Research Article

Probabilistic dynamic security assessment of large power systems using machine learning algorithms

Sevda JAFARZADEH, Veysel Murat İstemihan GENÇ*

Department of Electrical Engineering, Faculty of Electrical and Electronics, İstanbul Technical University,
İstanbul, Turkey

Abstract: Due to extensive utilization of intermittent energy sources in recent years, deterministic approaches cannot provide an accurate security assessment for power systems under large uncertainties. Therefore, probabilistic approaches have become crucial for making decisions based on more reliable assessments. In this paper, a new method based on machine learning and proper sampling techniques is proposed to overcome the difficulties of the conventional Monte Carlo approaches used in power system security assessment. The main purpose of the proposed method is to accurately quantify the dynamic security related risk at a forecasted operating condition of a power system utilizing a large number of intermittent energy sources, e.g., wind, which greatly extends the uncertainties in its operation. This is achieved through the proposed method, which captures an accurate probability distribution of the system's dynamic performance associated with both transient and small-signal angle stability. The accuracy of the fitted distribution is attained by adopting a generalized Pareto (GP) distribution for the left-tailed region that includes severe and rare cases using a multilayered perceptron neural network with the Relief feature selection technique, which speeds up the exceedance sample generation process required for the GP distribution. The Latin hypercube sampling technique, which samples the search space evenly, is proposed to create a dataset for training the neural network. To generate the Monte Carlo instances, the Gibbs sampling approach, which considers the correlation between random variables besides its simplicity, is utilized.

Key words: Power system stability, probabilistic security assessment, power system security, neural networks, feature selection

1. Introduction

Nowadays, power systems are operated under increasingly changing conditions as they are integrated with various intermittent renewable energy sources. The use of renewable energy sources introduces a considerable amount of uncertainty in the operation of power systems, making the conventional approaches that adopt deterministic security assessment less reliable. In order to take a proper preventive or corrective control action in the case of an alert or an emergency state, system operators should rely on a more realistic assessment of the system's security level, which cannot be obtained through deterministic approaches [1]. The necessities of applying probabilistic dynamic security assessment are studied in [2,3].

Power system security assessment can be classified into two broad categories: (a) static security assessment, which considers the steady-state behavior of the system, and (b) dynamic security assessment (DSA), in which the power system's dynamics and stability are taken into account. In recent years, DSA has attracted

---

*Correspondence: gencis@itu.edu.tr

more interest because of widespread blackouts caused by instabilities. These instabilities could be in the form of one or more of the following: angle, voltage, or frequency instabilities.

Probabilistic security assessment was first introduced by Wu and Tsai [4]. There are two types of methods for probabilistic security assessment: (a) analytic method and (b) simulation. In the analytic method [5,6], a probabilistic security index is developed by using statistical information of the uncertainties and mathematical relations without doing simulations repeatedly. One of the difficulties of this approach is due to the analysis in a high-dimensional parameter space when a large number of uncertainties are considered. The other problem with this method arises when the uncertainty of loads and generations are considered, since the analytic method needs to compute security translation rates in the case of uncertain loads and generations. In [1], a probabilistic security assessment based on security regions is introduced to overcome the difficulties related to the analytic method. In simulation [7], which is an alternative to the analytic method, the probability distribution of the output is obtained by performing a large number of simulations. With this approach, any uncertainty related to the system can be easily characterized. Monte Carlo (MC) is the most commonly used simulation method for probabilistic security assessment. One of the difficulties with MC is its heavy computational burden for high precision. Therefore, it is not appropriate to directly apply MC in order to generate cases that have a low probability of occurrence. However, some research has been carried out to put MC into practice for probabilistic security assessment and to overcome the difficulties of this method. In [8], a two-point estimate method was used to cut down on the computational burden, whereas a probabilistic collocation method is proposed in [9] for the problem of power system damping and voltage collapse. The problem with the methods applied in [8,9] is the assumption that the output to be estimated has a symmetric distribution. To overcome this difficulty, the generalized Pareto (GP) distribution is adopted in [10] for the tailed region of the output of the system performance related to small-signal stability, while a linear regression model is used to identify the exceedance sample (ES) regarding the tailed region. However, this approach suffers from not being able to distinguish the exceedance instances accurately, especially when the relation between the instances and the corresponding dynamic performances of system is complex. In order to remedy this matter, in this paper, we propose using a multilayered perceptron (MLP), a neural network that is able to map such a complex relation with higher accuracy than the linear regression model, to identify the exceedance instances for a given system performance during ES generation. Moreover, before training an MLP, Relief, a fast feature selection method, is implemented to identify the relevant features to enhance the accuracy of the trained neural network, while it also reduces the training time. The proposed methodology is applied for transient security assessment (TSA), as well as small-signal angle security assessment (SSSA). During the generation of MC instances, Gibbs sampling is adopted. This technique enables us to consider correlation between random variables in the generation of MC instances and give a more realistic view of the probability distribution of an output. Thus, with the proposed method encompassing the novelties above, the risk of a forecasted operating condition of a power system associated with the dynamic performances of interest can be computed more accurately.

2. Proposed methodology

In this study, we propose a new methodology enabling the system operators to efficiently make an accurate probabilistic security assessment for large-scale power systems operating under considerable uncertainties. The method involves the dynamic security assessment associated with angle stability under both small and large disturbances in interconnected systems with intermittent power generation. Using the method, these dynamic security-related risks of operating the power system under a forecasted condition can be calculated quite efficiently.

The method starts with considering a single point estimate of a forecasted operating condition, which is defined by the active power outputs of intermittent generation units and the existing load demand. This operating condition cannot be fully known because of the uncertainties inherent in the system due to randomly varying power generation and load demand. A sufficiently small period of time, for which the assessment is to be made, is considered while a normal (Gaussian) distribution with a mean equal to the forecasted value of each random variable is assumed.

The main objective of the proposed methodology is to compute the risk associated with the transient and small-signal angle stability. This requires an accurate computation of the probability distribution of each stability related system performance. For the left-tailed region of the system performance distribution where the cases with severe performance are encountered, a GP distribution is adopted, whereas the remaining part is fitted by a normal distribution. For fitting the GP distribution, an ES, which is a collection of severe and rare cases, is needed. In this paper, the generation of the ES, which requires an excessive computation, is efficiently obtained using machine learning techniques. Therefore, the first step of the process is the dataset generation for training a neural network; see Section 2.1. The next step is designing a good predictor for system performance to be used for distinguishing the exceedance instances; see Section 2.2. This is followed by the generation of MC instances for fitting the normal distribution; see Section 2.3. The next step is the ES generation using machine learning approaches; see Section 2.4. Finally, the distributions for the system performances are obtained (Section 2.5) followed by the computation of the associated risks (Section 2.6). A flowchart of the proposed methodology is presented in Figure 1.
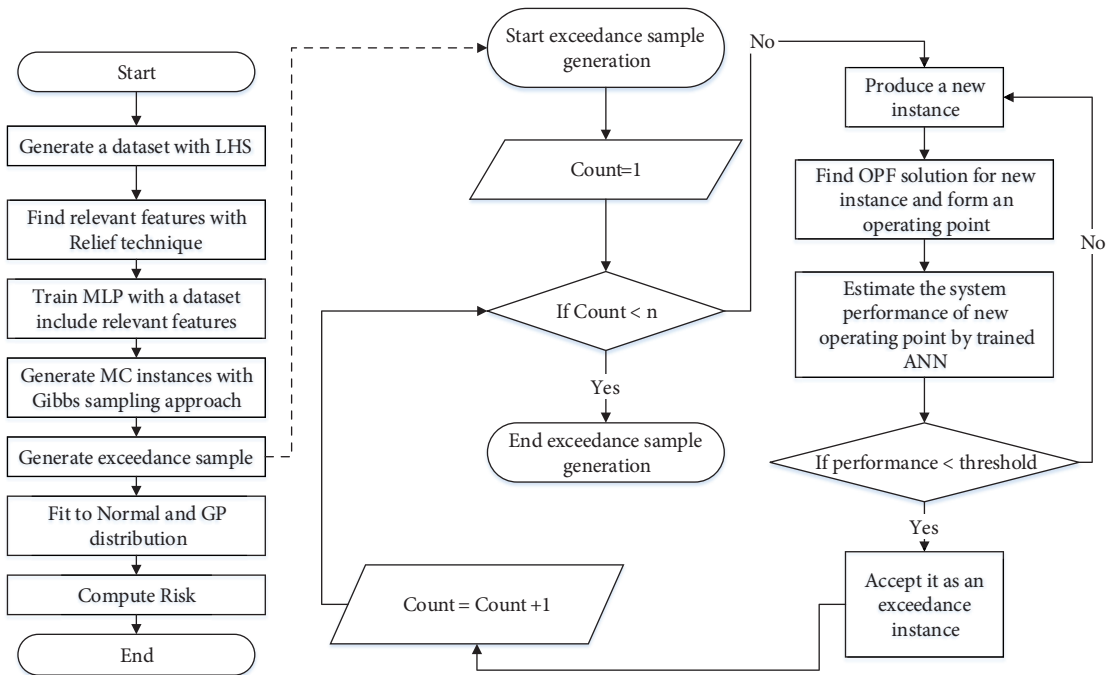

Figure 1. Flowchart of the proposed method including exceedance sample generation.

2.1. Generation of dataset for training neural network

A limited number of different operating conditions specified by the power outputs of wind generation units and load demands are produced, considering the uncertainties in their forecasted values. The Latin hypercube

sampling (LHS) [11] method is used to sample the search space evenly. For each operating condition produced, an optimal power flow solution, namely, an operating point (OP) is found. A number of dynamic simulations, including time-domain simulations under contingencies and modal analyses, are performed to evaluate the system's dynamic performances at each of these OPs. Thus, a dataset composed of steady-state values of OPs, which are their bus voltages, real and reactive power injections, and system performances, is generated to be used for training a neural network to predict each system's performance at its OPs.

For TSAs, the system's performance, η_{TS}, is computed as

$$\eta_{TS} = \frac{CCT - CT}{CT}, \tag{1}$$

where CT is the clearing time of a critical fault and CCT is its critical clearing time. The system's performance associated with small-signal angle stability, η_{SS}, is defined as

$$\eta_{SS} = \xi - \xi_{th}, \tag{2}$$

where ξ and ξ_{th} denote the damping ratio of the dominant electromechanical mode and its threshold, respectively.

2.2. Feature selection and training neural networks to predict system performances

The dataset created in the previous step is used to train a neural network that will predict each system performance at any OP in order to obtain an ES without an excessive computation. The MLPs are used for the regression problems of interest, which are system dynamic performance predictions [12].

Without using a neural network, the generation of a reasonably large ES takes an excessive amount of time, because an exceedance instance has a low probability of being sampled. In this case, a large number of instances will be examined through a time-consuming dynamic simulation. Instead of these computations, the neural network is used to predict the system's performance at the OPs, and thus it will speed up the process of obtaining the ES. A large dataset for training the neural network would not be appropriate, since an exact evaluation of the system's dynamic performance at each OP can only be obtained by the time-consuming dynamic simulations.

Prior to training a neural network, a feature selection method should also be used to cut down on the number of features to be adopted as inputs to a neural network. To reduce the training time and to enhance the performance of the MLPs, Relief [13], which is a fast and a reliable feature selection method, is used to determine the relevant features to the regression problems of interest. The number of inputs to the MLP would be equal to the number of features selected, whereas it has only one output for the system performance. Only one hidden layer with the number of neurons that is specified through a grid search would be sufficient to obtain an acceptable performance.

2.3. Generation of instances using Gibbs sampling

For a tolerable error with a predefined confidence level, the number of required instances to be generated by Gibbs sampling is determined according to the central limit theorem [14].

Using this approach, for a tolerable error ε with a confidence level α, the required number of instances n is calculated based on the following probability,

$$P\left\{ \left| \bar{X}_n - \mu \right| < z_{\alpha/2} \frac{\sigma}{\sqrt{n}} \right\} = 1 - \alpha, \tag{3}$$

$$n = (z_{\alpha/2} \times \sigma/\varepsilon)^2, \tag{4}$$

where $\bar{X}_n$ is the sample mean, μ is the expected value, σ is the standard deviation, and $z_{\alpha/2}$ is the upper percentile for the standard Gaussian distribution, $z_{\alpha/2} = Q^{-1}(\frac{\alpha}{2})$, where Q^{-1} represents the inverse function of a normal cumulative density function.

The sample standard deviation of the system performance is calculated based on the previously generated training dataset for the neural network.

For a given dynamic performance, the new dataset of OPs is produced by the method of Gibbs sampling, a type of MC sampling, to represent its initially guessed normal distribution [15]. As explained in Section 2.1, any instance in the sample is created by the performance evaluation of an OP that is obtained as the optimal power solution for a newly generated operating condition.

2.4. Generation of an exceedance sample

A GP distribution is used to fit the left-tailed region of the system performance distribution. For the GP distribution, an ES that includes the instances resulting in a system performance below a predetermined threshold is required [16].

Most of the instances that have previously been produced by the MC sampling method are not exceedance instances due to the fact that any exceedance instance has a very low probability of being sampled. New operating conditions are to be produced to generate new OPs at which the system performance is predicted by the trained neural network. If the system performance of the OP is below a threshold, it is considered an exceedance case, otherwise another OP is to be produced until the required number of exceedance instances are collected. For each exceedance instance, a deterministic dynamic security assessment through a time–domain simulation or modal analysis is made to validate the system's performance determined by neural network. The system performance of the exceedance instances will be used to fit the left-tailed regions of the probability density functions (PDFs) associated with the system performance. A flowchart for the ES generation process is presented in Figure 1.

2.5. Fitting the probability distribution

A GP distribution is fit to the exceedance instances, whereas the other instances are used for fitting a normal distribution. Thus, a more accurate distribution for the left-tailed region of a system performance, where the ES resides, is obtained and the calculation of risks related to poor performances becomes more reliable. The cumulative distribution function for a GP distribution is

$$F(x; k, \mu, \sigma) = \begin{cases} 1 - \left(1 + k\frac{(x-\mu)}{\sigma}\right)^{-\frac{1}{k}} & for\, k \neq 0 \\ 1 - e^{-(\frac{x-\mu}{\sigma})} & for\, k = 0 \end{cases}, \tag{5}$$

where μ, σ, and k are the threshold, scale, and shape parameters of the distribution, respectively.

To make the overall distribution (Figure 2) (the combination of GP and normal distributions) consistent, the area under the PDF is to be made equal to 1. Therefore, the following is performed: (a) GP distribution must be multiplied by $\frac{n_{exc}}{n_t}$, where n_{exc} is the number of exceedance instances and n_t is the total number of instances that are examined, and (b) the probability of performance must be divided by $s = A + B$,
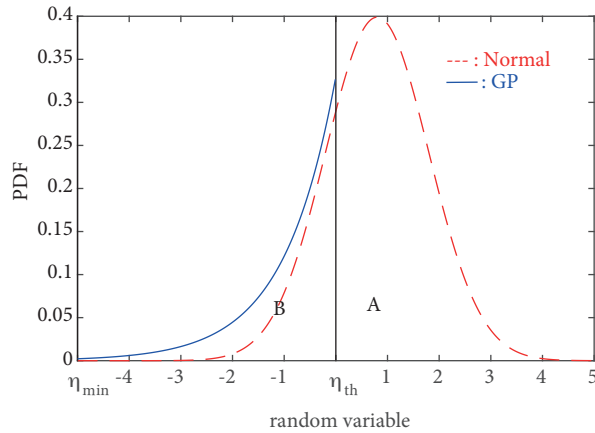
Figure 2. Combination of generalized Pareto and normal distributions.

$$A = F_{GP}\left(\eta_{th}\right)\frac{n_{exc}}{n_t} - F_{GP}\left(\eta_{min}\right)\frac{n_{exc}}{n_t} \tag{6}$$

$$B = 1 - F_N\left(\eta_{th}\right), \tag{7}$$

where F_N and F_{GP} are the cumulative distribution functions for the normal and the GP distributions, respectively. The threshold and the minimum values of the system performance are denoted by η_{th} and η_{min}, respectively.

2.6. Computation of risk

In order to compute the risk of the operating condition, a suitable severity function should be defined. In this study, a combination of a quadratic and a stepped function,

$$S'\left(\eta\right) = \begin{cases} 0 \, \eta < -0.05 \\ \left(\eta + 0.05\right)^2 - 0.05 \, -0.05 < \eta < 0.05 \\ 1 \, \eta > 0.05 \end{cases} \tag{8}$$

is properly scaled to define the severity function, $S(\eta) = w_\eta S'\left(\eta\right)$, for a given dynamic performance η, where w_η is a properly selected scaling factor selected for the performance.

Using the severity functions defined, the risk of the operating condition for both transient stability and small-signal angle stability are calculated. The risk related to transient stability for contingency i, $Risk_{TS,i}$, can be calculated as

$$Risk_{TS,i} = P_i \int_{-1}^{+\infty} P\left(\eta_{TS,i}\right) S(\eta_{TS,i}) d\eta_{TS}, \tag{9}$$

where P_i represents the probability of the occurrence of contingency i. The risk related to small-signal angle stability can be computed by the following:

$$Risk_{SS} = \int_{-1}^{1} P\left(\eta_{SS}\right) S(\eta_{SS}) d\eta_{SS} \tag{10}$$

3. Results

3.1. Test system

A modified version of the IEEE 68-bus, 16-generator test system [17] is selected as the power system in which all the studies in this paper are performed. To study the efficiency of the proposed methodology of probabilistic security assessment, three wind generation units, as intermittent power sources, are added to the system at the buses numbered 7, 30, and 37 (Figure 3). In order to make a TSA, first a set of critical contingencies are determined through a contingency scan performed by the time–domain simulations using the software DSATools [18] for the system operating at a range of OPs generated around a forecasted OP. Although the system is secure for all credible contingencies at the forecasted OP, three critical contingencies (A, B, and C), for each of which the system is insecure at some of the generated OPs, are found: contingencies A and B are the three-phase faults at bus 29 cleared by tripping lines 29–28 and 29–26, respectively, whereas contingency C is a three-phase fault at bus 22 cleared by tripping line 22–21 (Figure 3). For the generated OPs, the critical clearing time (CCT) computed for each critical fault varies between two numbers below (insecure case) and above (secure case) the clearing time $CT = 5\,cycles$, which is assumed for all faults. Clearly, even if the system is secure at the forecasted OP, the risk is not zero, since it can become insecure for some contingencies when its OP deviates from the forecasted value due to variations in loading and especially in intermittent generation.

3.2. Feature selection and neural network performance results

For each point in a set of 190 OPs, which are generated by the LHS technique around the forecasted OP, time–domain simulations have been performed to compute the CCT values of the critical contingencies, while the damping ratio associated with the dominant electromechanical mode is also computed by the software DSATools [18]. The OPs are essentially the standard AC-OPF solutions, which minimize the fuel cost under some security constraints, to the operating conditions generated, and they are computed using the software MATPOWER [19].

For the produced dataset, the features are ranked based on their relevancies using Relief [15], the feature selection technique chosen in this work. With the relevant subset of features, the MLPs are trained for predicting the targets, which are the CCT values and the damping ratio. MATLAB [20] is used for implementing the feature selection and training the MLPs, each of which has 50 neurons in its single hidden layer. In order to choose the best number of features in each case, the MLP is trained with different number of relevant features and its performance in prediction is considered as a basis for the selection. Table 1 presents the performance of the MLP trained with different number of features for predicting the CCT of contingency A. The results show that the best performance is obtained if a set of 50 features is used. Moreover, since training with a smaller number of features takes less time and reduces the complexity of the model, this set of features is found to be more favorable. The same procedure is followed for the other contingencies and small-signal security assessment (SSSA). Table 2 presents the performance of the MLPs trained with the set of features selected for the three critical contingencies and the small-signal security assessment.

3.3. Risk assessment

Using the sample standard deviations of the system performances corresponding to the points previously generated by LHS, the required number of MC instances to be obtained by the Gibbs method for the initial distribution of each performance is obtained (Table 3). In the present study, the maximum tolerable error is specified as 5% for TSA and 1% for SSSA and the confidence level is selected as 95%. It means that we are 95% sure that any error we make is less than 5% for TSA and less than 1% for SSSA.
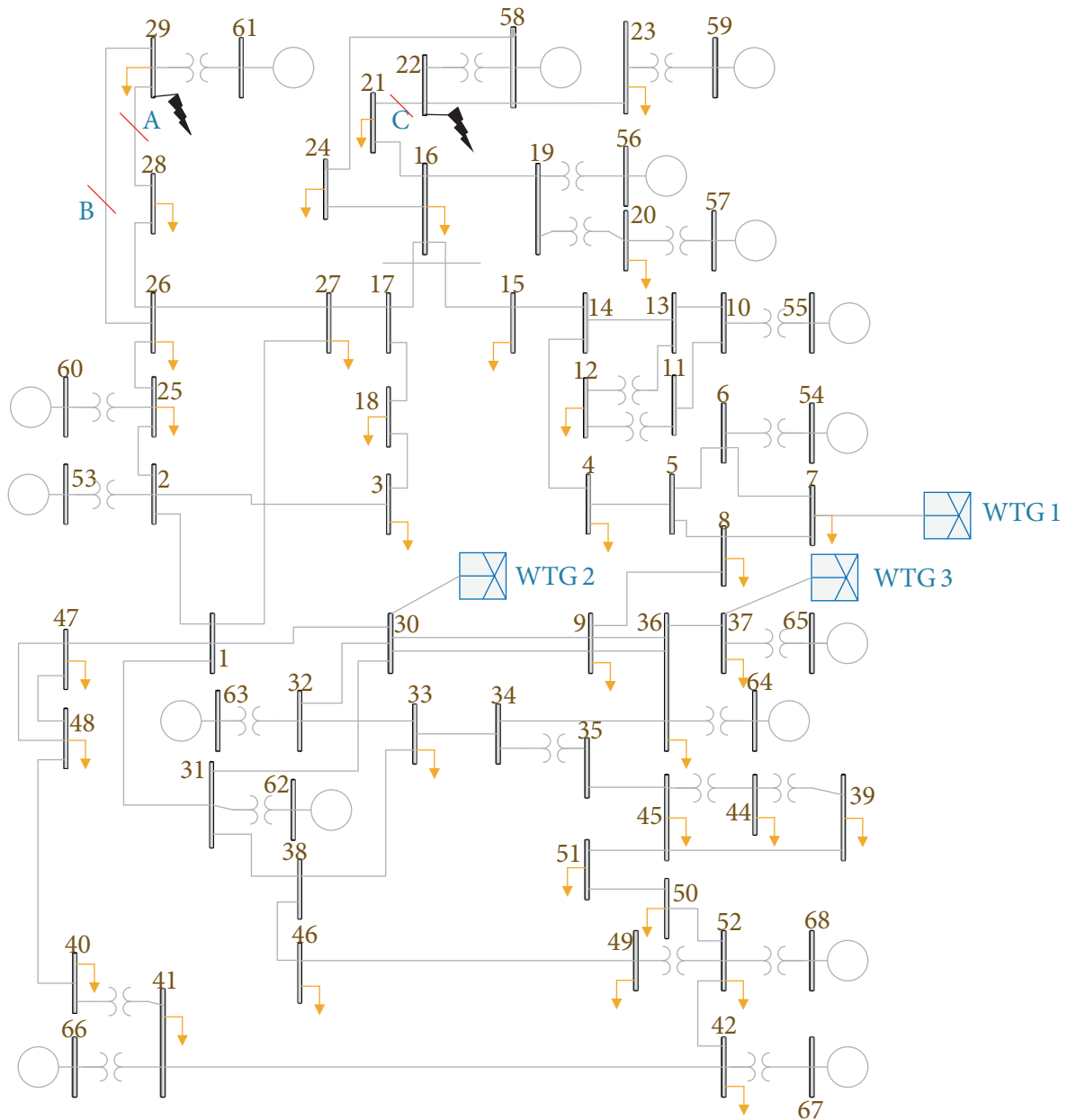
Figure 3. Test system.

The MC instances are used to fit the normal distribution, which is an initial approximation of the output distribution. Moreover, the exceedance instances, which are distinguished by the contribution of machine learning tools, are utilized to fit the left-tailed region of the distribution. The number of exceedance instances to be generated for the TSA and SSSA are selected as 60 and 30, respectively. In the process of exceedance sample generation, the total number of required instances (iterations), including the discarded instances, are given in Table 3. Using a workstation with an Intel Core i7 3.4 GHz, the times required for the ES generation with and without machine learning tools are also provided in Table 3. Clearly, the proposed methodology for the dynamic security assessments of interest is much faster when the machine learning tools are utilized.

Table 1. Feature selection and MLP performance for contingency A.

Number of features	Validation error	Training error	Test error	Time (s)
50	2.6×10^{-4}	3.2×10^{-5}	4.3×10^{-4}	5.07
100	8.9×10^{-4}	7.0×10^{-6}	1.7×10^{-3}	14.17
150	5.1×10^{-3}	2.8×10^{-3}	7.4×10^{-3}	30.31
244	2.2×10^{-2}	1.5×10^{-3}	1.5×10^{-2}	38.79

Table 2. MLP performances for SSSA and TSA.

Dynamic assessment	Number of features	Validation error	Training error	Test error	Time (s)
TSA (cont. A)	50	2.6×10^{-4}	3.2×10^{-5}	4.3×10^{-4}	5.07
TSA (cont. B)	50	2.6×10^{-4}	2.3×10^{-4}	2.5×10^{-4}	4.34
TSA (cont. C)	50	5.5×10^{-4}	1.3×10^{-4}	1.0×10^{-3}	4.31
SSSA	100	4.5×10^{-5}	4.2×10^{-10}	6.5×10^{-5}	19.27

Table 3. Number of iterations and time required for ES generation.

	Number of MC instances	Total number of iterations for ES	Time required without using ML (minutes)	Time required using ML (minutes)
TSA (cont. A)	106	238	25.9	6.6
TSA (cont. B)	100	772	84	7.5
TSA (cont. C)	241	4638	504.8	14.2
SSSA	80	200	21.6	3.2

Figure 4 illustrates the overall probability distribution of each system performance, which is obtained by the proposed method using the relevant MC instances and the ES. In Figure 4, the vertical lines separate the GP distributions fitted to the left-tailed regions from the normal distributions, while these distributions suggested by the proposed method are also compared with the normal distributions (dashed) obtained by MC instances only. The GP and initially guessed normal distributions over the left-tailed regions in which the exceedance samples reside are also given in Figure 5 in more detail.

In order to show the effectiveness of the proposed methodology, the risks associated with the system's dynamic performances are computed based on the probabilistic security assessments made both by using the conventional MC technique and the proposed method in this paper (Table 4). It is clear that the proposed method provides a more realistic risk assessment than the conventional probabilistic method, while no risk would be detected at all if a probabilistic approach is not adopted.

4. Conclusion

Conventional dynamic security assessment methods using deterministic approaches are not reliable for modern power systems integrated with distributed generations introducing a considerable amount of uncertainties in
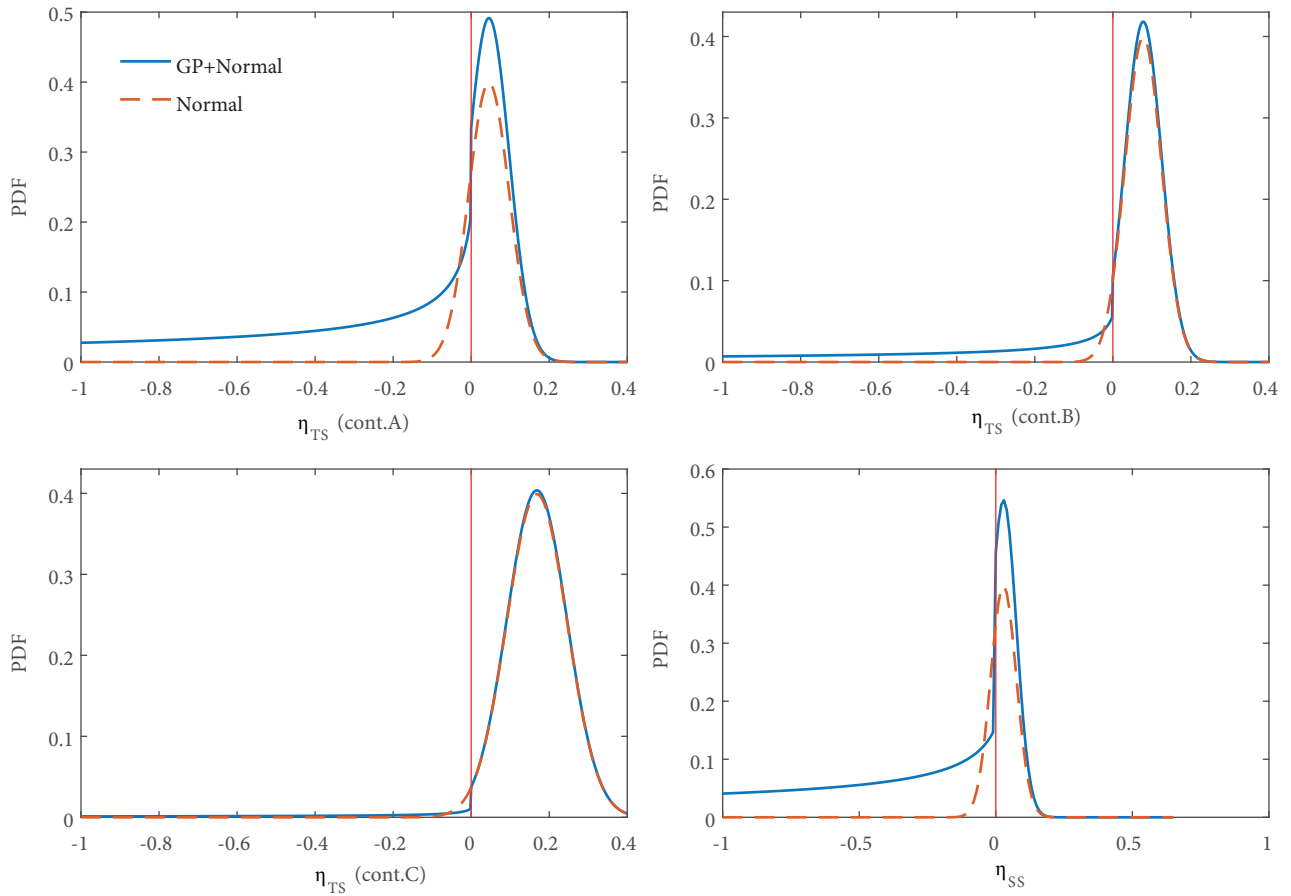
Figure 4. Probability density functions (PDFs) for dynamic performances.

Table 4. Risks computed by the conventional and the proposed methods.

Dynamic assessment	Risk computed by the conventional MC method	Risk computed by the proposed method
TSA (cont. A)	0.0112	0.0154
TSA (cont. B)	0.0022	0.0044
TSA (cont. C)	0.0012	0.0010
SSSA	0.0033	0.0264

systems' operating conditions. Therefore, a probabilistic approach should be adopted for taking preventive control actions when they are needed. MC simulation methods for probabilistic security assessment are not appropriate due to their computational burden and time consuming procedures. While they are used to perform a dynamic security assessment, a large number of OPs are to be generated; therefore a large computation time is needed, to attain an acceptable accuracy. Instead of this approach, as proposed in this paper, it is more reasonable to generate larger numbers of instances just in the tailed region of the distribution where the low system performance that creates risk is present. In the proposed methodology, the exceedance instances are used to improve the accuracy of the model for the left tailed region of the system performance distribution. Thus, the risk could be computed more accurately.
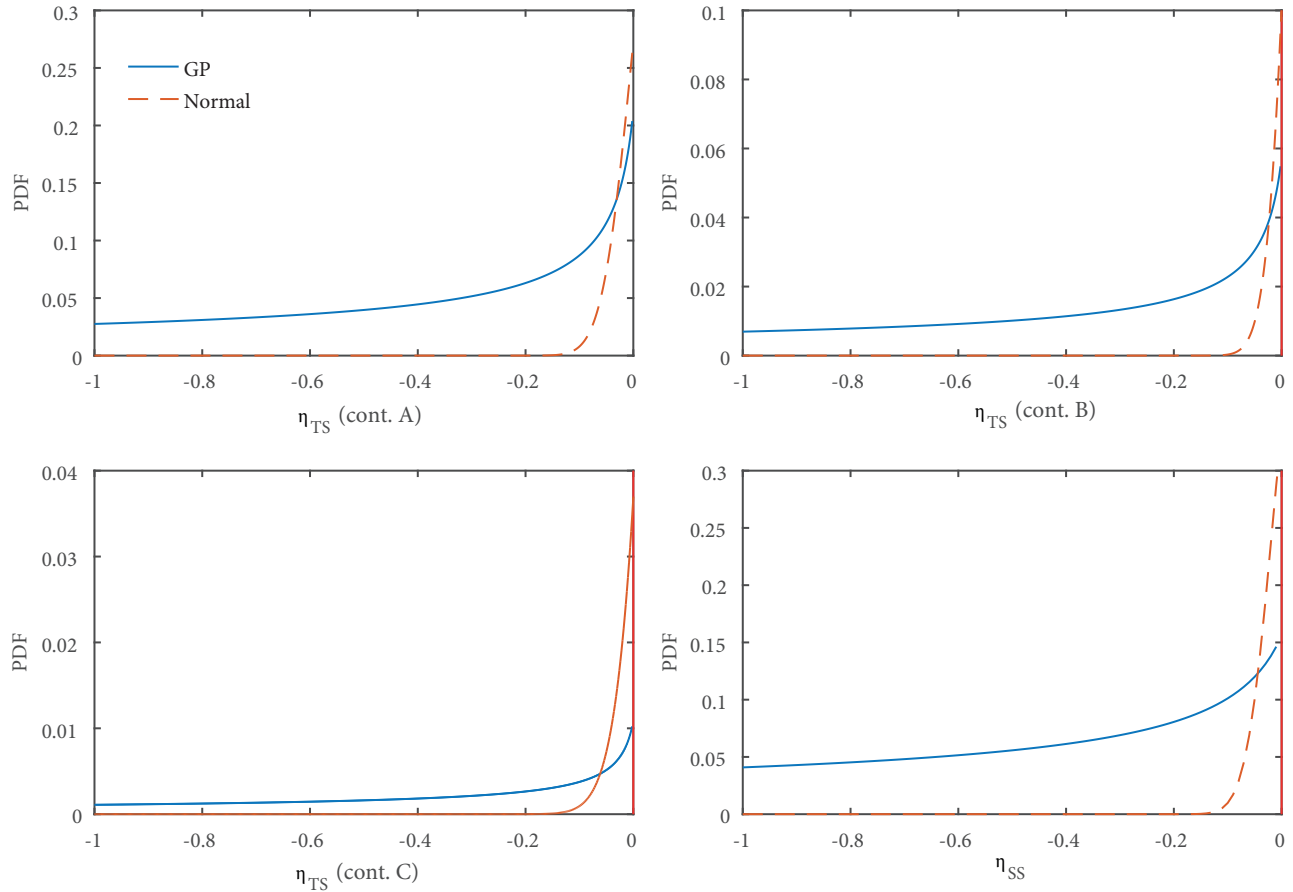
Figure 5. Probability density functions (PDFs) over the tailed region (ES).

Exceedance sample generation can be time-consuming due to the low probability of its instances being sampled; therefore, a large number of simulations are needed to obtain a sufficient number of exceedance instances. In this step, the proposed neural networks with an effective feature selection method contribute to speed up the process.

In order to demonstrate the efficiency of the proposed method, a test system with 68 buses and 3 wind generation units is used. The results show that the proposed probabilistic security assessment method gives a more realistic level of risk than the deterministic studies. Moreover, the method is fast enough to be applied to online probabilistic assessment. The proposed methodology is also compared with one using the conventional MC approach. The risk for one forecasted operating condition is computed with both MC and the proposed methodology. When compared to the conventional MC approach, since the proposed methodology utilizes more information to approximate the probability distribution of the system performance, the risk obtained by the proposed method is more accurate than the risk computed by the conventional approach. In addition, the proposed method requires much less computation time to create an ES of a sufficient size. In the proposed methodology, the use of machine learning approaches for the generation of an exceedance sample drastically decreases the computation time and makes the overall method more efficient. The performance of MLP neural networks is improved by integrating a feature selection algorithm. This approach not only the decreases their prediction error but also reduces their training time drastically.

References

[1] Wang D, Yu Y, Fu C, Zhang J, Wu J, Jia H, Chen X. Security region based probabilistic security assessment of power transmission system basic concepts. In: IEEE 2005 Transmission and Distribution Conference and Exhibition: Asia and Pacific: IEEE/PES. pp. 1-5.

[2] Rueda JL, Colomé DG, Erlich I. Assessment and enhancement of small signal stability considering uncertainties. IEEE T Power Syst 2009; 24: 198-207.

[3] Rueda JL, Erlich I. Probabilistic framework for risk analysis of power system small-signal stability. Proc Institution Mech Eng O 2012; 226: 118-133.

[4] Wu F, Tsai YK. Probabilistic dynamic security assessment of power systems-I: Basic model. IEEE T Circuits Syst 1983; 30: 148-159.

[5] Wu FF, Tsai YK, Yu YX. Probabilistic steady-state and dynamic security assessment. IEEE T Power Syst 1988; 3: 1-9.

[6] Billinton R, Kuruganty PR. Probabilistic assessment of transient stability in a practical multimachine system. IEEE T Power App Syst 1981; 7: 3634-3641.

[7] Ming D, Renching D, Yacheng L. Monte-Carlo simulation approach to probability stability. Journal of Tsinghua University 1999; 3: 79-83.

[8] Verbic G, Canizares CA. Probabilistic optimal power flow in electricity markets based on a two-point estimate method. IEEE T Power Syst 2006; 21: 1883-1893.

[9] Preece R, Woolley NC, Milanović JV. The probabilistic collocation method for power-system damping and voltage collapse studies in the presence of uncertainties. IEEE T Power Syst 2013; 28: 2253-2262.

[10] Preece R, Milanović JV. Efficient estimation of the probability of small-disturbance instability of large uncertain power systems. IEEE T Power Syst 2016; 31: 1063-1072.

[11] Stein M, Large sample properties of simulations using Latin hypercube sampling. Technometrics 1987; 29: 143-151.

[12] Rosenblatt F. Principles of Neurodynamics: Perceptions and the Theory of Brain Mechanism. Washington, DC, USA: Spartan Books, 1961.

[13] Kira K, Rendell LA. The feature selection problem: traditional methods and a new algorithm. In: AAAI'92 Proceedings of the Tenth National Conference on Artificial Intelligence; 12–16 July 1992; San Jose, CA, USA. Vol 2: pp. 129-134.

[14] Driels MR, Shin YS. Determining the number of iterations for Monte Carlo simulations of weapon effectiveness. Naval Postgraduate School, Monterey, CA, USA 2004.

[15] Smith AF, Roberts GO. Bayesian computation via the Gibbs sampler and related Markov chain Monte Carlo methods. J Royal Stat Soc Series B Stat Methodol 1993; 1: 3-23.

[16] Pickands III J. Statistical inference using extreme order statistics. Ann Stat 1975; 1: 119-131.

[17] Rogers G. Power System Oscillations. Boston, MA, USA: Kluwer Academic Publishers, 2000.

[18] DSATools^{TM}, (Version 14) [Computer software]. Surrey, BC, Canada.

[19] Zimmerman RD, Murillo-Sánchez CE, Thomas RJ. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. IEEE T Power Syst 2011; 26: 12-19.

[20] MATLAB 9.0, The MathWorks Inc. Natick, MA, USA, 2016.