Neural network approach to power system security analysis

Bidyut Ranjan Das Author\(^1\), and Dr. Ashish Chaturvedi Author\(^2\),
\(^{1,2}\) School Of Technology, CMJ University, ASCSA, Arni University

**ABSTRACT:**
Contingency analysis of a power system is a major activity in power system planning and operation. In general an outage of one transmission line or transformer may lead to over loads in other branches and/or sudden system voltage rise or drop. The traditional approach of security analysis known as exhaustive security analysis involving the simulation of all conceivable contingencies by full AC load flows, becomes prohibitively costly in terms of time and computing resources. A new approach using Artificial Neural Networks has been proposed in this paper for real-time network security assessment. Security assessment has two functions the first is violation detection in the actual system operating state. The second, much more demanding, function of security assessment is contingency analysis. In this paper, for the determination of voltage contingency ranking, a method has been suggested, which eliminates misranking and masking effects and security assessment has been determined using Radial Basis Function (RBF) neural network for the real time control of power system. The proposed paradigms are tested on IEEE 14 – bus and 30 – bus systems.

**Key words:** Input here the part of 4-5 keywords.

I. INTRODUCTION
Security refers to the ability of the system to withstand the impact of disturbance (contingency). The system is said to be secure if no security limit is seriously violated in the event of contingency. The process of investigating whether the system secure or insecure in a set of proposed contingencies is called Security Analysis.

The three basic elements if real-time security analyses are, Security monitoring, Security assessment. The problem of predicting the static security status of a large power system is a computationally demanding task [2] and it requires large amount of memory. In online contingency analysis, it has become quite common to screen contingencies by ranking them according to some severity index. Which is calculated solely as a measure of limit violations?. The methods developed are known as “ranking methods”. In this paper, for the determination of voltage contingency ranking, a method has been suggested, which eliminates misranking and masking effects and security assessment has been determined using Radial Basis Function (RBF) neural network for the real time control of power system. The proposed paradigms are tested on IEEE 14-bus and 30-bus systems.

II. ARTIFICIAL NEURAL NETWORKS
Artificial neural networks (ANN) are massively parallel inter connected networks of simple elements known as artificial neurons and their connectivity is intended to interact with the objects of real world, in a similar manner as the biological nerves systems do.

The simple neuron model is shown in fig(a). $\sum$ unit multiplies each input ‘x’ by a weight ‘w’ and sums the weighted inputs. The output of the figure is $\text{NET} = x_1w_1 + x_2w_2 + \ldots + x_nw_n$ ; $\text{OUT} = f(\text{NET})$
2.1) Basic features of ANNs are:
1. High computational rates due to the massive parallelism.
2. Fault tolerance.
3. Training the network adopts itself, based on the information received from the environment
4. Programmed rules are not necessary.
5. Primitive computational elements.

2.2) Radial basis function networks:

The Radial Basis Function is similar to the Gaussian function, which is defined by a center and a width parameter. The Gaussian function gives the highest output when the incoming variables are closest to the center apposition and decreases monotonically as the rate of decrease.

Where \(X = \) an input vector
\(u_i = \) weight of vector of hidden layer neuron I
\(D_i^2 = (x - u_i) \cdot (x - u_i), x \) and \(u \) are column vectors

The weights of each hidden layer neuron are assigned the values of input training vector. The output neuron produces the linear weighted summation of these,
\[ y = \sum h_i w_i \]

Where \(w_i = \) weight in the output layer

III. NETWORK OPERATION

The network has two operating modes, named, training and testing. During training the adjustable parameters of the network (\( u, \sigma \), and output layer matrix \( w \)) are set so as to minimize the average error between the actual network output and desired output over the vectors in a training set. In the testing phase, input vectors are applied and output vectors are produced by the network.

IV. TRAINING OF THE RBF NETWORK

A) Computation of RBF parameters:
1). Initialize the center of each cluster to a randomly selected training pattern.
2). Assign each training pattern to the nearest cluster. This can be accomplished by calculating the Euclidean distances between the training patterns and the cluster centers.
3). When all the training patterns are assigned, calculate the average position for each cluster center. Then they become new cluster centers.
4). Repeat steps 2) and 3) until the cluster centers do not change during the subsequent iterations.

b). Calculation of RBF unit widths

When the RBF centers have been established, the width of each RBF unit can be calculated. The width of any RBF unit selected as the root mean square distance to the nearest p, RBF units, where p is a design parameter for the RBF network. For the unit I, it is given by
\[ \sigma_i = \left[ \frac{1}{p} \sum_{j=1}^{p} \sum_{k=1}^{v} \left( X_{kj} - X_{kj} \right)^2 \right]^{1/2} \]
Neural network approach to power system security analysis

Where \( X_{ki} \) and \( X_{kj} \) are the \( k \)th entries of the centers of \( i \)th and \( j \)th hidden units.

c). Calculation of activation

The activation level \( O_j \) of hidden unit \( j \) is
\[
O_j = \exp \left[ - \left( X - W_j \right)^2 / 2\sigma_j^2 \right]
\]

The activation level \( O_k \) of an output is determined by
\[
O_k = \sum W_{kj} O_j
\]

V. STATIC SECURITY ASSESSMENT USING RBF NETWORK:

A). On-line security analysis:

There are three basic elements of on-line security analysis and control, namely, monitoring, assessment and control. They are tied together in the following framework.

Step 1) Security monitoring:

Using real-time systems measurements. Identify whether the system is in the normal state or not. If the system is in an emergency state, go to step (4). If load has been lost, go to step (5).

Step 2) Security Assessment:

If the system is in the normal state, determine whether the system is secure or insecure with respect to a set of next contingencies.

Step 3) Emergency controls:

Execute proper corrective action to bring the system back to the normal state following a contingency which causes the system to enter an emergency state. This is sometimes called remedial action.

Step 5) Restorative Control:

Restore service to system loads.

VI. PROPOSED RBF BASED SECURITY ASSESSMENT:

A). Real-power security assessment:

For the computation of Real-power security, the real power flows \( P_{ij} \) are calculated for each outage of the line or transformer or generator using Newton-Raphson load flow study. If any (contingency) line is violating the limits of the base cases line flows, it is labeled as insecure case (0) and if all the line flows (contingency) are within the limits of base case flows are labeled as secure case (1).

\[
P_{ij} = -V_i^2G_{ij} + V_iV_jY_{ij}\cos (\psi_{ij} + \delta_i - \delta_j)
\]

Where

- \( P_{ij} \) = real power flow between buses i and j
- \( V_i \) = voltage at bus I
- \( V_j \) = voltage at bus j
- \( Y_{ij} \) = admittance between bus i and j
- \( G_{ij} \) = conductance between bus i and j
- \( \delta_i \) = admittance angle, \( \delta \) = phase angle.

VII. SIMULATION RESULTS

The training and testing of RBF network has been carried out, for IEEE 14-bus and IEEE 30-bus systems. The training patterns were generated for base case and different network outages using a Newton-Raphson load flow program by varying the loads at each bus randomly covering the whole range of operating
condition up to 110% of the base case loading value. For each power system total 100 patterns were generated. Out of these, 75 patterns were used to train the RBF network and remaining 25 patterns were used to test the accuracy and robustness of the trained RBF network. RBF networks were designed for the real-power security and voltage security, for accurate classification of secure or insecure cases.

**Voltage and real power security:**

The number of input nodes, output nodes for the IEEE 14-bus and IEEE 30-bus systems are given in the table 4.1. The number of clusters of the input patterns, the number of hidden nodes are found to be optimum and resulted to accurate results. The learning rate (η) is taken as 0.5. Both the power systems have one output node, only as it represents the secure or insecure state of the system.

After training RBF network it has been tested for the novel pattern corresponding to different loading conditions. RBF network has been designed for the real power security assessment as well as voltage security assessment for better generalization.

**VIII CONCLUSIONS**

In this paper power system static security assessment has been investigated. The test results presented on IEEE 14-bus system and IEEE 30-bus system provides the following observations.

- A new method has been reported for calculating voltage performance index for contingency ranking. Which eliminates misranking and masking problems? Ranking of all contingencies is same irrespective of values of weights supplied.
- The RBF neural network model provides more accurate results for both the security and insecurity cases.
- Training is very fast as the RBF network has the capability of handling large date
- Testing time is less than 0.2 micro sec.