Correction to "Preliminary Results on Using Artificial Neural Networks for Security Assessment[1]

In the above paper,[1] the following discussion and closure should have appeared.

Discussion

D. S. KIRSCHEN, B. F. WOLLENBERG, G. D. IRISARRI, Control Data Corporation, Plymouth MN: A fast and reliable method for assessing on-line the dynamic security of a power system would be a very useful tool for power system operators. The neural net approach proposed by the authors appears attractive because of its highly parallel nature and its simplicity. However, as the authors correctly emphasize, the applicability of the method to systems of a practical size has not been demonstrated.

Since the consequences of a misclassification can be catastrophic, a large number of training cases are required to correctly assess the shape of the security contour. The behavior of the system near the boundaries is indeed particularly important because economic considerations often encourage the operation of the system near its limits. Furthermore, care must be taken to cover most of the possible operating conditions to avoid the need to extrapolate.

For a practical system, however, a simple calculation shows that the number of training cases becomes unmanageable. Consider a system with 1000 lines, 50 major generating units and 50 load groups. There are 500,000 possible line configurations for this system if we assume that no more than two lines are in an abnormal state at any given time. This number must be multiplied by at least 50 to account for the various configurations of generating units. For each of these 25 million configurations, the security limit must be determined in terms of the continuous parameters. In this case, let us assume that there 500 parameters (three for each generating unit and one for each load group). If the range of each parameter is spanned by an average of five samples (a number smaller than the one used by the authors in their examples), this conservative estimate of the total number of training cases reaches 62.5 billion.

One might argue that some parameters do not have a strong effect on stability and might be ignored. However, to the best of our knowledge, no reliable method has been found to determine a priori which parameters can be ignored.

Power system planners base their decisions for system expansion on a relatively small number (from a few hundred to a few thousand) key test cases which they determine based on their experience. Shouldn't the ANN be trained using such a set instead of a very large number of training cases spanning the whole problem space? Wouldn't an expert system that could determine the key training cases be useful?

The training mechanism used by the authors relies on a single pass of the training data through the ANN. As the authors indicate, with this method, the number of hidden units must exceed the number of training cases. As the above example shows, this number quickly becomes unfeasible. Furthermore, to compute the matrix **C** of Eq. 5 (which is nothing more than the result of a least square fit problem), one must invert the matrix $[\mathbf{H}^T\mathbf{H}]$ which is of dimension NxN where N is the cardinality of the training set. Besides its unmanageable dimension, this matrix is likely to be ill-conditioned when N is much greater than the dimension of the training vectors. It is clear that this technique is not applicable to problems (from power systems analysis or another field) much larger than the one considered in the paper.

The above considerations assume that the ANN is a good approach to the problem. However, past experience with related methodologies [5, 6] gave very disappointing results. Although the ANN may be superior in some respects than the pattern recognition, it is *marginally* better, while what is needed is a methodology which is *radically* better. Neural nets do not provide such drastic improvement because they are based on essentially the same principles as the old pattern recognition methods.

Manuscript received May 26, 1989.

[1]M. Aggoune, M.A. El-Sharkawi, D.C. Park, M.J. Damborg, and R.J. Marks II, *IEEE Trans. on Power Systems*, vol. 6, no. 2, pp. 890-896, May 1991.

M. A. El-Sharkawi, R. J. Marks and **M. J. Damborg**: The authors would like to thank the discussers for their interest. As the title of our paper indicates, the research work reported here is "preliminary". By no means we are claiming a fully developed Neural Network for immediate installation in real power systems. That is a task which might take several years to accomplish. This paper is an attempt to determine whether such an approach has promise.

The discussers properly recognize that a major need in an EMS center is a class of tools that permit systems to operate closer to the security boundaries. That is where additional economic and performance benefits are to be gained. The discussers also point out that misclassification is unacceptable. Hence, today's operators work at a "comfortable" distance from these very poorly known boundaries, a distance determined by experience. The entire thrust of our suggested use of ANN's is to provide more knowledge about security boundaries with the result that the system can be maintained closer to these boundaries with confidence.

However, the authors believe the discusser's dismissal of ANN's is premature. They cite many important problems, yet it is not clear that any of these is fatal to the approach. For example, it would indeed be ridiculous to suggest that a single ANN should be trained for all security issues in a full scale system. But we have shown that a single, rather modest ANN can be trained to respond to a single security question. Many individual ANN's could respond to many individual questions. Since ANN's are inexpensive and execute quickly on either general or special machines, it is quite reasonable to imagine a security monitor consisting of a collection of ANN's. The author's believe such an approach is consistent with today's operating experience where operators are most concerned with a few very specific contingencies for any operating state.

It is also inappropriate to dismiss current ANN technology as a "marginal" improvement over the previous attempts at using pattern recognition. Since ANN's are *not* based on prespecified classification functions, they appear to avoid many of the limitations that plagued the ability of previous pattern recognition approaches to discriminate complex patterns in high dimensional spaces. This is not to say that ANN's are proven to be "radically better" but that they may be if applied with care. On the other hand, it is also possible that we may all be disappointed upon further study of their potential.

Keeping these general comments in mind, we would like to offer the following specific responses:

1. The fact that a boundary can be established for dynamic security is by itself a major improvement to the current practice. The misclassification ratio, which are all near to the dynamic security boundary, is less than 2% of a sample of 10,000 testing points. We are not aware of any existing technique, short of the exhaustive search methods, that provides better interpolation accuracy.

In recent research, the accuracy of the ANN (at the boundaries) is shown to be enhanced when methods such as the inverted ANN [a] or the Oracles-based training [b] is used.

2. A common, and accurate, criticism of researchers in artificial neural networks is their application of neural networks to so called "toy problems". Indeed, the future success of artificial neural networks will be determined largely by their ability to successfully deal with large data bases. We have empirically observed that many popular neural network paradigms, such as back-propagation training, Hopfield-type networks and

Gram-Schmidt procedures, numerically fail for large networks and/or data bases. However, the problem may either be addressed algorithmically or by modularization [c]. For example, as the discussers mentioned, an expert system may be used to determine key training cases. Also, as mentioned earlier, modular Neural Networks can be used, where several ANNs are structured in a multi-level form. In the lower level several ANNs can be used where each one monitors some of the variables and configurations of the power system. The upper level ANNs can perform a supervisory role to activate the proper lower level ANN based on the current operating condition. In addition, adaptive training of the ANN can also be used. For instance, the back-propagation technique can be modified to update the network when additional data is received, either by off-line simulation or by real system measurement. In this case, the network is continually updated without the need for storing the training data.

3. The discussers are quite correct when they point out that inversion of large matrices of the form H^TH is computationally unacceptable. Matrices such as C, rather, are better crafted by a Gram-Schmidt type training procedure wherein training vectors are used to sequentially update the C matrix [d]. This procedure also allows for the censoring of data insufficiently noncolinear with previous data. In the procedure of matrix inversion, nearly colinear data manifests itself as an ill-conditioned H^TH.

The success of the neural network used in this paper to accurately represent the training data is dependent on the ratio of hidden neurons to the number of training vectors. If this ratio exceeds one, then, in the absence of any computational inexactness, we should have a successful representation. The success of some other neural networks, on the other hand, are not based on the cardinality of the training data, but on the diversity of the classification partition. In principal, if billions of training vectors are linearly separable in partition space, a single layer perceptron with a single output neuron will do the job.

It is also worth mentioning that in more recent research on ANN security, different training algorithms that do not need matrix inversion are used [e, f].

4. Lastly, We must address our choice of a performance index before we specify whether neural networks will perform marginally or radically better than other conventional methodology. For a given data base, for example, a table look-up approach will result in the most accurate assessment of the system's security if the current operating point is included in the table. However, a table look-up interpolation method, such as the nearest neighbor, does not interpolate as accurately as the ANN [e, f]. In addition, for large data bases, an ANN performs much faster than the nearest-neighbor approach in the classification mode [e, f]. Thus, if assessment time is incorporated into the cost function, the neural network may indeed radically outperform optimal exhaustive search approaches. Either method can be skewed to arbitrarily reduce the probability of misclassifications.

References

[a] A. Linden and J. Kindermann, "Inversion of Multilayer Nests," Proceeding of the International Joint Conference on Neural Networks, Washington, DC, June 18-22, 1989, pp. 425-430.

[b] Dana Angluin, "Queries and Concept Learning," Machine Learning, pp. 319-342, 1988.

[c] A. Waibul, "Modular construction of time-delay neural networks for speech recognition," Neural Computation, vol. 1, pp. 39-46 (1989).

[d] R. J. Marks II, L. E. Atlas and S. Oh, "Generalization in layered classification neural networks". 1988 IEEE International Symposium on Circuits and Systems, pp. 503-506, Helsinki, 7-9 June, 1988.

[e] M. E. Aggoune, L. E. Atlas, D. A. Cohn, M. J. Damborg, M. A. El-Sharkawi and R. J. Marks II, "Artificial neural networks for static system security assessment," Proc. 1989 IEEE International Symposium on Circuits and Systems, pp. 490-494, 9-11 May 1989, Portland-invited paper.

[f] M. A. El-Sharkawi, R. J. Marks II, M. E. Aggoune, D. C. Park, M. J. Damborg and L. E. Atlas, "Dynamic security assessment of power systems using back error propagation artificial neural networks," Proceedings of the 2nd Annual Symposium on Expert Systems Applications to Power Systems, 17-20 July 89, Seattle.

Manuscript received March, 5, 1991.