International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.99-114
http://dx.doi.org/10.14257/ijsia.2015.9.12.11

Risk Assessment of Power System Security based on a Hybrid Optimization GP Method

Xiaobin Wu, Hui Li and Xiaolu Chen

State Grid Shandong Electric Power Company Linyi Electric Power Company, Linyi, Shandong, China
wuxiaobin001@126.com, lh_suhan@163.com, lylxl123@163.com

Abstract

In this paper, we propose a hybrid optimization algorithm based on Improved Differential Evolution (IDE) algorithm and Gaussian Process (GP). Firstly, the paper constructs the assessment index system using Fault Tree Analysis (FTA) based on the summary and classification of the factors that could affect the power system security. Secondly, establish the risk assessment model of power system security based on the hybrid optimization GP algorithm. Hyper-parameter of GP has a great influence on construction of evaluation model, while conjugate gradient method which is usually used has strong dependence on initial values and is easy to fall into local optimal solution. So the paper uses the IDE algorithm for the traditional Hyper-parameter optimization, then the optimal Hyper-parameter is used to construct evaluation model for power grid security risk assessment. In the process of improvement, this paper adds the local search (Bees accelerated evolution operation) and global search (Bees scout operation) thought of ABC algorithm into the DE algorithm to reduce the population size required by the algorithm. After that, do the risk assessment of power system by using the established assessment model. Finally, do the simulation experiments using the standard data IEEE-39 and IEEE-118 bus example, and besides compare the IDE-GP with other optimization model like ABC-GP, DE-GP, MA-GP, GA-GP, and the experimental results show that hybrid optimization algorithm has better performance in accuracy while the time-consuming difference is minor. The validity of the proposed method is also demonstrated.

Keywords: *Risk Assessment of Power System Security, Gaussian Process (GP), Improved Differential Evolution (IDE), Artificial Bee Colony*

1. Introduction

Power system risk assessment refers to acquire security operating states of power grid by means of mining some potential risk factors proactively. This active assessment approach significantly improves the regulatory capacity for power system and increases the robustness of power system. However, with the expanding of power system scale, together with the increase of complexity, it is necessary to further improve the accuracy of power system risk assessment to assure the reliability and safety of power system.

According to the Power System risk assessment problems, a great deal of research has been conducted, and the main method at present is deterministic assessment, probabilistic assessment [2-3], and risk assessment [4]. Deterministic assessment method like N-P criteria [5] was used for the risk assessment of power system problems in the early time. This method usually considers the severest accident, but ignores the existence of various uncertain factors in the complicated power system, and the results are too conservative. Probabilistic assessment methods include analytical method, the Monte Carlo method and so on. The literature [6] introduces Markov chain in stochastic process to the Monte Carlo simulation and applies the new method called MCMC to large-scale system evaluation.

ISSN: 1738-9976 IJSIA

The literature [7] presents a methodology for generating capacity adequacy evaluation of power systems including wind energy using sequential Monte Carlo simulation. Probabilistic assessment method considers the fault possibility of accidents, but not includes the severity of accident consequences. While risk assessment method considers both combines fault probability and severity, and defines the risk of an accident as the product of probability and consequences. For example, [8] proposed one new probabilistic risk assessment method for cascading failure based on the discussion of different component outage model. The literature [9] proposed a method for transient security risk assessment of power system based on risk theory and fuzzy reasoning. In the model proposed by [10], the paper regarded the failure possibility of overhead lines as a random fuzzy variable, and according that, constructed the failure possibility model based on the evidence theory. Besides that the utility function is used to measure the degree of dissatisfaction induced by failures which can better reflect the actual operation situation of power system. Thus, risk assessment method overcomes the insufficient of the accident frequency in deterministic assessment and accident severity in probabilistic assessment respectively, and is widely used in the field of power system security risk assessment at present.

The above methods have achieved certain effects as for risk assessment of power system security, but there are still some problems such as low time efficiency, strong subjective factors and other issues. In recent years, machine learning methods were widely used in different fields. Machine learning method can adaptively adjust the weights, so as to reduce the influence of subjective factors, improving the performance evaluation. On the basis of the establishment of the assessment index system using Fault Tree Analysis (FTA), the paper proposed a method for risk assessment of power system security based on a hybrid optimization GP method. The paper uses the Improved Differential Evolution (IDE) algorithm optimize the traditional Hyper-parameter, and then uses the optimal Hyper-parameter construct Gauss process regression model for power system security risk assessment. Finally through the numerous simulation experiments using the standard data IEEE-39 and IEEE-118 bus example, which compare the IDE-GP with other optimization model like ABC-GP, DE-GP, MA-GP, GA-GP, the experimental results show that hybrid optimization algorithm has better performance in accuracy while the time-consuming difference is minor. The validity of the proposed method is also demonstrated.

2. Establishment of Index System for Power System Security Risk Assessment

2.1. Security Risk Assessment Index System

Risk index is the key of risk assessment. In order to get accurate and meaningful security risk assessment for power system, only to establish a scientific and rational evaluation index system. To establish power system security risk assessment system based on multivariate analysis, first of all, the analysis for domestic and international power system security risk accidents is necessary, which could summarize and classify factors that affect power system security. It is the basis for assessment index system [11]. Through the analysis of some power system security accident factors in recent years, the paper summarized five major factors that caused large-scale risk of accidents: structure, technology, equipment, external and management. Since management is complex, the paper mainly considers structure, technology, equipment, and external in construction of index system. To establish an assessment system, the paper uses the Fault Tree Analysis (FTA) [12], which can identify and evaluate the risk of various systems. Not only to analyze the direct cause of accidents, but also deeply reveal the potential causes, using

both qualitative and quantitative analysis, meet the requirements of power system risk assessment.

Based on above analysis, the study puts Power System security risk as the primary index of assessment index system. Primary index was further divided, finally established a three-tier hierarchical risk assessment index system, which included one primary index, four secondary indices, fourteen tertiary indices. Power system security risk assessment index system is shown in Table 1.

Table 1. Power System Security Risk assessment Index System

Primary indices	Secondary indices	Tertiary indices
Power system security risk A1	Equipment risk B1	Transformer load factor C1
		Line load factor C2
		Underload transformers proportion C3
		Overload transformers proportion C4
	Structure risk B2	Voltage deviation C5
		Power angle stability margin C6
		Voltage stability margin C7
	External risk B3	Risk caused by lightning disasters C8
		Risk caused by snow disasters C9
		Risk caused by fire disasters C10
		Risk caused by other disasters C11
		Risk caused by external damage accidents C12
	Technology risk B4	Double-circuit parallel transmission lines cross line failure C13
		Double-circuit transmission lines synonyms phase cross line failure C14

2.2. Calculation of Security Risk Assessment Index

The indices of power system security risk assessment index system include both quantitative indices (C1-C7) and qualitative indices (C8-C14). For the qualitative indices, using ratings principle, make different degree of risk correspond to scores between 0-1. The degree of risk is proportional to the scores. Each score corresponding risk degree and system security level is shown in Table 2.

Table 2. Risk Assessment Scoring Standard

Scores	Definition description	Security level
0.1	Lowest	
0.2	Low	Security
0.3	Lower	
0.4	Medium to low	
0.5	Medium	Alert
0.6	Medium to high	
0.7	Higher	
0.8	High	Danger
0.9	Highest	

In order to construct samples used in the experiments, firstly, on the basis of the established risk index system, make the pairwise comparison between c1-c14 based on the

1-9 scale method shown as Table 3 and using Analytic Hierarchy Process (AHP) [13], Delphi method to construct judgment matrix $Z_i, i=1,...,4$, as shown in formula (1).

$$Z_i = \begin{bmatrix} 1 & z_{12} & ... & z_{113} & z_{114} \\ z_{21} & 1 & ... & z_{213} & z_{214} \\ ... & ... & ... & ... & ... \\ z_{201} & z_{202} & ... & 1 & z_{1314} \\ z_{141} & z_{142} & ... & z_{1413} & 1 \end{bmatrix} \quad (1)$$

Secondly, calculate the maximum eigenvalue of judgment matrix and its corresponding positive feature vector, and then normalize the feature vector to get the index weight vector; finally, using the weighted sum method for the indices at all levels to get composite indices of power system risk. Build the sample by the indices and weights.

Table 3. 1-9 Scale Method

Scale z	Definition description
1	Two sub-index ci and cj of equal importance for the upper index
3	Comparing the two sub-index, ci is slightly more important than cj
5	Comparing the two sub-index, ci is obviously more important than cj
7	Comparing the two sub-index, ci is much more important than cj
9	Comparing the two sub-index, ci is extremely more important than cj
2,4,6,8	Compromise scale between technology scaling
$z_{ij} = 1/z_{ji}$	Anti- Comparison of two indices

3. Power Grid Security Risk Assessment based on Hybrid Optimization Gaussian Process

3.1. Gaussian Process Regression

Gaussian Process (GP) [14], is also known as the normal random process, defined as a collection of random variables. Any finite number of random variables in the collection obwy joint Gaussian distribution, that is to say, for any set of random variables X and corresponding to the process state $f(X)$, the joint probability distribution of them follows n -dimensional Gaussian distribution. From the perspective of function space, all statistical characteristics of GP can be determined by its mean $m(x)$ and covariance $k(x, x')$, $x,x' \in R^d$ are arbitrary random variables, so the expressions of Gaussian Process can be defined as the formula (2):

$$f(x) \sim gp(m(x), k(x, x')) \quad (2)$$

In general, mean function $m(x)=0$ is introduced for the expression simplicity, the covariance function of GP is equivalent to the traditional kernels function of machine learning method. Different covariance function is selected for different data characteristics, we usually chose covariance function of infinitely differentiable squared exponential (SE), the function is also known as Gaussian kernel function. This paper takes the form of:

$$K(x_p, x_q) = \sigma_f^2 \exp[-\frac{1}{2l^2}(x_p - x_q)^2] + \sigma_n^2 \delta_{pq} \quad (3)$$

Where l is called hyper-parameters for the measure of correlation, larger value of l indicates smaller correlation between the input and output. σ_f is the signal standard deviation of the covariance function. σ_n is called noise standard deviation. $\delta_{pq}=1$ is Kronecker symbol. $\delta_{pq}=1$ if and only if $p=q$; $\delta_{pq}=0$ if and only if $p \neq q$. The choice of

parameters l, σ_{f}, σ_{n} have direct impact on the predicted effect, they are called hyper-parameters.

(1) Training

$D=\{(x_i,y_i),i=1,...,n\}$ is a training set of Gaussian model. x_i is d-dimension input vector, the observation target $x_i \in R$. If X represents the $d\times n$-dimension input matrix, y represents the output vector, the training set can be express as $D=\{X,y\}$. Considering the practical problems have noise, Gaussian process regression model can be established as follows:

$$y=f(\mathrm{x})+\varepsilon \tag{4}$$

$$\varepsilon \sim N(0,\sigma_n^2) \tag{5}$$

Where y is the target observation value, ε obey Gaussian distribution, its mean value is zero and its variance is σ_{n}^2.

The prior distribution for the target observation value y is:

$$y \sim \mathrm{N}(0,\mathrm{K}(\mathrm{X},\mathrm{X})+\sigma_{\mathrm{n}}^2\,\mathrm{I}) \tag{6}$$

For new test input x^*, establish the joint Gaussian prior distribution of the output training samples and test samples output according to the prior knowledge of the y orienting to the formula (6).

$$\begin{bmatrix} y \\ y^* \end{bmatrix} \square\ N\left(0,\ \begin{bmatrix} K(X,X)+\sigma_n^2 I & K(X,x^*) \\ K(X,x^*) & K(x^*,x^*) \end{bmatrix}\right) \tag{7}$$

Where $K(X,X)$ is $n\times n$-order symmetric positive definite covariance matrix, any of its term k^{ij} measures the correlation between x^i and x^j; $K(X,x^*)$ is $n\times 1$-order covariance between test point x^* and all input points of training set; $K(x^*,x^*)$ is its own covariance of the test point x^*.

(2) Prediction

On the condition of giving input x^* and the training set D, the objective value of GP is the y^* corresponding to x^* calculated by the posterior probability formula (8), that is to say:

$$y^* \mid x^*, D \sim N(\mu_{y^*},\sigma_{y^*}^2) \tag{8}$$

Where

$$\mu_{y^*}=\mathrm{K}(x^*,\mathrm{X})\left[K(\mathrm{X},\mathrm{X})+\sigma_{\mathrm{n}}^2 I\right]^{-1}\mathrm{y} \tag{9}$$

Formula (8) is the key prediction equation of GP.

3.2. Hyper-Parameters Optimization of Gaussian Process based on IDE

Hyper-parameter of GP has a great influence on the results of risk assessment. The conjugate gradient method which is usually used for traditional GP algorithm has strong dependence on initial values and is easy to fall into local optimal solution. Thus it is hard to establish the optimal prediction model which has the best overall performance. The paper uses the IDE algorithm for the traditional GP Hyper-parameter optimization to overcome the above disadvantages.

Differential Evolution (DE) [15] is an optimization algorithm based on swarm intelligence theory. It adopts the mutation operation of the differential method and the individual competition survival strategy, and keeps the global search strategy based on the swarm, thus it is simpler than Genetic Algorithm, easy to realize, and has a strong global convergence and robustness. But DE algorithm still needs larger population sizes to avoid premature convergence. To solve this problem, the paper adds the local search(Bees

accelerated evolution operation) and global search(Bees scout operation) thought of ABC algorithm into the DE algorithm to reduce the population size required by the algorithm and improve performance of the algorithm. Finally, use the optimal Hyper-parameter to construct evaluation GP assessment model (IDE-GP).

IDE-GP algorithm concrete process is as follows:

(1) Initialization of population

(2) Basic DE algorithm operation

Execute the DE operation for each individual in the population by Mutation, Crossover, Selection to produce the new generation of individuals. And the concrete operation process is as follows:

a. Mutation, randomly generate three different integers $r_1, r_2, r_3 \in \{1,...,NP\}$ for each individual $x_i(t)$ and require three random integers not equal to i at the same time, then generate mutation individual $v_i(t)$ according to the formula (10).

$$\begin{cases} v_i(t) = \left(v_i^1(t),...,v_i^D(t)\right) \\ v_i^j(t) = x_{r_1}^j(t) + F \times \left(x_{r_2}^j(t) - x_{r_3}^j(t)\right) \end{cases} \tag{10}$$

where $j = 1,...,D$, $v_i^j(t)$ is the j-th variable of the i-th mutation individual in the first generation population; F is the scaling factor, $F \in (0,2)$.

b. Crossover

Firstly, randomly generate a integer $j\_rand \in \{1,...,D\}$, then generate the test individual $u_i(t)$ through $x_i(t)$, $v_i(t)$ according to the formula (11).

$$u_i^j(t) = \begin{cases} v_i^j(t), \text{if } \text{rand}(0,1) \le CR \text{ or } j = j\_rand \\ x_i^j(t), \text{others} \end{cases} \tag{11}$$

In the formula, CR is the crossover factor, $CR \in (0,1)$

c. Select the operation, by comparing the fitness-degree between test individual and original individual, we select individual with better fitness-degree as a new generation of individuals.

$$x_i(t+1) = \begin{cases} x_i(t), \text{if } fit(x_i(t)) < fit(u_i(t)) \\ u_i(t), \text{others} \end{cases} \tag{12}$$

where $j = 1,...,D$

(3) Calculation of fitness

Calculate the ratio of fitness distribution for all individuals in the population:

$$P_i = \frac{fit_i^*}{\sum_{n=1}^{NP} fit_n^*} \tag{13}$$

Where $fit_i^* = \left| fit_i - \max\{fit_1,..., fit_{NP}\} \right|$

(4) Calculation of the accelerated evolution numbers for each individual

According to the proportion of fitness distribution and the individual numbers of a population, the accelerated evolution numbers of individual can be calculated by $N_i = NP \times P_i$, where P_i is the fitness distribution proportion of the i-th individual in the population.

(5) Accelerated evolution operation of artificial bee colony

Adopting to the thought of ABC algorithm, the algorithm provides more local search opportunities for individuals with better evolution performance, to produce a new generation of individuals by cycle N_i of basic differential evolution operations for each individual.

(6) Determination the abandoned individual

Define the maximum number of evolution $\lim it = NP \times D$, where NP is the size of the population, D represents the individual dimension, if the performance of an individual still did not improve after the times of $\lim it$ evolution experiment, then this individual is defined as abandoned individual. If there are abandoned individuals, jump to step (7), otherwise jump to the step (8).

(7) Artificial bee colony Operations scout operation

Regenerate of the random individuals which meet the constraints, replacing the abandoned individual by random individual meanwhile referring to step (1), and then reset the number of evolution experiment at the same time.

(8) Judgement to the result whether satisfy termination condition

Determine whether the result satisfies termination condition, if the condition is satisfied, jump to step (9), otherwise, returns to step (2). The optimal termination condition can take the value that evolutionary process reaches a certain level, or after several successive generation evolutions, the objective function is not improved.

(9) Construction of optimal assessment model

The hyper-parameter is the optimal solution of the optimal process based on improved differential evolution algorithm. We use the optimal hyper-parameter, as well as input training samples, to construct the optimal GP assessment model.

(10) Assessment

Use optimal GP model to assess the result, and then input the test sample to GP model, finally, output the prediction accuracy.

IDE-GP algorithm flow chart is shown in Figure 1.

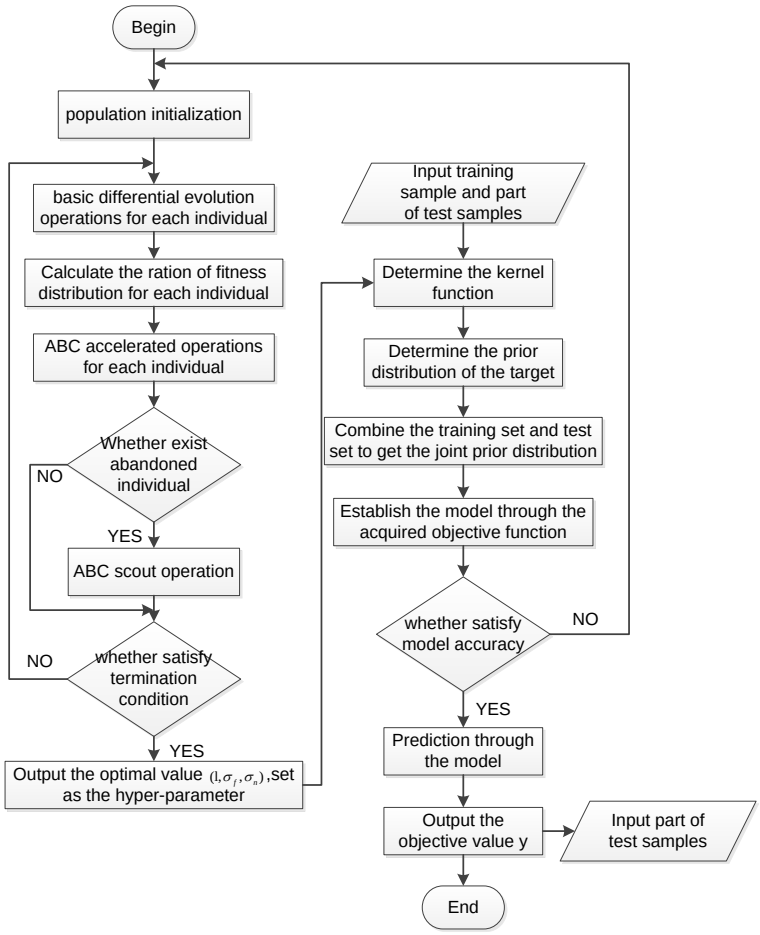

Figure 1. Gaussian Process Flowchart based on the Hybrid Optimization Algorithm

3.3. Power System Security Risk Assessment based on Improved Gaussian Process Model

Evaluating security risk of power system using previously established assessment model, the flow chart is shown in Figure 2.

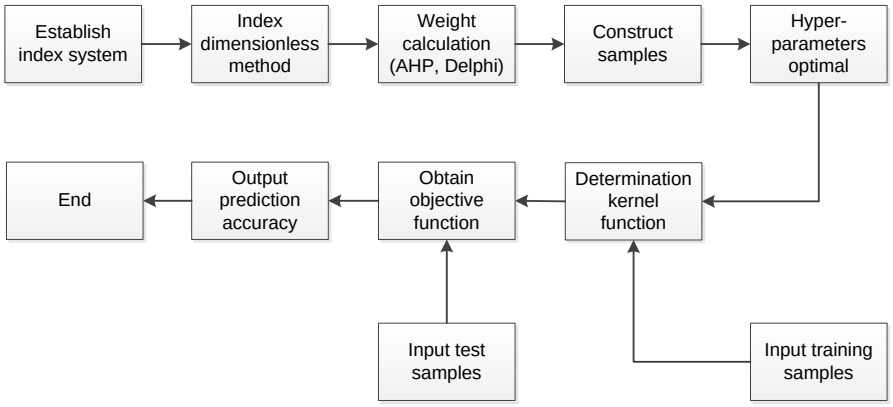

Figure 2. Power System Security Risk Assessment Flowchart based on the Improved Gaussian Process

The detailed steps of security risk assessment process are as follows:

(1) Based on the risk index system that have been established, using AHP and Delphi method to calculate the relative weight of these indices, then calculate composite index of system risk using the weighted sum method;
(2) Normalization the value of indices to prevent the large changes in the value which have a negative effect of the Gaussian learning process;
(3) Construct a learning sample of Gaussian process, and divide it into training-set and test-set;
(4) Input the training set to the Gaussian regression process for learning, using IDE algorithm to optimize the hyper-parameters, then establish power system security risk assessment model;
(5) Analyze the assessment-accuracy and error.

4. Experiment Results and Analysis

4.1. Experiment Analysis

A large number of simulative experiments have been made, using Matlab for verifying the validity that is based on the hybrid optimization GP method. The experimental data originated from the standard dataset of IEEE-39 and IEEE-118 bus systems. The experimental environment is: the platform of Inter Core Due CPU 2.10GHz and 2.00G RAM in Matlab 2010a.

4.2. Assessment Index

Two kinds of standard error are MAPE (Mean Absolute Percent Error) and MSE (Mean Squared Error), being used as model assessment index in these experiments. If the value of the MAPE and MSE is smaller, the model accuracy is higher and the attaining accuracy of risk assessment value is higher. The definition of MAPE and MSE is as follows:

$$MAPE = \frac{1}{N}\sum_{i=1}^{N}\left|\frac{y_i^{'} - y_i}{y_i^{'}}\right| \tag{14}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\left(y_i^{'} - y_i\right)^2 \quad (15)$$

N denotes the sample number, $y_i^{'}$ denotes the assessed value, y_i denotes the actual objective value.

4.3. Assessment Result Analysis

In the experimental progress of the Matlab, the public parameter settings of IDE algorithms and other frequently-used optimizing algorithms like ABC, DE, MA, GA are shown as the Table 4.

Table 4. Public Parameters Table

Parameter name	value	Description
NP	30	Population size
D	16	Numbers of Optimizing algorithms
Iterations	1000	Maximum iterations
Runtime	20	Repeated experiments' times
Upper Bounds	$10_{1\text{-}52}\&1_{53}$	The upper limit of individual values
Lower Bounds	0.0000001	The lower limit of individual values
Objective function	Improved Gaussian function	Optimizing algorithms' objective function

In addition to the above public parameters, each algorithm has its other unique parameter settings, being shown in table 5. ABC algorithm has only one control parameter, and the DE algorithm has two, but the IDE algorithm, which is combined with ABC and DE algorithm, has three control parameters. What's more, the MA being developed on the basis of GA, its parameters are almost the same as the GA. The different part is the MA increases local search strategy on the basis of the GA. The control parameters of the MA are six, but the control parameters of GA is five.

Table 5. Unique Parameters Table

Parameter name	MA	GA	DE	ABC	IDE
Selection strategy	Roulette selection	roulette	--	--	--
Crossover strategy	Single-point cross	Single-point cross	--	--	--
Crossover probability	0.8	0.8	--	--	--
Mutation strategy	Random variation	random variation	--	--	--
Mutation probability	0.01	0.01	--	--	--
Local search times	15	--	--	--	--

Limit=NP*D	--	--	--	480	480
Cross factor	--	--	0.5	--	0.5
Differential mutation factor	--	--	0.6	--	0.6

3.3.1. IEEE-39 Nodal Examples: After 1000 iterative times, the IDE-GP experiment got 16 parameters *i.e.* optimal super Gaussian process parameters, and the results are shown in Table 6.

Table 6. Values of the Hyper-Parameter Optimization (IEEE-39)

1	2	3	4	5	6	7	8
3.4581	10.0000	0.2558	10.0000	1.2799	9.9987	0.6852	0.2296
9	10	11	12	13	14	σ_f	σ_n
0.5662	3.9535	10.0000	5.0000	1.0000	5.0000	8.0000	1.0000

In the experiment, using standard data sets of the IEEE-118 and the IEEE-39 bus example respectively constructed 200 samples, including 180 randomly being selected as the training data, and the remaining 20 as test data. Construct the IDE-GP model using the optimal hyper-parameters obtained by IDE algorithm, while inputting 20 tested sample points to get the corresponding assessment value. The tested sample number and the corresponding assessment value are shown in table 7 and in Figure 3.

Table 7. Values of Assessment Results (IEEE-39)

15	163	141	76	97	75	187	115	43	89
0.3402	0.1495	0.3574	0.4896	0.6466	0.5857	0.5158	0.1140	0.2586	0.2386
108	107	7	192	191	51	159	82	93	3
0.1479	0.3503	0.4555	0.5898	0.4188	0.3651	0.5718	0.1363	0.1154	0.4694

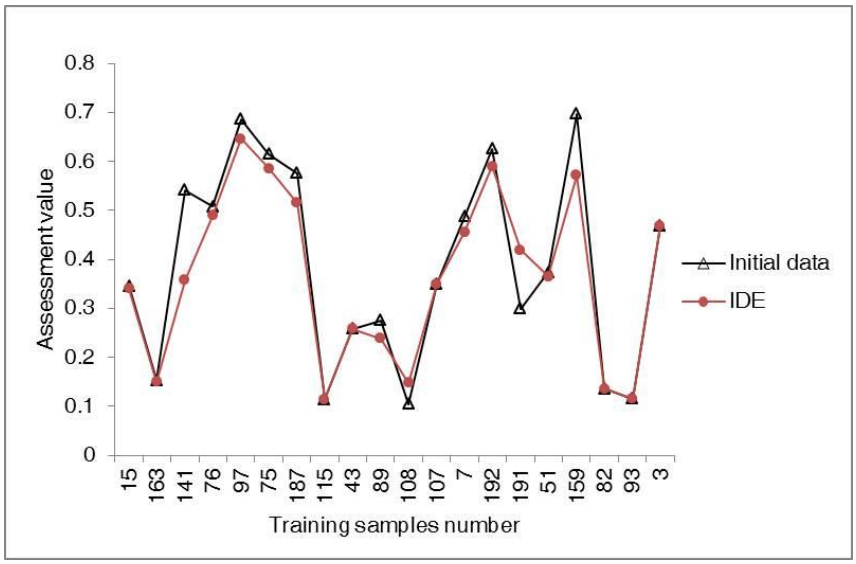

Figure 3. Comparison of the Evaluation Results of IDE - GP Model (IEEE-39)

According to assessment results and based on the range of assessment values, using risk assessment level table to get the corresponding system security risk level, and the risk assessment scale are shown in Table 8.

Table 8. Risk Assessment Rank Table

Assessment value	Security levels
0-0.2	low
0.2-0.4	medium low
0.4-0.6	medium
0.6-0.8	medium on the high side
0.8-1.0	high

The paper compares the IDE-GP method with ABC-GP, DE-GP, GA-GP, MA-GP algorithms from the points of assessment accuracy and time complexity to analyze the validity of the proposed method.

This experiment selected the best of 20 times experiments having been made as the result, and compared the average results of assessment accuracy, and the results were shown in Figure 4 and 5.

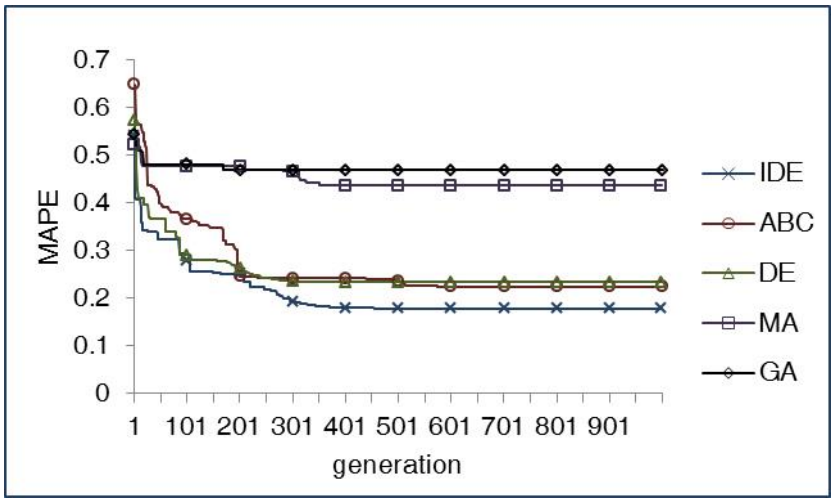

Figure 4. Comparison of the Assessment Accuracy MAPE of Company's Optimization Model (IEEE-39)

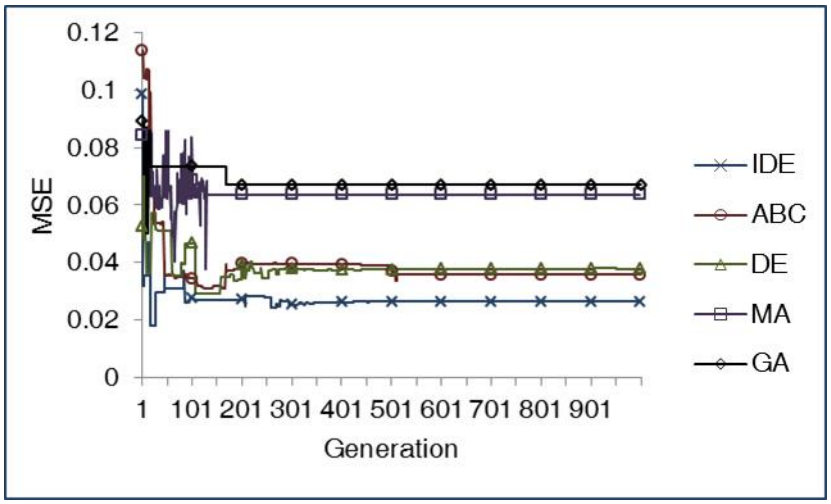

Figure 5. Comparison of the Assessment Accuracy MSE of Company's Optimization Model (IEEE-39)

According to Figure 4, 5, with the increasing number of iterations, all the model errors (MAPE, MSE) gradually decreases, but there will be no change and tend to a stable value.

Although GA algorithm has the fastest convergence time, the accuracy value is not high enough. Compared with other models, the MAPE value of IDE-GP model is minimum, *i.e*. 0.177638; at the same time MSE is minimum to 0.026273 and lower than the other four single models respectively, which verified the proposed hybrid optimization Gaussian process model is superior to other methods in evaluating the precision under the IEEE-39 standard data.

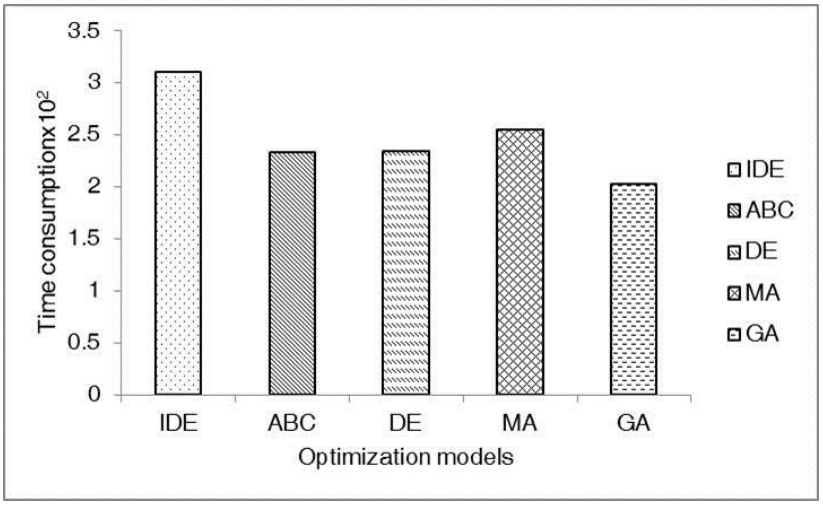

Figure 6. Comparison of the Time Consumption of Company's Optimized Model (IEEE-39)

For 20 times experiment, 1000 times iteration, different optimization models for the average time consumption contrast Figure are given, which can be seen from the Figure 6: the used time of the IDE-GP slightly more than ABC-GP, DE-GP, GA-GP, MA-GP, which is because the IDE-GP algorithm combines with ABC and DE algorithm and increases the ABC algorithm's onlook bee and scout bee algorithm for local search and global search respectively, based on the evolution of the DE algorithm, and the time consumption is slightly long. MA algorithm is improved on the GA algorithm increasing the local search, and its time is slightly longer than the GA algorithm's.

Under the situation that comprehensive comparison of IDE-GP algorithm in time consumption is similar with other algorithms and accuracy is higher than that of other algorithms, it suggests that the comprehensive effect of the IDE-GP is relatively good.

3.3.2. IEEE - 118 Bus Examples: To further verify the validity of the algorithm, and equal to the IEEE-39 bus examples, the paper also makes a series of simulative experiments about the IEEE-118 bus examples. The tested results are shown in table 9, 10 and Figure 7, 8, 9, 10, and the experiment obtains the similar results to the IEEE-39 bus examples.

Table 9. Value of the Hyper - Parameter Optimization (IEEE-118)

1	2	3	4	5	6	7	8
7.1222	9.9962	1.0623	0.1807	9.9994	9.9886	1.2401	10.0000
9	10	11	12	13	14	σ_f	σ_n
1.7181	1.2314	10.0000	1.0000	1.0000	10.0000	6.0000	1.0000

Table 10. Values of Assessment Results (IEEE-118)

15	163	141	76	97	75	187	115	43	89
0.4668	0.8775	0.6139	0.4977	0.5560	0.4182	0.7799	0.6245	0.9227	0.7602
108	107	7	192	191	51	159	82	93	3
0.4239	0.0844	0.4924	0.5972	0.6980	0.6247	0.6201	0.2246	0.5919	0.2752

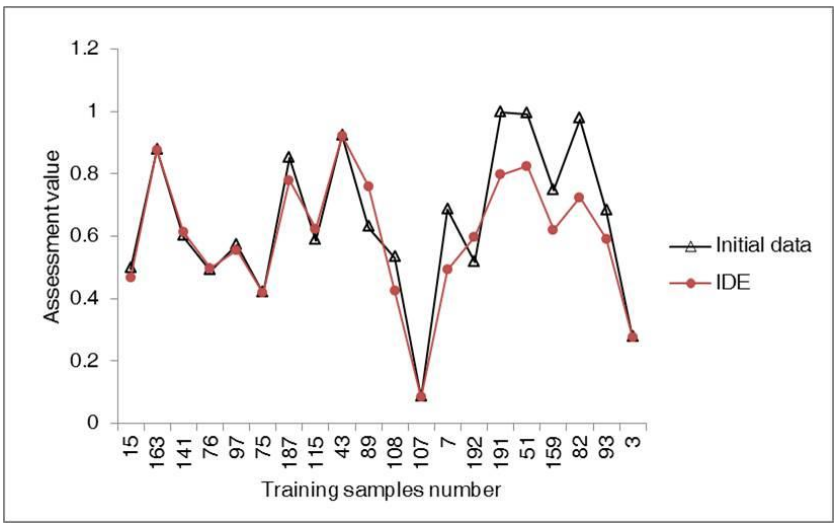

Figure 7. Comparison of the Evaluation Results of IDE - GP Model (IEEE-118)

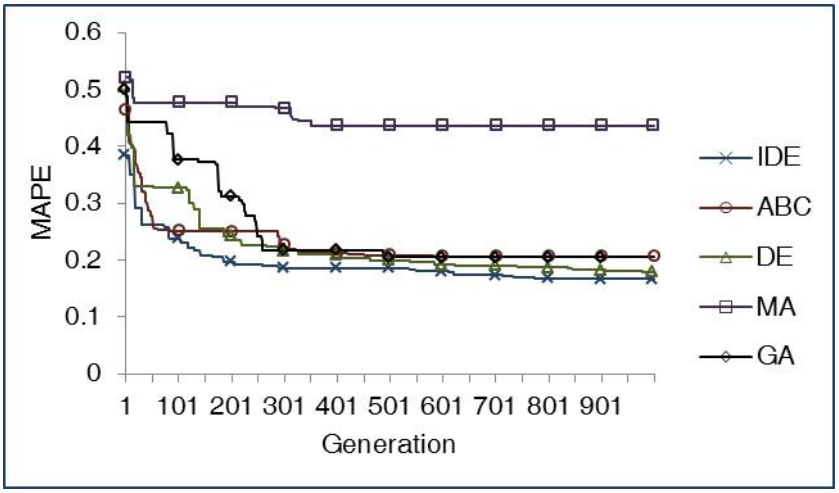

Figure 8. Comparison of the Assessment Accuracy MAPE of Company's Optimization Model (IEEE-118)

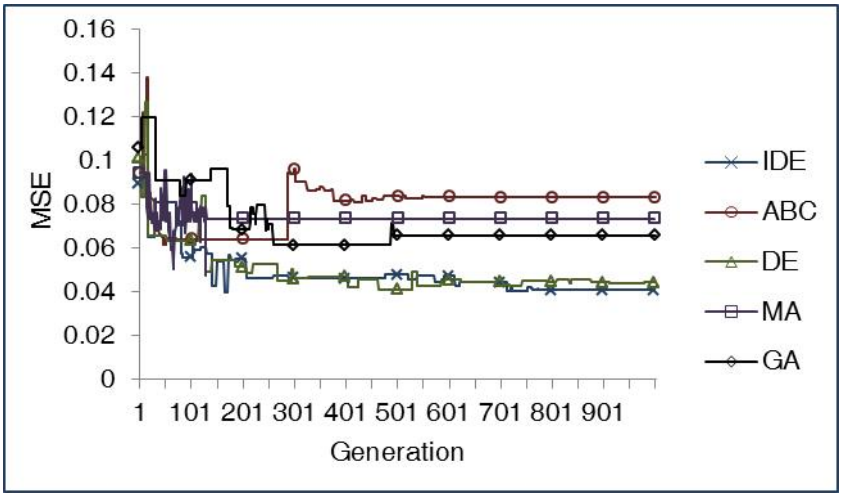

Figure 9. Comparison of the Assessment Accuracy MSE of Company's Optimization Model (IEEE-118)

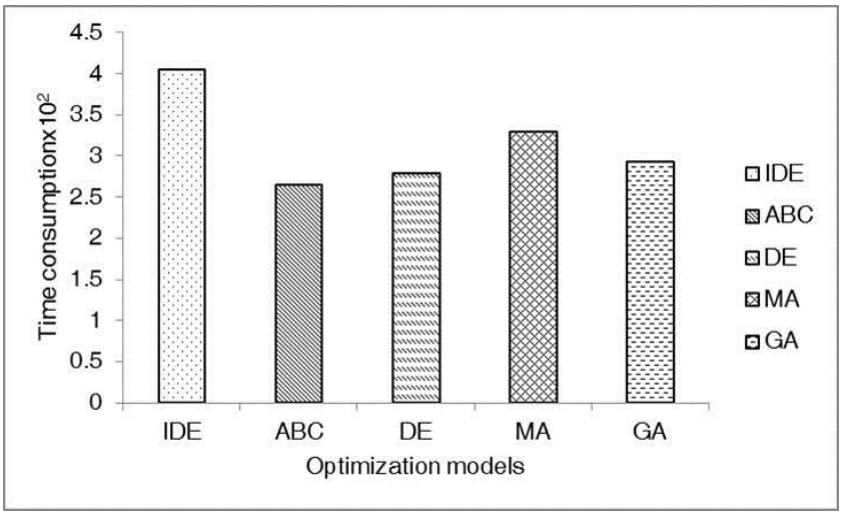

Figure 10. Comparison of the Time Consumption of Company's Optimization Model (IEEE-118)

From the above experiment results, the experimental results of the IEEE-118 bus examples are similar to the IEEE39 bus examples'. Under the same number of iterations, the time consumption of the IDE-GP and other algorithms are similar, but the precision is higher than other algorithms. The comprehensive results of IEEE-39 and IEEE-118 bus calculation are similar, which shows that the comprehensive effect of the IDE-GP is relatively good.

5. Conclusions

On the basis of the establishment of the assessment index system using Fault Tree Analysis (FTA), the paper proposed a method for risk assessment of power system security based on a hybrid optimization GP method as to the power system security risk assessment. The paper uses the Improved Differential Evolution (IDE) algorithm optimize the traditional Hyper-parameter, and then uses the optimal Hyper-parameter construct Gauss process regression model for power system security risk assessment to establish the optimal assessment model in overall performance. In order to verify the validity of the algorithm, this paper uses the standard data of the IEEE-39 and IEEE-118 bus examples

to make simulative experiment. And then the paper compares the IDE-GP with other optimized models of ABC-GP, DE-GP, MA-GP, GA-GP from two aspects of evaluation accuracy and time complexity. The results show that the hybrid algorithm compared with other algorithms in time consumption is small, and its precision is higher than other algorithms, and also proves the effectiveness of the algorithm, which shows that the algorithm is applicable to solve the problem of grid security risk assessment.

References

[1] P. Kundur, J. Paserba, V. Ajjarapu and G. Andersson, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions", IEEE Transactions on Power Systems, vol. 19, no. 3, (2004), pp. 1387-1401.
[2] Z. Yang, L. Huaqiang, W. Yimiao and L. Peiqing, "A complex network theory and conditional probability based risk assessment method for disastrous accidents", Power System Technology, vol. 37, no. 11, (2013), pp. 3190-3196.
[3] Z. Guohua, Z. Jianhua, Y. ZhiDong, P. Qian and Y. Jingyan, "Risk Assessment Method of Power System N-K Contingencies", Power System Technology, vol. 33, no. 5, (2009), pp. 17-21.
[4] Z. Guo, L. Huaqiang, H. Yan, and H Qiang. "A risk assessment method based on importance of component and operational state under catastrophic accident", Power System Technology (POWERCON), 2014 International Conference on. Chen Du, China: IEEE, (2014), pp. 1217-1223.
[5] W. Zhengqiu and W. Liangyuan, "Sensitivity analysis of transient stable margin with complicated load modeling", Power System Technology, vol. 27, no. 3, (2003), pp. 53-58.
[6] S. Wenhui, B. Zhaohong and W. Xifan, "Applications of markov chain monte carlo in large-scale system reliability evaluation", Proceedings-Chinese Society of Electrical Engineering, vol. 28, no. 4, (2008), pp. 9-15.
[7] L. Wenyi, Z. Baohui and B. Gen, "Reliability impacts of large scale utilization of wind energy on electric power systems", Proceedings-Chinese Society Of Electrical Engineering, vol. 28, no. 1, (2008), pp. 100-105.
[8] S. Yi and W. Chenshan, "A probabilistic risk assessment method for cascading failure of power system", Proceedings of the CSEE, vol. 29, no. 4, (2009), pp. 27-33.
[9] L. Xindong, J. Quanyuan, C. Yijia and C. Weihua, "Transient security risk assessment of power system based on risk theory and fuzzy reasoning", Electric Power Automation Equipment, vol. 29, no. 2, (2009), pp. 15-20.
[10] Z. Guohua, D. Manyin, Z. Jianhua, C. Degang and Y. Jingyan, "Power system risk assessment based on the evidence theory and utility theory", Automation of Electric Power Systems, vol. 33, no. 23, (2009), pp. 1-4.
[11] W. Bo, Y. Dahai, Y. Xianggen and C. Qingqian, "A security risk assessment system of complicated power grid based on multiple factor analysis", Power System Technology, vol. 35, no. 1, (2011), pp. 40-45.
[12] A. Volkanovski, M. Čepin and B. Mavko, "Application of the fault tree analysis for assessment of power system reliability", Reliability Engineering & System Safety, vol.94, no. 6, (2009), pp. 1116-1127.
[13] X. Chuansheng, D. Dapeng, H. Shengping, X. Xin and C. Yingjie, "Safety Evaluation of Smart Grid based on AHP-Entropy Method", Systems Engineering Procedia, vol.4, (2012), pp. 203-209.
[14] M. A. Alvarez , D. Luengo and N. D. Lawrence, "Linear latent force models using gaussian process", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 11, (2013), pp. 2693-2705.
[15] A. P. Piotrowski, "Differential Evolution algorithms applied to Neural Network training suffer from stagnation", Applied Soft Computing, vol. 21, (2014), pp. 382-406.
[16] . Akay and D. Karaboga, "A modified artificial bee colony algorithm for real-parameter optimization", Information Sciences, vol. 192, (2012), pp. 120-142.

Authors

Xiaobin Wu (1985-), Master's degree, and now he is the Engineer of State Grid Shandong Electric Power Company Linyi Electric Power Company. His current research interests include Security risk prevention and control system for Power Grid S mart Grid operation and control, power electronic.

Hui Li (1970-), bachelor's degree, Engineer. Her current research interest is Power System operation mode management.

Xiaolu Chen (1989-), Master's degree, Engineer. His current research interest is the research on Electric Power System and Automation.

