www.serd.ait.ac.th/reric

The Application of Bayes Classifier in Power System Security Assessment

Hyungchul Kim and Chanan Singh
Dept. of Electrical Engineering,
Texas A&M University,
College Station, TX 77843-3128
USA

ABSTRACT

This paper proposes a probabilistic method for power system security assessment, using Bayes classifier. The Bayes classifier, one of data classification tools, can apply to the power system reliability area for calculations such as probabilistic security indices. The determination of security breach is a cumbersome and time-consuming process due to consideration of dynamic and steady state effects. The straight Monte Carlo simulation, one of the commonly used methods in power system reliability, requires evaluation of each sampled state and can result in high computation time. Once joint probability density of feature vectors is obtained, the Bayes classifier provides assessment of system security without complicated contingency analyses and can reduce the computational burden. Security status of a given feature vector can be determined by a Bayes rule, which can be implemented in power system reliability studies.

1. INTRODUCTION

The primary role of a power system is to provide reliable and continuous electrical energy to satisfy system load. Power system reliability, in a broad sense, can be defined as the ability of the system to provide an adequate supply of electric power with satisfactory quality. The reliability of a composite power system is comprised of both adequacy and security assessments [1-2]. Adequacy assessment relates to the ability of the system to supply energy requirements of customers in a satisfactory manner. Since adequacy assessment deals with static condition, it does not include the evaluation of the system response to transient disturbances. Security assessment deals with the ability of the electric systems to survive sudden disturbances such as electric short circuits or unanticipated loss of system elements. This includes the response of the system to the loss of generations and transmission lines.

With the advent of competition, one of the primary consequences under deregulated environment is the effect on power system reliability. Many utilities are operating with high security margin in power system reliability. According to a recent report [3], deregulation may greatly increase power transfers and degrade power system reliability. The impact of deregulation influences reliability evaluation for power system planning and operation.

In a more competitive environment, security assessment should be performed more realistically so that the investment of resources can be accomplished in a cost-effective manner. Probabilistic criterion can recognize the uncertain nature of system components. Monte-Carlo simulation method can obtain the results by collecting and analyzing sample data based on statistical experiments. Monte-Carlo simulation is suitable for analysis of complicated systems such as power systems, but it also requires large amount of computation time to achieve satisfactory statistical convergence and the characterization of repeated sampling states in security assessment. Moreover, when local phenomenon such as voltage stability is considered for contingency analysis, computation burden is even further

increased. This paper tries to address this situation by treating power system security assessment as a pattern classification problem.

This paper shows how Bayes classifier can be implemented for security assessment. After the selection and analysis process of feature vectors, system security can be tested by the Bayes decision rule. The case study of WSCC system is presented to demonstrate the efficiency of the proposed method through calculation of system reliability indices for steady state and dynamic security assessment.

2. THE DETERMINATION OF SECURITY BREACH AND OPERATING STATES

There can be various types of feature vectors in a power system, such as real and reactive power or voltage magnitude and angle at each bus. In this paper, the feature vector can consist of transmission line status, generator status and normalized system load for power system reliability studies. While the status of transmission lines and generators is only represented as zero (down state) and one (up state), normalized system load is computed as *L=(actual load)/(average load)*. Since the elements of the feature vector X do not influence other elements, these are statistically independent of each other. The feature vector corresponding to a system state can be represented as Eq. (1)

$$X_i = [\ T_{1,i}, \text{- - - - - -}, T_{k,i}, \text{- - - - - -}, T_{m,i}, G_{1,i}, \text{- - - - - -}, G_{j,i}, \text{- - - - - -}, G_{n,i}, L_i\ ] \quad (1)$$

where, T_k = The status of transmission line k in i th feature vector,
G_j = The status of generator of generator bus j in i th feature vector,
L_i = Normalized total system load in i th feature vector,
m = The total number of transmission lines, and
n = The total number of generation buses.

During the classification of feature vectors in power system security analysis, system post-contingency status can be generally divided into two groups, “secure” and “insecure”. To determine system status, the decision of security breach of feature vectors is required. The determination of security breach for a system state can be defined as the characterization of feature vectors. The state characterization of feature vectors may include transient behavior as well as evaluation of post-contingency steady state. In static security assessment, the characterization of feature vectors requires the evaluation of post-contingency steady state. For successful operation, a system should supply system load without violating operating conditions and load shedding in steady state. The optimal power flow (OPF) is performed under the constraints such as the limit of power flow and power generation for a contingency. Here, the objective of the OPF is to minimize the sum of curtailed load. Curtailed load at each load bus is represented as the difference between the real load demand and the load after rescheduling of generation. When the objective function of OPF is not zero, this means that the sampled state results in loss of load. Voltage instability may be related to voltage collapse caused by a certain contingency. Voltage stability is considered as a local phenomenon. Voltage stability indicator [5] shows the portion of the system that is directly affected by the contingency. The indicator at each load bus varies between zero and one. The indicator is zero when there is no load in the system and is one at the collapse point. The voltage stability indicator of the overall system is the maximum value among voltage stability indicators of the load buses. When this value is above the threshold value, the system is regarded as having voltage instability problem. If the system has any problem such as load shedding or voltage instability, it belongs to “group-zero”. If all equipment and operating constraints are within their limits, the feature vector is defined as “group-one” in this paper. In dynamic security assessment, transient stability is a dynamic part of security studies. The power system is

considered stable if the fault is cleared before the critical clearing time (CCT), that is fault-clearing time (CT) is less than the CCT. Thus the first step for satisfying transient stability constraints is to calculate CCT. For simplification, we assume that the probability density function (p.d.f.) of CT is a normal distribution. Since large amount of computation time is required for calculating CCT step by step, bisection method [6] is used in this paper. After the probability of successfully clearing a fault from the p.d.f. of clearing time is obtained and is less than the minimum acceptable probability of stability, the system is regarded as unsafe.

If the system has any problem such as dynamic or static insecurity, it belongs to emergency state as one of the system operating-states [7]. A feature vector corresponding to emergency state belongs to "group-zero". The probability of emergency state is the expected period per year during a given period, in which the system may violate the equipment and operating constraints. The frequency of emergency state is the expected number of occurrences during a given period of time. If all equipment and operating constraints are within their limits, system operating-states can be classified as normal state or alert state in probabilistic security assessment. In the normal state, all equipment and operation constraints are within their limits. The system can tolerate an assumed contingency without violating limits. As expected, the system including generators, transmission lines and loads has no difficulty. The security index can be expressed as the normal period per year during a given period for the probability of normal state and the expected number of occurrence during a given period of time for the frequency of normal state. The alert state is similar to a normal state in that all constraints are satisfied. However, when an assumed contingency occurs, sufficient margin is no longer available. Similar to emergency and normal state, the security index can be defined in alert state.

3. THE FUNDAMENTALS OF BAYES CLASSIFIER

As mentioned in a previous section, the determination of security breach is a time-consuming process. It is impossible to perform the evaluation of security breach of all possible contingency cases resulting from load variation. By employing Bayes classifier, computation time in power system security analysis can be considerably reduced. Here, the fundamentals of Bayes classifier are summarized.

Suppose there are m numbers of a feature vector X. A feature vector X belongs to one of the n numbers of groups. Our objective is to find class or group a feature vector belongs to. If the conditional probability of group G_c is larger than that of the other groups, a feature vector X belongs to group G_c. By Bayes rule, conditional probability of each group $p(G_c|X)$ can be expressed as in Eq. (2).

$$p(G_c \mid X) = \cdot \frac{p(X \mid G_c) \cdot P(G_c)}{p(X)} = \frac{p(X, G_c)}{p(X)} \tag{2}$$

where, $p(X|G_c)$ = the conditional probability for the feature vector X, given that it belongs to group G_c,
$P(G_c)$ = the prior probability of group G_c,
$p(X,G_c)$ = the joint probability density of the feature vector X, and
$p(X)$ = the probability of feature vector X.

Since the probability $p(X)$ of feature vector X is independent in each group, the joint probability density $p(X,G_c)$ of the feature vector X is the subject of study. The prior probability $P(G_c)$ can be approximated as the number of samples of group G_c divided by the number of all samples. The assignment of feature vectors to the group with the highest joint probability density can be easily made by the

conditional probability and the prior probability. The Bayes decision rule [8, 9] is to choose the group with maximum $p(X,G_c)$ among n number of joint probability densities of the feature vector X, i.e..

$$X \in G_c \qquad If \;\; p(X, G_c) = Max\{p(X, G_1), p(X, G_2), - - - - -, p(X, G_n)\} \tag{3}$$

The status of elements in this paper is assumed independent of each other. When the elements of a feature vector are all statistically independent, conditional probability can be expressed as the product of conditional probability for each element in the feature vector X.

$$p(X \mid G_c) = \prod_{b=1}^{d} P(x_b \mid G_c) \tag{4}$$

where, x_b = the b th element of feature vector X, and
d = the dimension of feature vector X.

The elements of feature vectors are of two different types, binary elements and non-binary elements. With binary elements of feature vectors, the probability for each element can be estimated by Eq. (5). P_{bc} can be approximated by the mean of samples.

$$P(x_b = 1 \mid G_c) = \frac{T_{bc}}{S_c} = p_{bc}, \qquad P(x_b = 0 \mid G_c) = 1 - p_{bc} \tag{5}$$

where, S_c = the number of samples for group G_c, and
T_{bc} = the occurrences number with one in the u th element among all S_c.

The non-binary elements of feature vectors can be assumed to have a particular probability function by the characteristic of element. The mean and variance for each group are obtained from all samples. When Gaussian function is implemented as the probability density function of each element of feature vectors, the Gaussian density for each element can be written as Eq. (6).

$$y = f(x_b = a \mid \mu, \sigma, G_c) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{6}$$

where, a = the value of b th elements in feature vector X,
m = the mean of b th elements in feature vector X, and
s = the variance mean of b th elements in feature vector X.

The selection of the feature vectors in Bayes classifier has a great influence on classification accuracy. In power system security analysis, it is impossible to store the decision of security breach of all possible contingency cases resulting from load variation. The suitable selection of feature vectors, therefore, is one of the important factors in the success of the Bayes classifier. In the power system security study, feature vectors have various types, for example, a base case, a single line or a generator contingency and a double contingency etc. The base case is the case without generator or transmission line outage. The number of feature vectors also plays an important role in the Bayes classifier. With more feature vectors used for obtaining the distribution, the classification accuracy may be better but more computation effort is needed for the decision of security breach.

4. MONTE-CARLO SIMULATION USING THE BAYES CLASSIFIER

The sequential simulation is based on component state duration. It proceeds by generating a sequence of events using random numbers and probability distributions of random variables. Further, there are two methods in sequential Monte-Carlo simulation, the fixed interval method and the next event method [4]. In the fixed interval method, system states are updated with a fixed interval. In the next event method, system states are updated at the occurrence of an event. Here, the next event method is implemented with Bayes classifier used for state evaluation.

The first consideration of Monte-Carlo Simulation using the Bayes classifier is to obtain probability for each element of feature vectors, which is required for the Bayes decision-making.

Step 1: Select feature vectors by random sampling based on Gaussian function of the system load. The selection of feature vectors is also an important factor for getting desirable results. Feature vectors can be easily obtained by random sampling such as straight Monte-Carlo simulation.

Step 2: Perform state characterization of each feature vector, which can be classified as group-one or group-zero.

Step 3: Obtain the conditional probability for each element in the feature vector, which is obtained by Eq. (5) for binary-element and by Eq. (6) for non-binary element.

Now, Bayes decision rule is ready to be applied for probabilistic security index calculation in the power system. With a given new sampled feature vector, the groups are sorted by the posterior probabilities calculated with Bayes rule. The procedure is described in following steps.

Step 4: Generate a random number for each component such as transmission line or generator. In power system security assessment, random sampling of Monte-Carlo simulation is defined as an artificial contingency. The output of random sampling is represented as a base case, a contingency, double contingencies and so on. The evaluation of double and higher order contingencies should be handled in security analysis. For example, double contingencies are the overlaps of two outages. They can often make a system insecure, even though a system satisfies operating conditions when either happened separately.

Step 5: For each sampled state, make a Bayes decision making process instead of state characterization. When there is a dynamic or static problem, go to step 6.1. Otherwise, perform step 6.2.

Step 6.1: Update the index of the emergency state. The index of emergency state is similar to a conventional LOLP (loss of load probability). The probability of emergency state is (the duration time with system problem) / (total simulation time). The frequency of emergency state can be expressed as (the number of occurrences with system problem) / (year).

Step 6.2: Consider assumed additional contingencies. Like step 5, perform a Bayes decision instead of state characterization. It can be determined whether a feature vector is the normal or alert state. With an N-component system and a N' component contingency, (N-N') calculation is required for state characterization of additional contingencies. For example, (N-2) calculations are carried out for double contingencies. Additional contingencies, however, should be defined on the basis of the probability of system failure caused by the outage of the component [10]. The probability of normal state is (the duration time with system security) / (total simulation time). The frequency of normal state can be expressed as (the number of occurrences with system security) / (year).

Step 7: Check the coefficient of variation and a maximum iteration number. Repeat above steps until coefficient of variation is less than a specified threshold or maximum iteration is achieved.

5. CASE STUDY

Table 1 Probability Distribution of Fault Clearing Time and Reliability Data of Transmission Lines

Line		Distribution Type	Mean Clearing time (sec)	standard deviation (sec)	Failure Rate (1/hours)	Repair Rate (1/hours)
From	To					
1	4	Normal	0.20	0.02	1.5e-5	0.1
2	7	Normal	0.20	0.02	1.5e-5	0.1
3	9	Normal	0.20	0.02	1.5e-5	0.1
4	5	Normal	0.20	0.02	1.5e-5	0.1
4	6	Normal	0.20	0.02	1.5e-5	0.1
5	7	Normal	0.05	0.02	1.5e-5	0.1
6	9	Normal	0.10	0.02	1.5e-5	0.1
7	8	Normal	0.10	0.02	1.5e-5	0.1
8	9	Normal	0.15	0.02	1.5e-5	0.1

Western System Coordinating Council (WSCC) 3-machine, 9-bus system [11] is used in a case study. The base MVA is 100 and system frequency is 60 Hz. The parameter and thermal limit of transmission lines, generator and exciter data used in this simulation are shown in [11]. A value of system load is selected randomly from normal distribution with mean one and variance 0.3. When the selected random value is multiplied by the mean real load value of load bus in Table 1, the corresponding value is real load of each load bus. Reactive loads are also calculated assuming constant power factor. Two hundred feature vectors are selected from each of following cases: a base case, a one-contingency and a double contingency. These vectors are characterized as group one or zero. Reliability data of transmission lines and generators is shown in Tables 1 and 2 respectively.

Table 2 Bus Data and Reliability Data of Generator

Bus No.	Real power generation (MW)	Mean value of Load(MW)	Failure Rate	Repair rate
1	71.6	N/A	1.5e-3	0.1
2	163.0	N/A	1.5e-3	0.1
3	85.0	N/A	1.5e-3	0.1
4	0.0	N/A	N/A	N/A
5	0.0	125.0	N/A	N/A
6	0.0	90.0	N/A	N/A
7	0.0	N/A	N/A	N/A
8	0.0	100.0	N/A	N/A
9	0.0	N/A	N/A	N/A

(Power factor : 0.95)

The state characterization in probabilistic security assessment considers dynamic as well as steady state aspects. To determine dynamic aspect, the angle difference of generators is investigated.

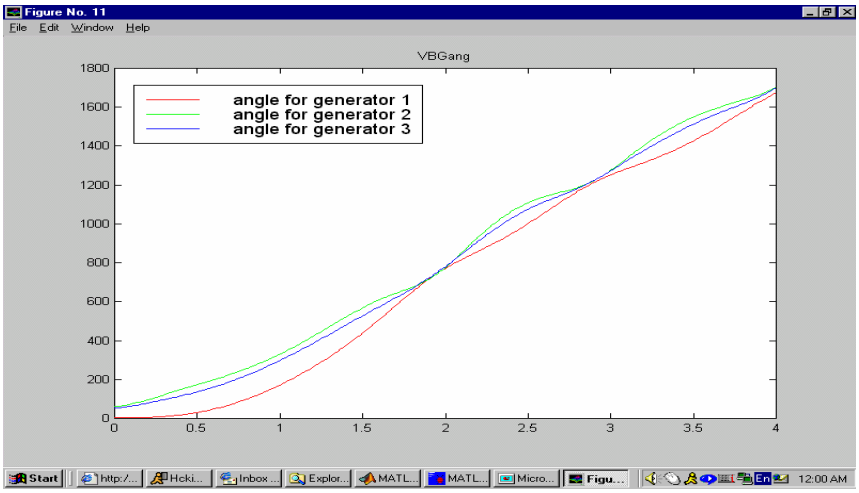

Fig. 1 The Angle Curves of Each Generator (when clearing time is 0.83 with a fault on line 5-7)

An example of angle graphs, when clearing time is 0.83 with a contingency on transmission line 5-7 and mean system loads, is shown in Fig. 1. The angle curves of all generators are similar, and the system is stable. That means the system is dynamically secure. In steady state, satisfaction of load without violation of constraints and voltage stability studies are investigated. With the same condition, there is no load curtailment with satisfaction of constraints. The voltage stability index of the overall system is the largest among voltage stability indicators for each bus. This value is compared with a threshold value. When it is larger than the threshold value, the system is near to a collapse point. Here, the threshold value is set as 0.3. With a contingency on line 5-7, voltage stability indicator is less than the threshold value. The system is regarded as stable in a contingency on 5-7. Since a system is satisfied both dynamic aspect and steady state aspect, the integrated security for a contingency on line 5-7 is secure and a system belong to "group-one".

The complexity of state characterization does not influence the procedure of Monte-Carlo Simulation but does effect state characterization itself. The consideration of dynamic aspect may characterize more systems unsafe among considered cases. This study was also conducted by varying the system load. The status of transmission lines, generators and load levels are the elements of feature vector, e. g. X_i = [1, 1, -----, 0, -----, 1, 1, -----, 1, -----, 1, 0.95]. Since WSCC has 9 transmission lines and 3 generators, the dimension of feature data is 13 including system load level.

The probability and frequency of each operating state is shown in Table 3. The system operating states can provide a conceptual basis for making security decisions in operational and long term planning. The proposed method using the Bayes classifier gives almost the same results as straight Monte-Carlo simulation. Each simulation is carried out for 300 years or until convergence criteria is satisfied. This result can be a little different when using different seeds. From the Table 4, it can be seen that proposed method has much less computation time than the straight Monte-Carlo simulation due to the reduced time for state characterization. While straight Monte-Carlo simulation requires state characterization for each sampled state, the proposed method needs state characterization only for selected sampling states (3967 feature vectors). As expected, simulation time of the proposed method is only 5.6 % of the straight Monte-Carlo simulation.

Table 3(a) and (b) The result of each operating state with load variation

(a) Probability

	Normal	Alert	Emergency
Proposed Method	0.0438	0.0416	0.9145
Monte-Carlo Simulation	0.0441	0.0416	0.9143

(b) Frequency (occurrences/year)

	Normal	Alert	Emergency
Proposed Method	41.680	1.795	39.415
Monte-Carlo Simulation	41.860	1.787	39.243

Table 4 The Classification Rate and simulation time

	Classification rate	Simulation time(min)
Proposed Method	99.85%	220.59
Monte-Carlo Simulation	N/A	3961.09

6. CONCLUSIONS

A method for security assessment employing the Bayes classifier is proposed in this paper. The WSCC has been used to demonstrate the efficiency of the proposed method. Case study shows that Monte-Carlo simulation using the Bayes classifier can be used to overcome the problem of the large amount of computation time required of straight Monte-Carlo simulation. The results indicate that simulation time of the proposed method is only 5.6 % of the straight Monte-Carlo simulation. The classification accuracy of Bayes classifier is 99.85%. In practice, probabilistic security evaluation methods are generally applied to reduced equivalent models or sections of systems that are of interest. However, research needs to continue to increase the capability of methods to deal with large networks.

7. ACKNOWLEDGEMENTS

This work reported in this paper is partly supported by Texas Advanced Technology Program and NSF Grant ECS-9903747.

8. REFERENCES

[1] Balu, N.; Bertram, T.; Bose, A.; Brandwajn, V.; Cauley, G. et al. 1992. On line power system security analysis. In *Proceedings of IEEE*. 80(2): 262-280.

[2] Billinton, R. 1969. Composite system reliability evaluation. *IEEE Transactions on Power Apparatus & Systems* PAS-88(4): 276-281.

[3] Patton, A. D.; Singh, C.; and Robinson, D. G. 1998. The impact of restructuring policy changes on power grid reliability. Final Report, Project SAND98-2178, Sandia National Laboratories, Albuquerque, NM.

[4] Singh, C. and Billinton, R. 1977. *System Reliability Modelling and Evaluation*. London: Hutchinson Educational.

[5] Kessel, P. and Glavitch, H. 1986. Estimating the Voltage Stability of a Power System. *IEEE Transactions on Power Delivery* 1(3): 346-354.

[6] Aboreshaid, S.; Billinton, R.; and Fotuhi-Firuzabad, M. 1996. Probabilistic Transient Stability Studies Using the Method of Bisection. *IEEE Transactions on Power Systems* 11(4): 1990 - 1995.

[7] Lester H. Fink and Kjell Carlsen. 1978. Operating under Stress and Strain. *IEEE spectrum*.

[8] Duda, R. O. and Hart, P. E. 1973. *Pattern Classification and Scene Analysis*: John Wiley & Sons.

[9] Yoh-Han Pao. 1989. *Adaptive Pattern Recognition and Neural Networks*: John Wiley & Sons, Longman.

[10] Hyungchul Kim and Singh, C. 2003. Steady-state and dynamic security assessment in composite power system**.** In *2003 IEEE International Symposium on Circuits and Systems*. 3: 25-28.

[11] Peter W. Sauer and Pai, M. A. 1997. *Power System Dynamics and Stability*. First edition: Prentice Hall.