International Journal of Modern Computer Science (IJMCS)
Volume 2, Issue 6, December, 2014
ISSN: 2320-7868 (Online)

Development of an Online Static Power System Security Assessment Module Using Artificial Neural Networks in 118-Bus Test System

Lekshmi M
Research Scholar,
Jain University, Bangalore

Sowmya
M.Tech Student (Power System), EEE, AIT
Bangalore

Dr. M.S. Nagaraj
HOD &Professor, Dept of EEE,
Bappuji Institute of engineering & technology, Davengare, India

Abstract: Contingency analysis is an important task in today's power system. Fast and accurate contingency analysis is some of the major issues. In this paper two types of Artificial Neural Network (ANN) viz. Multilayer feed forward neural network (MLFFN) and Radial basis function network (RBFN) are used to implement online static security assessment. Newton Raphson (NR) method is done on an IEEE 118-test bus system and Composite Security Index (CSI) is calculated. Loads are varied from the base case values and for each load condition, line flow and bus voltages are calculated using a model based on the NR load flow method for training an ANN with the help of back propagation algorithm. Expected range of load variation and randomly selected 20-contingencies are tested in the training ANN model. The results obtained by the above ANN methods are matched with NR methods. The CSI is found out for various loads and contingencies in MLFFN and RBFN. The computation time required for MLFFN and RBFN is compared with NR method and found that RBFN is using less computation time average of 35.67291s.

Keywords: Contingency analysis, Composite Security Index, Multilayer-Feed Forward Network, Radial Basis Function Network, Newton Raphson method

I. INTRODUCTION

Security refers to the degree of risk in a power system's ability to survive imminent disturbances (contingencies) without interruption to customer services. It relates to robustness of the system to imminent disturbances and, hence, depends on the system operating condition as well as the contingent probability of disturbances [1]. The power system security assessment can be divided into three major functions which are system monitoring, contingency analysis and security control. System monitoring provides up-to-date information such as voltage, currents, power flows and the status of the circuit breaker through the telemetry system. From this system monitoring, operator can easily identify the system in the normal state or in abnormal condition. On the other hand contingency analysis is carried out to evaluate the outage events in the power system and it is in a critical part in the security assessment [2]. During the insecure condition, security control will take the preventive actions to ensure the system is back to secure condition. Sunitha R et al. in 2011-13 [10 &18] have proposed a single composite security index to indicate bus voltage and line flow limit violations which is calculated Newton Raphson load flow technique. The index is defined in such a way that it completely eliminates the masking problem, and provides a better definition of security.In which the secure state is indicated by an index value "0", while a value greater than "1"indicates an insecure state. Index values lying between "0" and "1" indicate the alarm limit. It also avoids the difficult task of selecting the weights. This index works a projection of the multiple factors into a hyperbole region as a scalar value, considering both power flow and bus voltage violations, making it more robust. An overview is given in the following screen.

The main objective of this paper is developing an online static security assessment (OSSA) module in order to overcome the large computational overhead of real time static security assessment procedure. The proposed module utilizes the composite security index (PI_c) for the fast and accurate static security evaluation. The proposed OSAA module utilizes an ANN module that computes the composite security index for a particular loading and contingency condition. The training of the ANNs involves the development of composite security index for a wide range of loading conditions, for different contingencies. In this work a multi-layer feed forward network (MLFFN) and radial basis function network (RBFN) based OSSA modules are developed for IEEE 118-bus test system.

II. ONLINE STATIC SECURITY ASSESSMENT MODULE USING ANN

In the proposed approach, power system security assessment against unplanned line outages are done by utilizing the high adaption capability of ANNs, as these are better suited to deal with nonlinear problems. Fig. 1 shows the structure of the proposed OSSA module. The real and reactive power generation at the generator buses (P_G, Q_G), real and reactive power loads on all load buses (P_D, Q_D), the voltage magnitudes and phase angle δ for all buses are used for describing the system operating point and are chosen as the input for the security assessment module. This module is

 ISSN: 2320-7868 (Online)

capable of providing the security index for the given operating condition.

The proposed OSSA module utilizes an ANN module for which the loading condition and contingency are the inputs and composite security index as the output. The contingencies are represented as a binary number in which "0" represents the outage of the corresponding line. Two types of ANNs viz. MLFFN and RBFN are used to implement the proposed OSSA module, details of which are given in the following subsections.

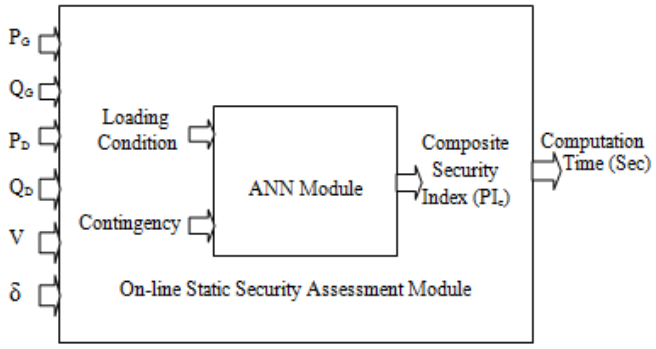

Fig 1. Structure of online static security assessment (OSSA) module

A. Multilayer Feed Forward Network (MLFFN)

In this work MLFFN has two hidden layers which have nodes with nonlinear activation function . This is proposed for power system security assessment. Each node in one layer connects with a certain weight to every other node in the following layer. Real and reactive power demand at various load buses and binary numbers representing contingency are taken as the inputs to the MLFFN. The number of inputs mainly depends upon the topology of the system under consideration. The activation used in the hidden layers is the "hyperbolic tangent" and at the output layer, the linear function is used. The network is trained with "Levenberg-Marquardt" back propagation algorithm [11] due to its good convergence properties. In order to obtain the optimum number of neurons in the hidden layer, the number of neurons in the first hidden layer is varied from 3 to 10 and the second hidden layer from 10 to 20. For each change, in the number of hidden units, the ANN is trained and the mean square errors are compared. The number of neurons with minimum mean square error is selected for the final structure of MLFFN.

B. Radial Basis Function Network (RBFN)

RBFN is a special class of feed forward neural network and consists of an input layer, a hidden layer and an output layer. The network is capable of performing nonlinear mapping of the input features into the output. The hidden layer consists of neurons with Gaussian activation functions, while the output layer neurons are with linear activation function. During training, all the input variables are fed to the neurons in the hidden layer directly through interconnections with unity weights and only the weights between hidden and output layers are to be trained. Thus, RBFN gives faster convergence than the conventional MLFFN.

C. Training and Testing pattern

The purpose of the ANN technique for power system security assessment, related to the system's stability, is described by the following procedure: The probable contingencies are listed out. In this work only the line outages are considered. The training data are generated by varying loads randomly between 50 and 150 percentage of their base case value. For each loading condition the pre and post-outage bus voltages and line flows are calculated with a full iteration of Newton Raphson (NR) load flow analysis. For each case, the composite security index is calculated using (5) by taking the value of "n" as "2". Nearly 90 training sets are generated from the test system under consideration. The trained module is tests for various random loading conditions, within the expected range of load variations. Various loading condition in terms of P_G, Q_G, P_D, Q_D, , δ and randomly selected contingencies are taken as the input for the trained ANN module. It can provide composite security index value for all contingencies identified as those with index value greater than one. The contingencies can also be ranked in the order of severity based on the composite security index PI_c.

III. COMPOSITE SECURITY INDEX

In this paper the composite security index (CSI) defined in terms of both line flow and bus voltage limit violations. Two types of limits are defined for bus voltages and line loading, namely the security limit and the alarm limit. The security limit is the maximum limit specified for the bus voltages and the line flows. The alarm limit adjacent to the security limit, which gives an indication of closeness to the limit violations. It is also possible to treat the constraints on the bus voltage and the line flow as soft constraints, thereby the violation of these constraints, if not excessive, may be tolerated for a short period of time.

It is assumed that the desirable voltages at each bus is known and is represented as V_i^d. The upper and lower alarm limits and security limits of bus voltages are represented as F_i^u, F_i^l, V_i^u and V_i^l respectively. The normalized upper and lower voltage limit violations beyond the alarm limits are defined as in (1):

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

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

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

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

Where V_i is the voltage magnitude at bus i. For each upper and lower limit of bus voltages, the normalization factor is defined in (2):

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

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

 ISSN: 2320-7868 (Online)

According to (1) and (2), it can be observed that the ratio of (d/g) will give a value of "0" if the value of the bus voltage is in between the upper and lower alarm limit. If the value of the bus voltage vector is above the upper alarm limit or below the lower alarm limit, it gives a value greater than "0". Moreover, if the value bus voltage is above the upper security limit or below lower security limit, the value of (d/g) vector is in between "0" and "1", it is said to be in the alarm limit. Similar explanations holds good for power flows as well.

For the line flows, the limit violation vectors d_p and the normalization vector g_p are defined in the similar manner. Since only the maximum limits are required to be specified for the power flow through each line, two types of upper limits are specified for each line: the alarm limit P_F and the security limit P_P. The normalized power flow limit violation vectors for each line j can be defined as in (3):

$$d_{p,i} = \frac{[|P_i| - P_{F,i}]}{Base\ MVA}; \quad \text{if } |P_j| > P_{F,i}$$

$$d_{p,j} = 0 \quad ; \text{ if } |P_j| \leq P_{F,j} \tag{3}$$

Where is the absolute value of the power flow through the line j.The normalization factor for each line j is defined in (4):

$$g_{p,j} = \frac{[P_{P,j} - P_{F,j}]}{Base\ MVA} \tag{4}$$

For an N-bus, M-line system, there are (N + M) dimensional normalized limit violation vectors of both bus voltages and line flows. The concept of hyper-ellipse inscribed within the hyper-box is used for constructing the scalar valued composite security index (CSI) PI_c from the vector valued limit violation vectors [10] and it is defined in (5) as

$$PI_c = \left[\sum_i \left(\frac{d^u_{v,i}}{g^u_{v,i}}\right)^{2n} + \sum_i \left(\frac{d^l_{v,i}}{g^l_{v,i}}\right)^{2n} + \sum_j \left(\frac{d_{p,j}}{g_{p,j}}\right)^{2n}\right]^{\frac{1}{2n}} \tag{5}$$

Where "n" is the exponent used in the hyper ellipse equation. The value of "n" is chosen as "2", because the approximation of hype-box for the hyper-ellipse has not improved beyond "n"=2 [10].

IV. TESTS AND RESULTS

The proposed method has been tested with IEEE 118-Bus test system. The aim is to develop an online static security assessment module using the MLFFN and RBFN network architecture is discussed in the following subsection.

IEEE 118-Bus test System

The OSSA using MLFFN and RBFN are developed for IEEE 118-bus test system. The system consists of 54 generators and 117 transmission lines and 9 transformers. The single line diagram of the system is as shown in Fig. 2.

All line outages, except the lines which are the only line connected to a generator bus, are considered and simulated for system security evaluation. To calculate the composite security index, both alarm and security limits are to be chosen for each bus voltage. For PV buses the specified bus voltage is taken as the desired bus voltages and for PQ buses it is assumed to be "1 p.u". For line flows, 80% of the specified thermal limit is chosen as the alarm limit.

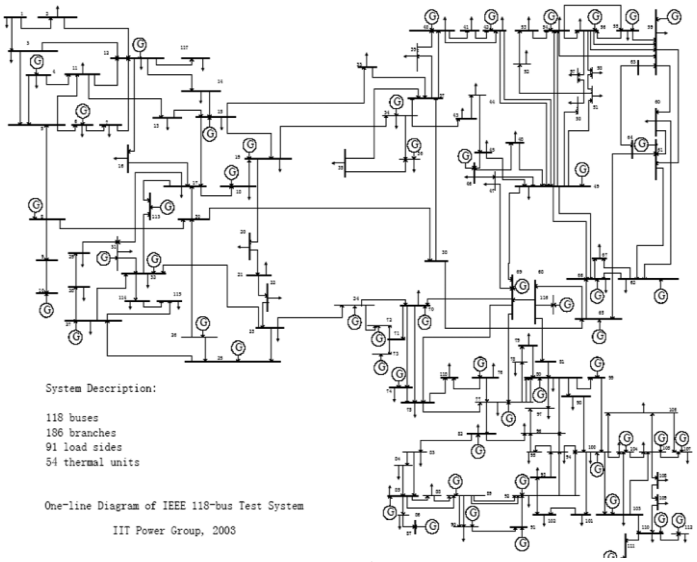

Fig 2. Single line diagram of IEEE 118-bus test system

To develop the proposed OSSA module for IEEE 118-bus system, the training sets are generated for the proposed ANN architectures by the composite security index for different contingencies considering random loading conditions within the stipulated load ranges. The training parameters used for both MLFFN and RBFN architectures, to get best converge characteristics. The performances of the trained MLFFN, RBFN and the performance of the proposed OSSA module are presented in the following subsections.

1) MLFFN Based OSSA: The structure of MLFFN developed for the proposed OSSA consists of the real and reactive power loads and the binary number which represents the contingency as the inputs and the corresponding composite security index as the output. The number of neurons in the hidden layers, chosen with minimum mean square error is 3 to 10 respectively, for the respective hidden layers. Fig. 3 shows the variation of mean square error (MSE) with reference to the number of epochs obtained for training the MLFFN network. It is shown that the MSE obtained for IEEE 118-bus test system is 1.78738×10^{-28}.

2) RBFN Based OSSA: The RBFN is also trained using the same training set that is developed for MLFFN. In this case, the number of neurons in the hidden layer is equal to the number of training sets. For evaluating the performance, the composite security indices obtained with trained RBFN is compared with those computed using (5) based on NRLF analysis.

Once the ANNs are trained, the composite security index values for different loading conditions with different contingencies obtained with proposed MLFFN and RBFN architecture are compared with that obtained using (5) which is based on Newton Raphson load flow (NRLF) analysis. For base load, light load conditions like 80% and 90% of base load and heavy load condition like 110% of the base load, 20 contingencies are selected randomly and numbered as shown in Table I.

For each case, the composite security indices obtained with trained MLFFN and RBFN network and that calculated using

(5) are plotted against the contingency number are as shown in the Figs 3 to 10. It is observed that the trained RBFN is capable of computing the index values as accurate when

Contingencies	Composite Security Index Using	Composite Security Index Using	Composite Security Index Using
54-55	0.316829	0.31682	0.31682
104-105	0.338557	0.33855	0.33855
69-3	0.280161	0.28016	0.28016
40-41	0.255192	0.25519	0.25519
4-11	0.749008	0.74900	0.74900
82-83	0.310203	0.31020	0.31020
77-78	1.237381	1.23738	1.23738
68-116	0	0	0
66-67	1.238325	1.23832	1.23832
49-54	0.36294	0.36294	0.36294
8-30	0.412901	0.41290	0.41290
74-75	3.527503	3.52750	3.52750
88-89	0.656026	0.65602	0.65602
49-50	0.361829	0.36182	0.36182
48-49	0.339538	0.33953	0.33953
55-56	0.329791	0.32979	0.32979
89-92	0.341313	0.34131	0.34131
80-96	0.245825	0.24582	0.24582
106-107	0.241387	0.24138	0.24138
98-100	0.511457	0.51145	0.51145

compared to the MLFFN as that by NRLF analysis. The computation time required for NR, MLFFN and RBFN for different loading condition is as shown in Table II.

In Fig. 3-8 the (d/g) ratio is playing a crucial role in developing a higher composite security index and hence contingency at a particular bus number. This means that the bus where there is a spike in contingency situation shall be given attention. This is happening in all types of load conditions. This ratio is consistently high at contingency number 10-14.

The alarm limit for specific bus number could be matched with specified voltage thereby reducing the value ratio d/g. This might help to indicate a mechanism of less contingent bus number in case of variation of load. Ofcourse it should not affect the CSI of the other contingency number.

Among NR, MLFFN AND RBFN networks, the ANN algorithm used in RBFN gives the output with less time compared to other two. This signifies a superiority of the Radial Basis Function Network (RBFN).

Table I
Randomly Selected Contingencies for Testing The Mlffn And Rbfn For Different Loading Conditions

Contingency	Base load	80% of base load	90% of base	110% of base
1	54-55	89-92	77-80	49-66
2	104-	49-66	101-	100-
3	69-3	75-77	1-3	25-27
4	40-41	17-31	15-19	68-
5	4-11	49-51	80-99	38-37
6	82-83	93-94	50-57	35-37
7	77-78	81-80	103-	100-
8	68-	56-59	88-89	89-90
9	66-67	49-69	77-82	15-19
10	49-54	80-96	47-49	4-5
11	8-30	11-12	23-25	100-
12	74-75	71-73	22-23	26-30
13	88-89	4-11	30-17	40-41
14	49-50	54-56	55-56	77-80
15	48-49	40-42	100-	37-40
16	55-56	100-103	61-62	59-60
17	89-92	4-5	80-98	2-12
18	80-96	91-92	56-59	12-
19	106-	27-115	48-49	24-70
20	98-	75-118	54-59	55-56

SIMULATION RESULTS

1. Base load condition

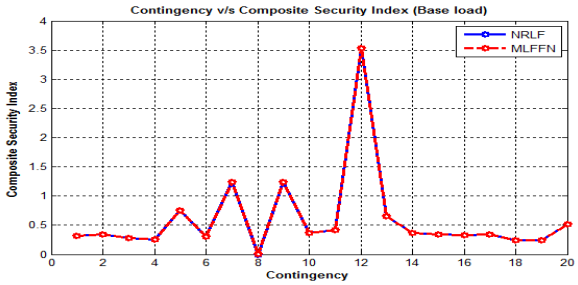

Fig 3. Composite security indices for MLFFN and NR (base load)

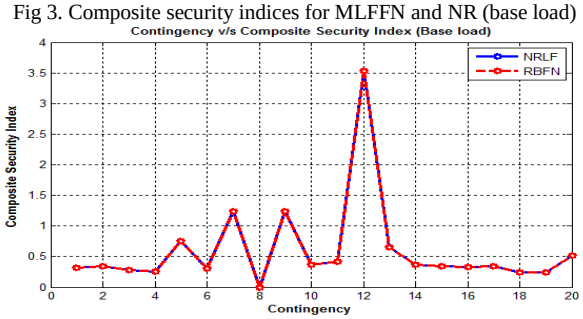

Fig 4. Composite security index for RBFN and NR (base load)

2. 80% of base load condition

Contingencies	Composite Security Index Using NR	Composite Security Index Using MLFFN	Composite Security Index Using RBFN
89-92	0.722018	0.733568	0.722018
49-66	0.970269	0.649853	0.970269
75-77	0.683757	0.693446	0.683757
17-31	0.607762	0.649853	0.607762
49-51	1.08375	1.048001	1.08375
93-94	0.979495	0.879439	0.979495
81-80	0.991451	0.649853	0.991451
56-59	1.105715	1.106771	1.105715
49-69	0.685869	0.688877	0.685869
80-96	0.995688	1.059431	0.995688
11-12	1.095611	1.093583	1.095611
71-73	0	0.649853	0
4-11	5.789486	6.05932	5.789486
54-56	1.914565	1.900708	1.914565
40-42	0.434738	0.649853	0.434738
100-103	0.590697	0.592107	0.590697
4-5	1.74633	1.743933	1.74633
91-92	0.90385	0.895149	0.90385
27-115	0.985954	0.971602	0.985954
75-118	6.589455	6.28447	6.589455

ISSN: 2320-7868 (Online)

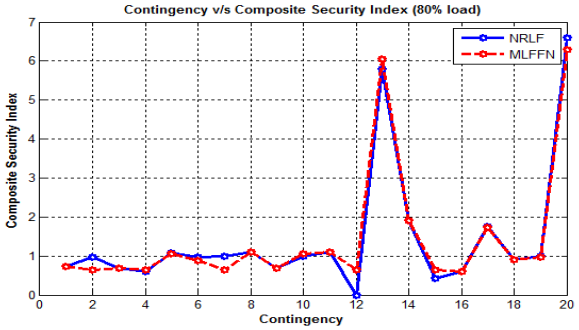

Fig 5. Composite security indices for MLFFN and NR (80% of base load)

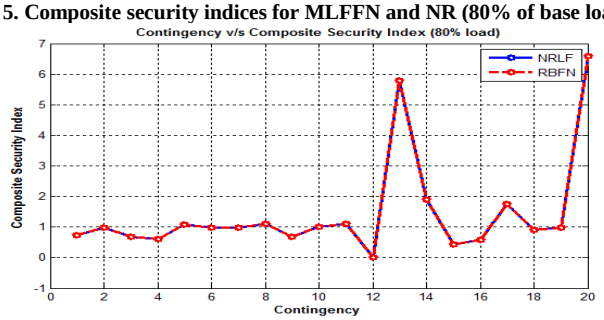

Fig 6. Composite security index for RBFN and NR (80% of the base load)

3. 90% of the base load condition

Contingencies	Composite Security Index Using	Composite Security Index Using MLFFN	Composite Security Index Using RBFN
77-80	1.321545	1.321683	1.321545
101-102	0.422049	0.422039	0.422049
1-3	0.442453	0.442543	0.442453
15-19	0.319954	0.319971	0.319954
80-99	0.396701	0.396707	0.396701
50-57	0.409115	0.409102	0.409115
103-105	0.399874	0.399855	0.399874
88-89	3.360424	3.360433	3.360424
77-82	0.377177	0.377189	0.377177
47-49	0.317792	0.317518	0.317792
23-25	2.222307	2.222303	2.222307
22-23	1.670785	0.439543	1.670785
30-17	1.031272	1.031276	1.031272
55-56	0.440335	0.440426	0.440335
100-101	0.352423	0.352425	0.352423
61-62	0.288712	0.288758	0.288712
80-98	0.4996	0.499596	0.4996
56-59	0.399466	0.399272	0.399466
48-49	0.410456	0.410455	0.410456
54-59	0.377624	0.377593	0.377624

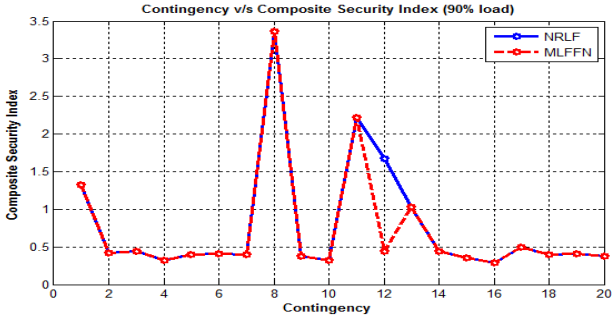

Fig 7. Composite security indices for MLFFN and NR (90% of base load)

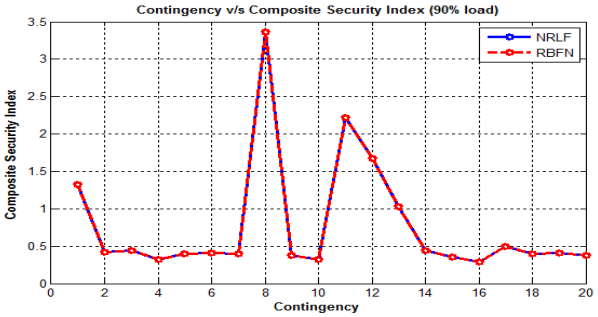

Fig 8. Composite security index for RBFN and NR (90% of the base load)

4. 110% of the base load condition

Contingencies	Composite Security Index Using NR	Composite Security Index Using MLFFN	Composite Security Index Using RBFN
49-66	0.484892	0.484892	0.484892
100-104	4.501788	4.501788	4.501788
25-27	4.319959	4.319959	4.319959
68-116	0	0	0
38-37	6.398665	6.398665	6.398665
35-37	0.279376	0.279377	0.279376
100-103	3.283608	3.283608	3.283608
89-90	0.424165	0.424165	0.424165
15-19	0.328915	0.328914	0.328915
4-5	0.480289	0.480288	0.480289
100-106	0.411443	0.411444	0.411443
26-30	0.447263	0.447263	0.447263
40-41	1.159949	1.159949	1.159949
77-80	0.307782	0.307782	0.307782
37-40	0.275972	0.275972	0.275972
59-60	5.841	5.841	5.841
2-12	0.253189	0.25319	0.253189
12-112	0	0	0
24-70	0.299889	0.299889	0.299889
55-56	3.800609	3.800609	3.800609

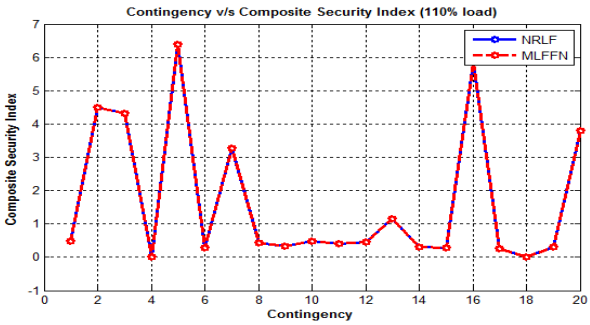

Fig 9. Composite security indices for MLFFN and NR (110% of base load)

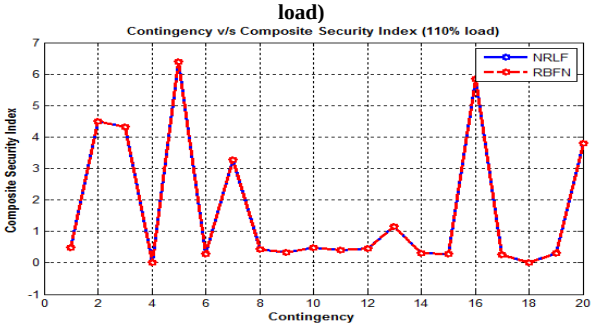

Fig 10. Composite security index for RBFN and NR (110% of the base load)

 ISSN: 2320-7868 (Online)

TABLE II
COMPUTATION TIME REQUIRED FOR NR, MLFFN AND RBFN FOR DIFRRENT LOADING CONDITIONS

	Base load	80% of base load	90% of base load	110% of base load
NR	74.012428 s	72.42567 s	68.125934 s	76.890492 s
MLFFN	50.817632 s	46.212928 s	29.890058 s	44.361361 s
RBFN	35.772090 s	36.546622 s	32.058471 s	35.188185 s

V. CONCLUSION

The effectiveness of the proposed OSSA module is demonstrated on IEEE 118-bus test system in terms of accuracy of computation and reduction in computation time required for static security assessment. Two types of ANN are used viz. MLFFN and RBFN. Average computation time required for four different loading conditions using MLFFN, RBFN and NR methods are 42.82049s, 35.67291s and 72.86363s respectively. Proposed OSSA based on RBFN architecture is capable of accurately assessing the security of the system against outages significantly faster than the conventional techniques.

REFERENCES

[1] K. Morison, L. Wang, and P. Kundur, "Power system security assess- ment," IEEE Power and Energy Mag., vol. 2, no. 5, pp. 30–39, Sep./ Oct. 2004.

[2] K. Morison, "Power system security in the new market environment: Future directions," in Proc. IEEE PES Winter Meeting, 2000, pp. 78–83.

[3] L. H. Hassan, M. Moghavveni, Haider A.F. Almurid, O. Steinmayer, "Current state of neural networks applications in power system monitoring and control," Electrical Power and Energy systems 51(2013), pp 134-144.

[4] H.M. Khattab, A.Y. Abdelaziz, S.F. Mekhamer, M.A.L Badr, "Static security assessment using a probabilistic neural network based classifier," OJEEE, vol (3)-vol (4), Ref. no-W11-0019, pp 454-461.

[5] J.Jasni, M.Z.A. Kadir, "Static power system security assessment via artificial neural network," JATIT, Sep. 2011, vol. 31, No. 2, pp 119-128.

[6] B.R. Das, Dr. A. Chaturvedi, "Static security analysis in real time using ANN," IOSR-JEEE, vol. 5, Issue 1, Mar/ Apr. 2013, pp 50-54.

[7] T. A. Mikolinnas and B. F. Wollenberg, "An advanced contingency selection algorithm," IEEE Trans. Power App. Syst., vol. PAS-100, no. 2, pp. 608–617, Feb. 1981.

[8] H. Song and M. Kezunovic, "Static analysis of vulnerability and se- curity margin of the power system," in Proc. PES IEEE Transmission and Distribution Conf. Expo., T&D, May 2006, pp. 147–152.

[9] C. Subramani, S.S. Dash, M.A. Bhaskar, M. Jagdeshkumar, "Simulation technique for voltage stability analysis and contingency ranking in power systems," ACEEE, vol. 2, No. 5, Nov. 2009, pp 263-267.

[10] Sunitha R.,R.SreeramaKumar,andA.T.Mathew,"Acomposite security index for on-line static security evaluation," Elect. Power Compon. Syst., vol. 39, no. 1, pp. 1–14, Jan. 2011.

[11] V. S. Vankayala and N. D. Rao, "Artificial neural network and their application to power system—A bibliographical survey," Elect. Power Syst. Res., vol. 28, pp. 67–69, 1993.

[12] H.H. Yan, J.C. Chow, R. Fischl, R.X. Chen, "Power system security assessment using a hybrid expert system/ neural network architecture," IEEE 1992, pp 1713-1716.

[13] Y. Mansour, E. Vaahedi, M.A. Sharkawi, "Large scale dynamic security screening and ranking using neural networks," IEEE transactions on power systems, vol. 12, No. 2, May 1997, pp 954-960.

[14] K. S. Swarup and P. B. Corthis, "ANN approach assesses system se- curity," IEEE Comput. Applicat. Power, vol. 15, no. 3, pp. 32–38, Jul. 2002.

[15] K. L. Lo, L.J. Peng, J.F. Macqueen, A.O. Ekwue, D.J.Y. Cheng, "Fast real power contingency ranking using counterpropogation network," IEEE Transaction on power systems, vol. 13, No. 4, Nov. 1998, pp 1259-1264.

[16] R. Fischl, "Application of neural networks to power system security: Technology and trends," in Proc. IEEE World Congr. Computational Intelligence, Jul. 1994, vol. 6, pp. 3719–3723.

[17] S. Varshney, L. Srivastava, M. Pandit, "ANN based integrated security assessment of power system using parallel computing," Elsevier, Electrical power and energy systems 42 (2012), pp 49-59.

[18] Sunitha R.,R.SreeramaKumar, and A.T.Mathew,"Online Static Security Assessment Module Using Artificial Ne9ural Networks," IEEE TRANSACTIONS ON POWER SYSTEMS, vol. 28, no. 4, (2013), pp 4328-4335