/Label	FLCC
Class A	800 to 850
Class B	850 to 900
Class C	Above 900

After specifying classes Artificial Intelligence tools is applied to separate different classes

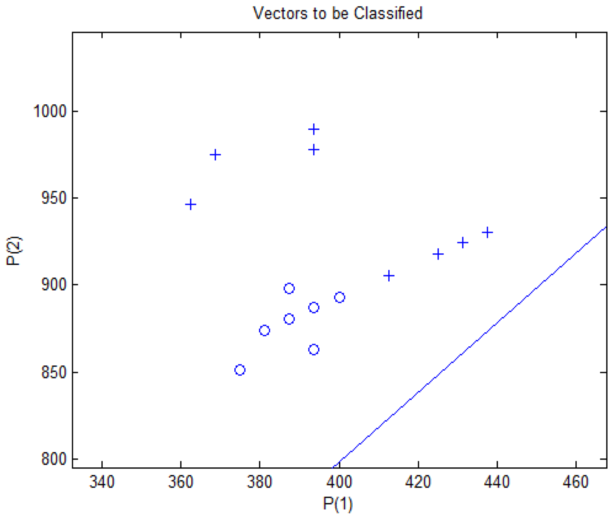

Fig. 3 Classification of system security using ANN

The simulation results obtained by artificial intelligence tools are shown in Figs. 3-10. By using artificial neural network pattern are not classified successfully. So for classifying patterns support vector machine has been used [8]. For identifying the support vectors we use fast iterative algorithm for given set of points. This algorithm makes repeated passes over the data to satisfy Karush-Kuhn-Tucker (KKT) constraints. Our algorithm works by maintaining a candidate support vector set.

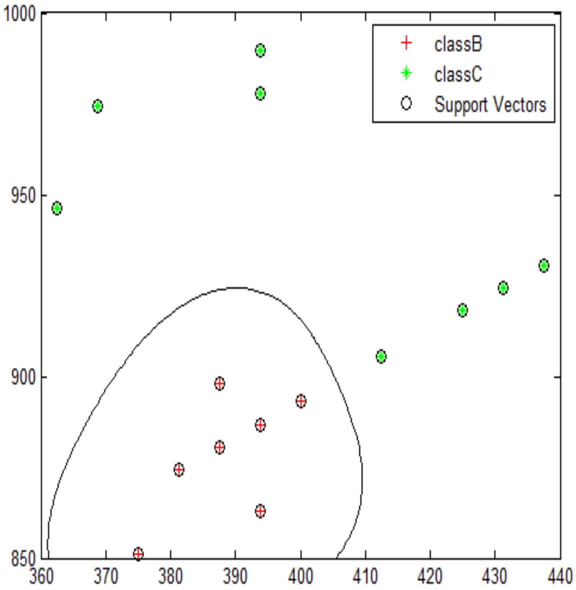

Fig. 4 Classification of system security using SVM for class B & C

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

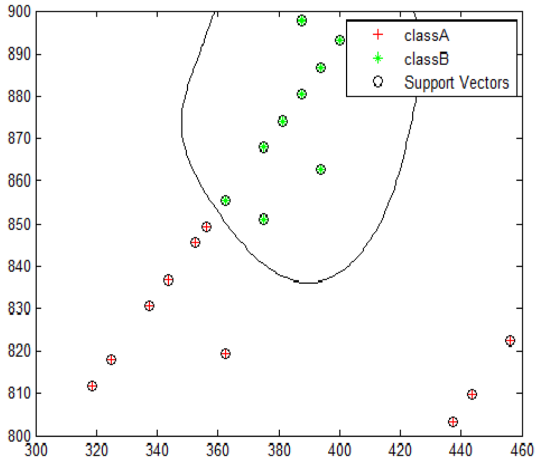

Fig. 5 Classification of system security using SVM for class A & B

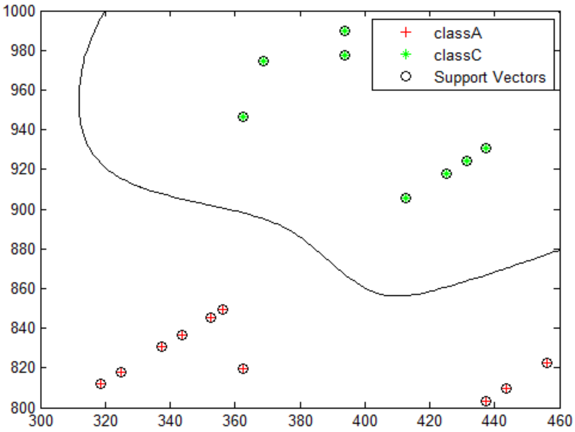

Fig. 6 Classification of system security using SVM for class A & C

CLASS	OSILL	OSIVP	OSI	OSI	OSI	FLCC
			VSI	QG	TP	
Class A	331.25	216	96	54	126	824.25
Class A	350	216	96	54	126	843.001
Class B	368.75	216	96	54	126	861.751
Class B	406.2496	216	96	54	126	899.251
Class C	424.9996	216	96	54	126	918.001
Class A	331.25	216	96	54	126	824.251
Class C	462.4996	216	96	54	126	955.501
Class B	406.2496	216	96	54	126	899.251
Class C	437.4996	216	96	54	126	930.501

Table 2 Patterns FOR IEEE 30-Bus System for Generation Change

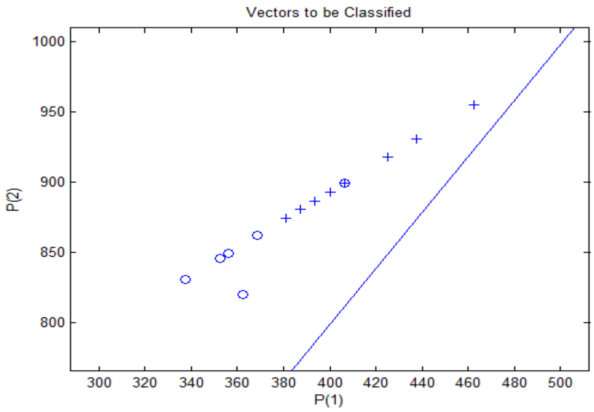

Fig. 7 Classification of system security using ANN

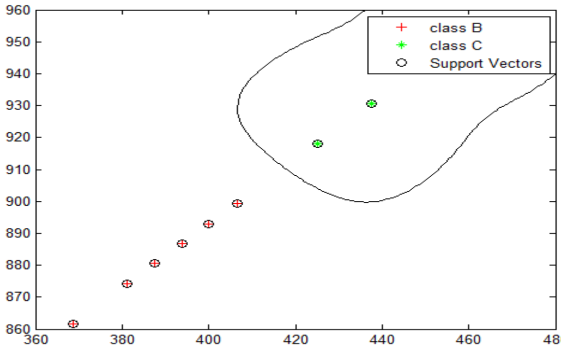

Fig. 8 Classification of system security using SVM for class B & C

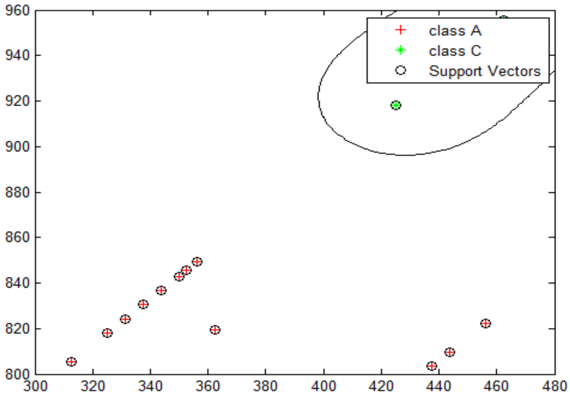

Fig. 9 Classification of system security using SVM for class A & C

V. PROPOSED ALGORITHM

```
Simple SVM
Candidate Support vector = {closest pair from opposite classes}
While there are violating points do
Find a violator
```

```
Candidate Support vector = candidate Support vector U violator
If any $\alpha p < 0$ due to addition of c to S then
Candidate Support vector = candidate Support vector \ p
Repeat till all such points are pruned
End if
End while
```

For better classification we use Support vector machine (SVM) which uses iterative algorithm as mentioned above. Pattern classification by using support vector machine (SVM) is shown below.

VI.CONCLUSION

This study explores the application of SVM for power system security assessment. By comparing results of Neural Network and SVM we can conclude SVM has less misclassification rate and high accuracy. The classification of the system security gives an indication about security level of the system to the operator and helps to take necessary control actions at the appropriate time for preventing system collapse.

REFERENCES

[1] S. Kalyani and K. Shanti Swarup; “Power System Security Assessment Using Binary SVM Based Pattern Classification,” IEEE Transactions world Academy of Science, Engineering and Technology vol: 3 2009-04-28.

[2] S. Kalyani and K. Shanti 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, no. 5, September 2011.

[3] S. Lalitha Kumari and B. Sesha Sai; “Static Security Analysis Using Support Vector Machine,” International Journal of Engineering Research & Technology (IJERT) ISSN:2278-0181 Vol. 3 Issue 9, September-2014.

[4] S. Kalyani and K. Shanti Swarup; “Static Security Assessment in Power System Using Multiclass SVM with Parameter Selection Methods” International Journal of Computer Theory and Engineering, Vol. 5, No. 3 June 2013.

[5] S.V.N. Vishwanathan, M. Narasimha Murty “A Simple SVM Algorithm” Dept. of Comp. Sci. and Automation, Indian Institute of Science, Bangalore -560 012, INDIA

[6] Sami Ekici “Support Vector Machine for Classification and Locating Faults on Transmission Lines,” Elsevier 12(2012)1650-1658.

[7] Toshi Mandloi Anil Jain, “A Study of Power System Security and Contingency Analysis,” International Journal of Scientific Research Engineering & Technology (IJSRET) ISSN: 2278-0882 Vol. 3 Issue 4, July-2014.

[8] P. Satyendra Kumar S. Lalitha Kumari; “SVM Based Power System Security Assessment Using Composite Criteria” International Journal of Emerging Trends in Engineering and Development Issue 5 Vol.3 (April-May 2015) ISSN 2249-6149.

[9] B. Biswal, M.K.Biswal, P.K.Dash, S.Mishra “Power quality event characterization using support vector machine and optimization using advanced immune algorithm” Elsevier-2012.

[10] Bidyut Ranjan Das, Dr. Ashish Chaturvedi “Static Security analysis in Real time using ANN” IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676 Volume 5, Issue 1 (Mar. - Apr. 2013), PP 50-54

BIOGRAPHY

P. Satyendra Kumar pursuing M. Tech (Power and Industrial Drives) Dept of Electrical and Electronics Engineering from GMR institute of technology, Andhra Pradesh, India