IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676 Volume 5, Issue 1 (Mar. - Apr. 2013), PP 50-54
www.iosrjournals.org

Static Security analysis in Real time using ANN

Bidyut Ranjan Das Author [1] and Dr. Ashish Chaturvedi [2]
School Of Technology ,CMJ University, ASCSA, Arni University

Abstract: *This paper presents a method for automatic contingency selection and static security evaluation of electrical power systems. The method employs multi-layer Perceptron neural networks whose inputs are power flows and injections, while the outputs identify potentially harmful contingencies. The performance of the method is evaluated for different operating conditions using the IEEE 24 bus test system. It is shown that the neural network classifiers perform very well the contingency selection task and enables a previous classification of system operating state with respect to static security..*

Key words: *Power system security assessment; Contingency selection; Pattern recognition; Artificial neural networks.*

I. Introduction

During power system operation, it is important that load demands be met without violations of system operational constraints. Besides, for a given operating condition, the system should be capable of resisting the loss of any component, with no operational problems. Thus, contingency analysis plays an important role in real-time power system security evaluation. Contingency analysis comprises the simulation of a set of contingencies in which the system behavior is observed. Each post-contingency scenario is evaluated in order to detect operational problems and the severity of violations. The most common operational problems are transmission equipment overloads and inadequate voltage levels at system buses. In static security analysis the identification of operational constraints violation involves the solution of an AC load flow problem, described by a set of nonlinear equations, that has to be solved for each post-contingency scenario. This procedure leads to a high computational effort, which is not desirable for real-time applications. Some approximate models have been proposed for real-time power system static security evaluation [1]. These models reduce computational effort, but they may not classify system contingencies accurately.

It is not possible to analyze system performance considering all contingencies. It is necessary to reduce the number of contingencies to only those that are more likely to occur. These form the critical contingencies set, which is in general defined based on system operation past experience and/or off-line simulations. The need for computational efficiency in real-time contingency analysis can make not possible the analysis even for the critical contingencies set. Then, it becomes necessary to select in the critical set the contingencies that can really lead the system to an emergency state, with operational constraints violations. It is important to note that, as system operating conditions change, the harmful contingencies may also change. Then, the potentially harmful contingencies have to be selected and updated in real-time. This selection, when based only on the operational experience of an utility, may be inadequate. Some models have been proposed for automatic contingency selection [2]. These models employ approximate methods, which may cause false alarms or miss to detect harmful contingencies.

In the last few years artificial neural networks (ANNs) have been successfully applied for the solution of many problems associated with power systems operation and planning [3-6]. Applications of ANNs to security analysis indicate that this is a very promising research field [7-9]. Among other features, ANNs have the ability to learn from historical (or simulated) data and, once trained, exhibit a very fast response when executed.

This work presents a method for power systems automatic contingency selection and static security evaluation. It is possible to identify potentially harmful contingencies in a very short computational time, being the risk of false alarms and contingency misses very reduced. The method is tested for many different operating conditions simulated with the IEEE 24 bus test system. Classification rates for contingency selection and static security evaluation are also provided.

II. Static security analysis

During power systems normal operating conditions the following constraints must be satisfied:
Pk^{nown} **-** P_k (**v**,**0**) = **0**, k = 1,..., $n^{k}{}_{known}{}^{k}$ (1) $Qk^{\prime\prime own}$ **-** Q_k (**v**,**q**) = **0**, k = 1,..., n
$V_k^{mm} < V_k < V_k^{max}$, k = 1,...$n^{k\,k\,k}$ $_{(2)}$ I P_{km} \ < P™^{ax}, *for every branch k* – m

III. Proposed Methodology

where:
pknown and *Qknown* are the injected real and reactive power
at bus k, respectively,
0 and **v** are nodal voltage angle and magnitude vectors;
V_k is the voltage magnitude at bus *k*,
Pkm represents real power flow at branch k-m; and *n* is the number of system buses.

Equation (1) corresponds to power balance requirements (power flow equations), while equation (2) corresponds to system operational constraints, represented by limits imposed to nodal voltage magnitudes and real power flow at system branches and transformers.

System operating state is classified as secure if constraints (1) and (2) are satisfied for a given operating scenario (basic scenario) and also for operating scenarios derived from the occurrence of system contingencies, such as transmission lines outages, transformers outages, etc. (post-contingency scenarios). If constraint (1) and/or (2) are violated for at least one of the post-contingency scenarios, system operating state is classified as insecure [10]. Constraints (1) and (2), when referred to the postcontingency scenarios, are also known as security constraints.

The evaluation of system performance for all possible post-contingency scenarios is not practical. Therefore it becomes necessary to define a set of finite contingencies to be tested, by considering only those that are more likely to occur. This set is usually built based on the utility's operational knowledge and experience, and also on off-line simulations and analysis.

The need for efficiency in real-time power system contingency analysis can make the analysis of all contingencies not feasible even for the pre-selected set. Then it is still necessary to choose, among the pre-selected contingencies set, the potentially harmful ones, i.e., those which occurrence can really drive the system to an emergency condition (violation of constraints (1) and/or (2) in the post-contingency scenario). It is important to observe that, as system operating conditions change, the harmful contingencies also change. Then, the critical contingencies set should be dynamically constructed during real-time operation. The contingency selection based only on the utilities operational experience may be inadequate. Methods for automatic contingency selection have been proposed. These methods employ approximate models, which may increase the risk of false alarms or miss to select contingencies that are really critical.

As discussed in Section 2, real-time contingency analysis may be time-consuming or even unfeasible, particularly for large-scale power systems with too many contingencies.

In the proposed method, artificial neural networks are employed for automatic selection of potentially harmful contingencies. The power flows and injections observed for a basic operating scenario are used as input variables to an ANN that identify in the output the potentially harmful contingencies.

The ANN model adopted is the multi-layer perceptron (MLP-ANN), which has been extensively employed for the solution of pattern recognition problems. The MLP-ANN, illustrated in Figure 1 with only one hidden layer, is a feed forward ANN that employs supervised learning and is capable of approximating any decision region. The neuron model most commonly employed uses a sigmoid activation function [12].

input output

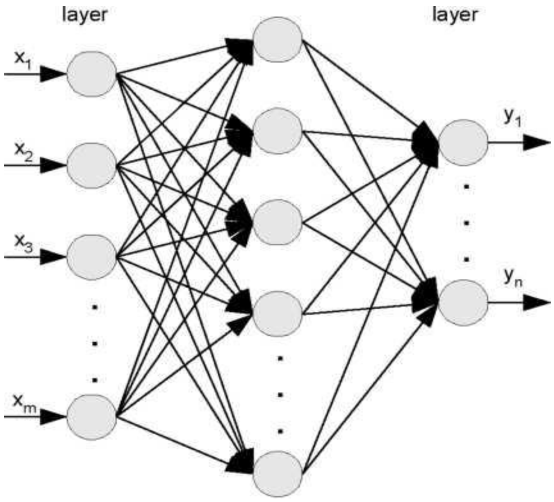

Figure 1 - Multi-Layer Perceptron

For large-scale power systems the number of input variables may be extremely large, which would make the training process not feasible. However, it is known that the occurrence of a given contingency does not affect all system components in the same way. It is expected that those that are electrically close to the contingency under consideration will be most affected. This local characteristic may be explored by assuming that the power system is decomposed into areas, in which different ANNs will perform the contingency classification. In this case, contingencies in one area will be classified by a specific artificial neural network, whose input variables are the power flows and injections observed in the area and in network branches and buses at the area boundaries. This strategy reduces the number of input variables used for each ANN, while preserving the necessary information for the classification task. System areas may be obtained following heuristic criteria, such as: clustering of important contingencies, limitation of ANNs input vector dimensions, etc.

In this work the input vectors for each area are the power flows at the area branches and the power injections at the area generation buses. The power flows at network branches connected to the area boundary buses and the power injections at the terminal buses of these branches are also used as input variables. This may improve the performance for the evaluation of contingencies involving branches close to the area boundary. The input variables chosen are usually available as measurements and may be processed in real-time using the state estimator results or even raw measurements.

Each ANN is trained to identify potentially harmful contingencies based only on the information obtained from the basic operating scenario. The input vector dimension is strictly related to the area size. The number of neurons in the output layer corresponds to the number of contingencies to analyze. Each neuron output classifies a given contingency as potentially harmful or not harmful. The contingencies selected as potentially harmful can be further processed by a conventional method in order to analyze the severity of constraints violations.

The proposed methodology can be divided into two phases:

Phase 1: Classifiers construction (off-line)

- identification of contingencies to be considered (by system operation experts);
- simulation of contingency analysis for many different operating conditions (using conventional analytical methods);
- definition of system areas;
- selection of input variables for each area and construction of the training set;
- ANNs training.

Phase2: Real-time classification

- input variables observation (from state estimation results);
- ANNs execution and identification of the potentially harmful contingencies.

IV. Tests and results

The proposed method has been tested with the IEEE 24 bus test system [13] for many different operating conditions. This system is illustrated in Figure 2, where two different areas and the boundary buses are represented.

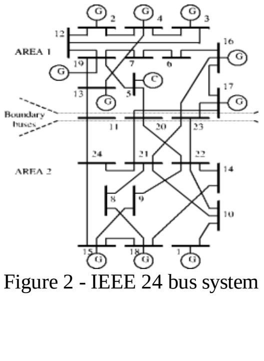

Figure 2 - IEEE 24 bus system

4.1Description of simulation

Contingency analysis has been carried out for the system of Figure 2 by using a conventional load flow program and considering *10 contingencies* randomly chosen for each area. During the simulation, 100 different operating scenarios (basic scenarios) have been considered. Contingency analysis has been performed for each basic scenario and the results obtained have been used to build the training sets for the ANNs. Each training pattern consist of power flows and injections observed for the basic scenario and the corresponding outputs, which are defined based on the analysis of each post-contingency scenario.

According to the proposed methodology, one ANN has to be trained for each area. As stressed in

Section 3, the input variables adopted for each ANN are: the power flows at the area branches, the power injections at the area generation buses and also external power flows at branches connected to the boundary buses, and power injections at the terminal buses of these branches.

4.2 ANNs training

The ANNs training phase is performed offline and only once. The training set must contain samples that represent many different operating scenarios. These samples can be obtained by offline simulation and/or extracted from historical data about system operation. This work considered operating scenarios where the total system load ranges from 50% to 100% of its peak value. Different system topologies have also been considered. The system peak load is 2850 MW and 100 training samples have been used.

During the training phase, many different ANN topologies have been investigated. Among those, the ANN with one hidden layer containing 10 neurons presented the best performance.

As discussed before, the output *yk* of each output neuron classifies each contingency as potentially critical or non-critical. The following target outputs have been used for each output neuron during the training phase:

- yd_k = 0.1, if contingency *k* is not critical; or
- yd_k = 0.9, if contingency k is critical.

The values 0.1 and 0.9 were used to represent the binary output instead of 0.0 and 1.0 in order to avoid the saturation regions of the sigmoid activation functions employed for modeling the ANN neurons [12].

4.3 Tests and training validation

The trained ANNs are employed for contingency classification for new 200 operating scenarios (not used during the training phase). The input variables observed for the new operating conditions are then presented to the ANNs and the computed outputs classify the contingencies according to the following criteria:

- $0.0 < y_k < 0.3$ ® contingency *k*is not critical
- $0.7 < y_k < 1.0$ ® contingency *k*is critical
- $0.3 < y_k < 0.7$ ® unable to classify contingency *k*

The thresholds above have been heuristically defined. The performance of the ANNs is evaluated for the new operating scenarios using the following indexes:

% of false alarms - cases in which a non-critical contingency has been classified as critical.

% of misses - cases in which a critical contingency has been classified as non-critical.

% of undetermined classification - cases in which a contingency classification could not be obtained.

False alarms or undetermined classifications do not bring any harm to power system operation. Whenever a false alarm occurs, a non-critical contingency is classified as critical and selected for severity evaluation through a conventional contingency analysis algorithm. This analysis will reveal that the contingency is not critical. In case of undetermined contingency classification, it is recommended that the contingency be selected for further analysis, when its effect in system operation may be then evaluated.

On the other hand, when critical contingencies are missed, their effects on system operation are not known. Decisions made based on contingency analysis may not be effective to prevent problems due to the occurrence of the missed contingencies.

The new samples used for testing the ANNs have been further analyzed through a conventional contingency analysis program in order to evaluate the performance of the proposed method. Table 1 presents the results obtained.

Table 1 - ANNs performance

Number of tested samples	200
Number of contingencies tested	4000
False alarms	0.2%
Contingency misses	0.1%
Undetermined classifications	3.6%

The results in Table 1 show that the ANNs presented excellent performance, with very few occurrences of false alarms or missed contingencies. Then, the ANNs may not only select potentially harmful contingencies but also provide a classification of system state with respect to static security (secure or insecure). The following indexes can be used to measure system operating state classification accuracy:

% of secure misclassifications - cases in which system operating state is classified as secure, while it lies in an insecure region.

% of insecure misclassifications - cases in which system operating state is classified as insecure, although it is a secure operating point.
% of unknown state classifications - cases in which it is not possible to determine if the system operating state is secure or insecure.

Table 2 presents the operating state classification rates for the same samples used to obtain the indexes shown in Table 1. The ability to classify system operating state has been confirmed.

Table 2 - Security analysis performance

Number of tested samples	200
Secure misclassifications	1.0%
Insecure misclassifications	1.0%
Unknown state classifications	3.0%

It is also important to remark that the computational burden for contingency analysis through the trained ANNs is negligible. Due to the local strategy adopted, the proposed methodology can be easily implemented for large-scale power systems. The local ANNs act as independent classifiers. These ANN classifiers can still be executed in a parallel/distributed environment in order to achieve better results in real-time.

V. Conclusions

This work presented a method that employs artificial neural networks for automatic contingency selection during power systems static security assessment. The contingency analysis is viewed as a local problem and the power system is decomposed into areas for which specific artificial neural networks are responsible for contingency classification. The multi-layer perceptron artificial neural network is used. The input variables are power flows and injections, while the outputs identify the potentially critical contingencies. Tests have been performed using the IEEE 24 bus test system, considering many different operating scenarios. Test results show that the neural classifiers are able to select as potentially critical contingencies those that really lead to system operational problems. The classification accuracy indicate that the automatic contingency selection performed may serve also to classify system operating state with respect to static security. The artificial neural networks generalization capability has been also confirmed for the tested samples.

References

[1] A.S. Debs and A.R. Benson, "Security assessment of power systems",Proc. *Engineering Foundation Conf. on Systems Engineering for Power: Status and Prospects,* pp. 144-176, Henniker, USA, 1975.
[2] G.C. Ejebe, B.F. Wollenberg, “Automatic Contingency Selection”, *IEEE Trans, on PAS,* Vol. PAS-98, pp. 97109, Jan./Feb. 1979.
[3] CIGRE TF 38-06-06 on Artificial Neural Networks Applications for Power Systems, Dagmar Niebur (convener), "Neural network applications in power systems", *Int. Journal of Engineering Intelligent Systems,* Vol.1, No.3, pp.133-158, Dec. 1993.
[4] J.C.S. Souza, A.M. Leite da Silva, A.P. Alves da Silva, "Data debugging for real-time power system monitoring based on pattern analysis", *IEEE Trans, on Power Systems,* Vol.11, No.3, pp.1592-1599, Aug. 1996.
[5] J.C.S. Souza, A.M. Leite da Silva, A.P. Alves da Silva, “Online Topology Determination and Bad Data Suppression in Power System Operation Using Artificial Neural Networks”, Proceedings of the *XX* International Conference on Power Industry Computer Applications (PICA ’97), *pp. 46-53, Columbus, Ohio, May 1997.*
[6] *Applications in Power Systems",* CRL Pub. Ltd., London, UK, 1996.
[6] J S. Weerasooriya and M.A. El-Sharkawi, "Towards static security assessment of large scale power systems using neural networks", *IEE Proceedings-C Generation, Transmission and Distribution,* Vol./issue 139/1, pp.64-70, Jan.. 1992.
[7] D. Niebur, A.J. Germond, "Power system static security assessment using the Kohonen neural network", *IEEE Trans, on Power - Systems,* Vol.7, No.2, pp.865-872, May 1992.
[8] J S. Weerasooriya and M.A. El-Sharkawi, "Feature Selection for Static Security Assessment using Neural Networks", *IEEE Proc. Of1992ISCAS,* pp. 1693-1696, San Diego, California, USA, May 1992.
[9] A.S. Debs, "Modern power system control and operation", *Kluwer Academic Publishers,* Boston, 1988.
[10] G. Irisarri, A.M. Sasson and D. Levner, "Automatic contingency selection for online security analysis - Real time tests", *IEEE Trans. on PAS,* Vol. PAS-98, pp. 1552-1559, Sept./Oct. 1979.
[11] S. Haykin, *Neural Networks: A Comprehensive Foundation,* Macmillan College Publishing Company, 1994.
[12] IEEE Reliability Test System, *IEEE Trans, on Power Systems,* Vol. PAS-98, pp. 2047-2054, Nov./Dec. 1979.