Application of Neural Networks in Power System Security Assessment

Atabak Mashhadi Kashtiban[1], Majid Valizadeh
Faculty of Electrical and Computer Engineering, Tabriz University
[1]atabak_mashhadi@ee.iust.ac.ir

Abstract— Security assessment (SA) refers to the analysis required to determine whether or not a power system can meet specified reliability and security criteria in both transient and steady-state time frames for all credible contingencies.
This paper proposed a review in application of artificial neural network (ANN) in power system security assessment. Systems security identification, neural network capabilities, conventional methods and main problems in data generation and main challenges in using ANN have been discussed.

Keywords: Security Assessment, Neural Network, Contingency Analysis, Power System

I. INTRODUCTION

Due to the ever-increasing economical and environmental pressures power systems are increasingly being operated near their limits of operation. Fast and accurate security assessment, therefore, has become a key issue to ensure secure operation of power system. Therefore security reefers to the degree of risk in a power system's ability to survive imminent disturbances (contingencies) without interruption to customer service and be in some special limited spaces. 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 [1,2,3].

Generally there are two types of security assessments: static security assessment and dynamic security assessment. In both types different operational states are defined as follows [4]:

- Normal or secure state: In the normal state, all customer demands are met and operating limit is within presented limits.
- Alert or critical state: In this state the system variables are still within limits and constrain are satisfied, but little disturbance can lead to variable toward instability.
- Emergency or unsecured state: the power system enters the emergency mode of operation upon violation of security related inequality constraints. For a 3-bus-3-line power system that is shown in Fig. 1-a, considering limitations, operating and constrained space illustrated in Fig. 1-b.

Fig. 2 show a simplified diagram of the principle data flow in a power system where real-time measurements are stored in a database [5,6]. The state estimation then adjusts bad and missing data. Based on the estimated values the current mathematical model of the power system is established. Based on simulation of potential equipment outage, the security level of the system is determined. If the system is considered unsafe with respect to one or more potential outages, control actions have to be taken.

II. SECURITY ASSESSMENT

1) *Static Security Assessment (SSA)*

Static security of a power system addresses whether, after a disturbance, the system reaches a steady state operating condition that does not violate given system operating Constraints. These constraints ensure the power in the network is properly balanced, the magnitude of all bus voltage is within acceptable limits, and the thermal limit of each transmission line is not exceeded. If any one constraint is violated, the system may experience disturbance that could result in a “brown up” or even a “black out”. Hence, the power system is insecure [7,8].

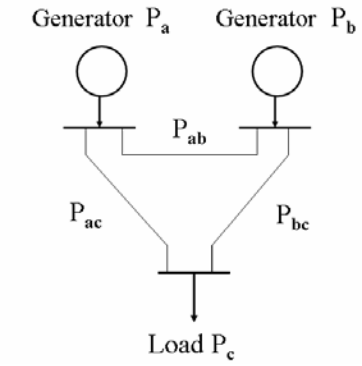

Fig 1-a. three bus- three line typical power system

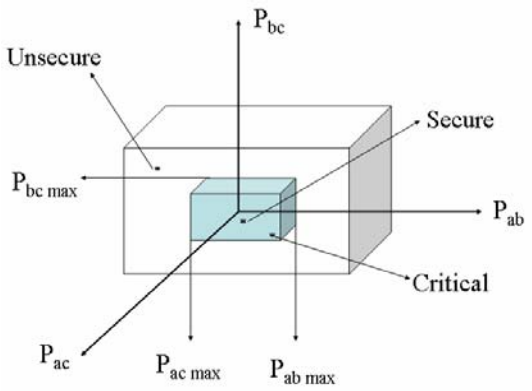

Fig 1-a. Constraints and operating space for considered system in Fig 1-a

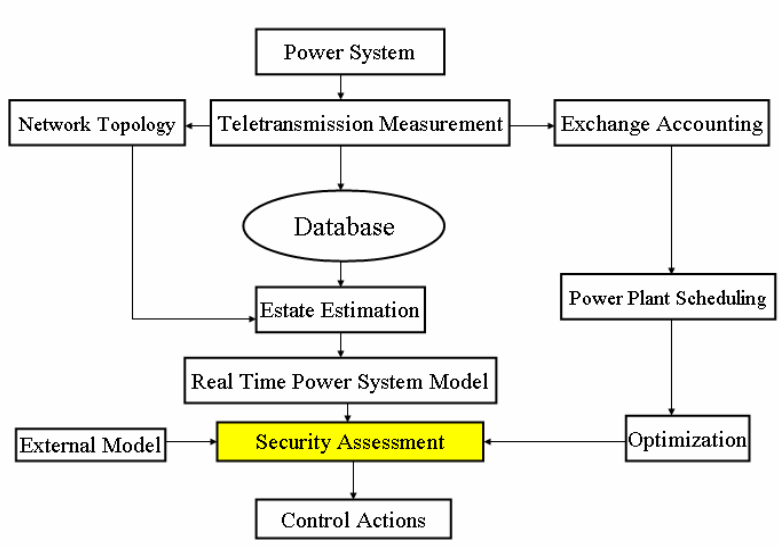

Fig. 2. Data flow in power System Operation

In static security assessment, the status of the power system is evaluated for various probable disturbances, such as the loss of a transmission line *or* a generating unit. In steady state, the static security is evaluated using the load flow equations. The load flow is solved for various types of disturbances and the results are compared with the system

constraints. Violations, if any, are then identified and the operating condition is labeled secure or insecure. For convenience, the results of this off-line analysis are stored in lookup tables.

The normal steady state operation of a power system requires that the generator power satisfy:

$$\sum_i P_{Gi} = P_D + P_L \quad (1)$$

$$\sum_i Q_{Gi} = Q_D + Q_L \quad (2)$$

Where P_{Gi} and Q_{Gi}, are the real and reactive powers of generator at bus (i); P_D and Q_D, are the total real and reactive load demands; P_L and Q_L, are the real and reactive losses in the transmission network.

Inequality constraints must always be imposed on the system to ensure secure operation. All bus voltages must be bounded, all line currents must not exceed the respective thermal limits, and all generator power outputs must be limited. These constraints can be expressed as followed:

$$V_{min} \le V \le V_{max}$$
$$P_{i,min} \le P \le P_{i,max}$$
$$Q_{i,min} \le Q \le Q_{i,max}$$
$$S_{i,min} \le S \le S_{i,max}$$

where S_i is apparent power of line. In all cases for classification of power system security level, assume that the steady state operating condition of the power system is governed by an optimal dispatch strategy. Typically total power cost function is given by:

$$C = \sum_i C_i \quad (3)$$

where C_i the cost function of individual generators, is given by:

$$C_i = C_1 P_{Gi}^2 + C_2 P_{Gi} + C_3 \quad (4)$$

where C_1, C_2 and C_3 are constant coefficient for a given generator.

The optimum dispatch problem is solved by minimizing the cost function C while satisfying equation 1, 2. Mathematically, the problem reduces to minimizing the following augmented cost index J,

$$J = C - \lambda(\sum_i P_{Gi} - P_D - P_L) \quad (5)$$

where λ is Lagrange multiplier.

2) *Dynamic Security Assessment (DSA)*

DSA refers to the analysis required to determine whether or not a power system can meet specified reliability and security criteria in both transient and steady-state time frames for all credible contingencies. In the operating environment, a secure system is one in which operating criteria are respected at pre- and post contingency conditions [9,10,11].

Online DSA takes measurements of the actual system condition and performs security analysis in near real time and passes information to the operator or directly on to control systems. The main components are shown in Fig. 3.
System measurements can be obtained from a number of sources, including traditional system control and data acquisition (SCADA), phasor measurement unit (PMU) and disturbance monitors. The measurements obtained are used for four primary purposes, as follows [10]:

- Input to state estimation from which system models will be developed (SCADA or PMs).
- Direct input to security computation engines (SCADA or PMs)
- Bench marking of state estimation results or computational results (PMs or disturbance recorders)
- Arming or triggering special protection system (SCADA or PMs).

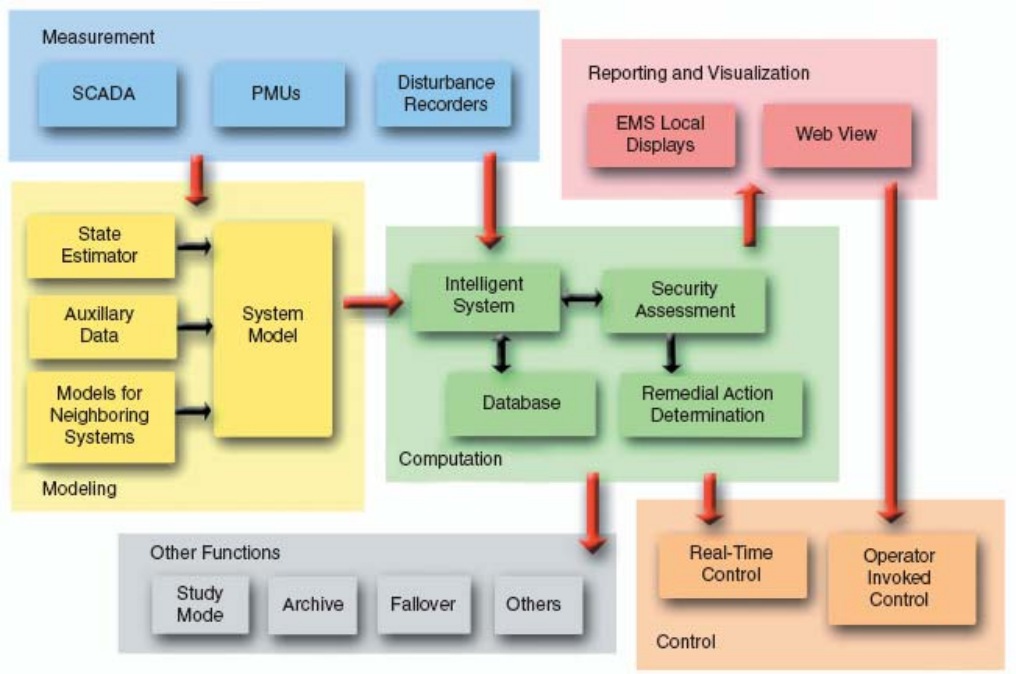

Fig. 3.The components of an online dynamic security assessment system

III. ANN ARCHITECTURE

An ANN required three main functions:

- An organized topology of interconnected processing elements
- A suitable training or learning algorithm
- A method of recalling information

The following are the key element of the ANN operation:

- Processing element; the processing elements are often called nodes or neurons where most of the computing is done.
- Architecture; ANN's architectures are formed by connecting processing element into layers and linking them with weighted interconnections.

- Learning; learning is accomplished by changing the value of the weighs to achieve the desired results; i.e. the correct classification.

Because of growth the energy demand in large cities and development the power marketing and moreover the capabilities of ANN to fast and online analysis of large power systems, the number of proposed paper in this are increased enormously. Fig. 4-a shows the application of ANN in main power system subjects during 2000-2005. Fig. 4-b shows the sage various ANN that used in SA.

To choosing the type of NN or learning algorithm and adjusting their parameters finely, some recommended in some references and papers proposed [4]:

In practical power systems the dimension of the operating system is very high. To overcome this "curse of high dimensionality", three main approaches can be followed:

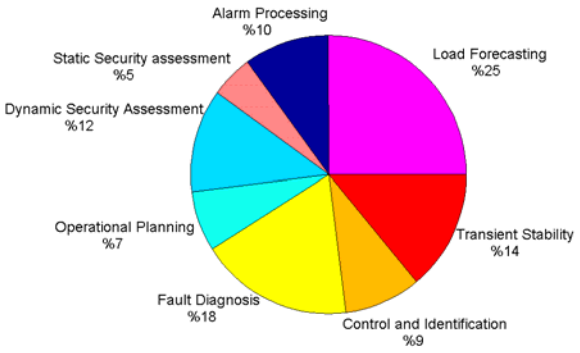

Fig. 4-a.Neural networks applications in power systems; 2000-April 2005

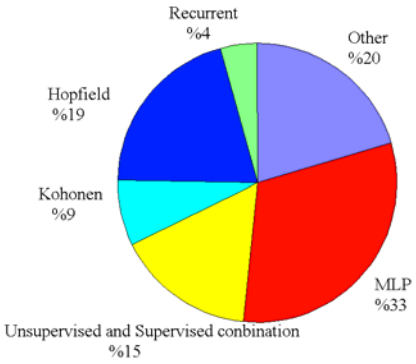

Fig. 4-b.NNs types used for security assessment

- Restrict the number of contingences and characterization of the security boundaries. This is for example done with supervised NNs like MLP.
- Reduce the dimension of the operating vector; this is for example done with unsupervised NNs like Oja-Sanger networks.
- Quantify of the operating point into a reduced number of classes, this is done with clustering algorithms for instance the nearest neighbor or the k-means clustering algorithms

Commonly NN that satisfies these conditions is multi-layered perceptron(MLP) with backpropagation training algorithm. The reason for this is on-line learning capability. There are two problems with using MLP, selecting of input data and overtraining. A good method for first problem is using some of the security indicators presently calculated by the energy management system (EMS) as inputs to the ANN. To overcome the latest problem using the backpropagation with selective training algorithm proposed.

Input vector for NN in real power system is very large and can be involved [4]:

- Amplitude and angle of bus voltage
- Active and reactive power of all generator
- Active and reactive power of all connected load
- Active and reactive power of all lines

Moreover these parameters thermal limitations of generators and lines, active power of especial lines and other parameters that affected on contingency could be considered.

Proposed that the dimension of input vector chosen by considering contingency parameter and neglected other data that nt very important in analysis.

IV. CONCLUSION

In this paper application of ANN in power system security assessment considered and evaluated. Challenges and main drawbacks and advantages of proposed method have been studied and introduced. Considering above we can draw the conclusions that:

- The most popular and commonly NN that satisfy high speed for analysis is MLP with backpropagation training algorithm.
- For reduce the input vector, moreover using selective backpropagation algorithm for training algorithm, we must consider contingency parameter in choosing data from optimal power flow software.
- Proposed that for better convergence declining method is used for adjusting learning parameter in backpropagation training algorithm.

ACKNOWLEDGENT

Authors would like to thanks Dr. Vakil Baghmisheh and Dr. Tarafdar Haque for their helpful discussions and their valuable suggestions.

REFERENCES

[1] M. A. El Sharkawi, Neural Networks' Power, IEEE Potentials, pp 12-16, 1996
[2] K. Morison, X. Lin, F. Xue, L. Wang, Critical Requirements for Successful On-Line Security Assessment, IEEE, 2004
[3] F. Wu, Y. Tsai, Probabilistic Dynamic Security Assessment Of Power Systems: Part I-Basic Model, IEEE Trans on Circuits and Systems, Vol.30, no. 3, March 1983
[4] A. M. Kashtiban , M. Tarafdar Haque, Application of Neural Networks in Power System; A review, International Conference of Neural Network Systems (ENFORMATIKA), 26 June 2005
[5] M.T. Vakil, N. Pavesic, A Fast Simplified Fuzzy ARTMAP Network, Kluwer Academic Publisher, pp. 273-316, 2003
[6] K. Warwick, A. Ekwure, R. Aggarwal, Artificial Intelligence Techniques in Power Systems, IEE Power Engineering Series 22, Bookcratt Printed, pp. 117-119, 1997
[7] T. Kim, J. Choo, S. Lee, J. Kim, Security Assessment for Bus Voltage Using Probabilistic Load Flow, 8th International conference on Probabilistic Method, September 2004
[8] V. Vittal, A. Michel, Stability and Security Assessment of a Class of Systems Governed by LaGrange's Equation with Application to Multi-Machine Power Systems, IEEE Trans on Circuits and Systems, Vol.33, no. 6, June 1986
[9] K. Morison, H. Hamadanizadeh, L. Wang, Dynamic Security Assessment Tools, IEEE, 1999
[10] K. Morison, L. Wang, P. Kundur, Power System Security Assessment, IEEE Power and Energy Magazine, September 2004
[11] J. Huang, K. Morison, A. Moshref, An Intelligent System for Advanced Dynamic Security Assessment, IEEE, 2002