International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 2, April 2016, pp. 870~876
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i2.9572

New Classifier Design for Static Security Evaluation using Artificial Intelligence Techniques

Ibrahim Saeh, M.W. Mustafa, Nasir A. Al-geelani
Faculty of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Malaysia

Article Info

Article history:

Received Aug 12, 2015
Revised Nov 25, 2015
Accepted Dec 16, 2015

Keyword:

Artificial Intelligence
Classification
Classifier design
Feature Selection
Static Security Evaluation

ABSTRACT

This paper proposes evaluation and classification classifier for static security evaluation (SSE) and classifica-tion. Data are generated on (30, 57, 118 and 300) bus IEEE test systems used to design the classifiers. The implementation decision tree methods on several IEEE test systems involved appropriateness SSE and classi-fication by using four algorithms of DT's. Empirically, with the present of FSA, the implementation results indicate that these classifiers have the capability for system security evaluation and classification. Lastly, FSA is efficient and effective approach for real-time evaluation and classification classifier design.

Corresponding Author:

Ibrahim Saeh,
Department of Electrical and Electronic Engineering,
Faculty of Electrical Engineering, Universiti Teknologi Malaysia,
Johor Bahru 81310, Johor, Malaysia.
Email: ibrahimsaeh@yahoo.com

1. INTRODUCTION

The electric market competition forces generating entities and system operators to operate the system within their security level. Load and operating constrains are two sets of power system operation con-strains [1]. The load constraint is an equation constraint which sets the total generation equal to total load plus total power losses. The operating constraints are upper and/or lower limits of system's variables. Long term planning or even in operational, making security decisions and a conceptual basis provide by system operating states.

Under contingent condition, security can be defined as the ability of the power system to remain in a se-cure state [2]. Security assessment involves estimation of the relative security level of the current operat-ing condition of the system using available data measurements. The task of security assessment is per-formed in three modes - static, transient and dynamic [3]. More specifically the static security is the steady state system behaviour under a specified contingency, whereas the transient security is dealing with evaluating rotor angle oscillations under a transient disturbance. Dynamic security deals with the long term behaviour from the instant of the system transiently secure to the instant of the system will reaches steady state.

All the three modes need to be sequentially performed on-line. In case of insecurity in any mode of as-sessment, an alarm is signalled for the operator to take an appropriate remedial action. Through simula-tion, Static Security Evaluation (SSE) assists operators to detect following a given list of contingencies such as a voltage out-of-limit or potential a system branch overloaded. Due to the large system size and deregulated power system, a steady-state security analysis becomes an impossible task due to the associated computation burden.

In SSE, the contingencies severity is judged on scale performance index (PI) basis. In [1-3], numerous PI based methods have been reported. Artificial intelligence (AI) can be divided into two types of

tech-niques, clustering techniques and classification techniques, and its powerful of reducing the data complexity, made it to use in various areas like medical and engineering [4, 5].

1.1. Static Security Evaluation Indices Selection

Power system networks are required to operate with security limits. Security is defined as promising the continuous operation of a power system capability under normal operation even next some important contingency [6].

In the literature, several keys have been suggested as standards for static security classification and eval-uation [2, 7-10] include lines overloaded or \ and bus voltages collapse which let the system deviate from normal operating state limits. However, violations are not in the same level of the same significance.

In the assessment process of static security, it is evaluated for several feasible contingencies via solving power flow nonlinear equations. These contingencies possibly will contain outage of a generating unit or N-1 transmission line or a transformer.

For numerous disturbances, the load flow is simulated and the security limitations are gauged. The oper-ating state of power system is categorized as static secure (SS-Binary 1) if two the limitations in equations (1), and (2) are fulfilled. In case of one limitation is identified subsequent a contingency, the state of the system is categorized as static insecure (SI-Binary 0).

Therefore, it is compulsory to develop an efficient methods to deal about the complexity of data [10]. The traditional element accounts for coaching the device understanding methods for classification of static security evaluation contents.

2. ARTIFICIAL INTELLIGENCE TECHNIQUES

Generally, most of the artificial intelligence techniques approaches assess information through the data-base. Nowadays, database becomes larger in size, and as result, it is very difficult to interpret complex data. Therefore, it is compulsory to develop efficient methods to deal about the complexity of data [10]. Multi-layer feed forward artificial neural network (MLFFN) and radial basis function network (RBFN) are proposed to implement the online module for power system static security assessment [11]. The security classification, contingency selection and ranking are done based on the composite security index which is capable of accurately differentiating the secure and non-secure cases. For each contingency case as well as for base case condition, the composite security index is computed using the full Newton Raphson load flow analysis. The proposed artificial neural network (ANN) models take loading condition and the probable contingencies as the input and assess the system security by screening the credible contingencies and ranking them in the order of severity based on composite security index.

The traditional element accounts for coaching the device understanding methods for classification of static security evaluation contents. Figure 1 presents the methodology for static security evaluation content classification approach based upon the artificial intelligence techniques.

The methodology is attained through four phases: data set collection, data set preprocessing, training phase, and classifier evaluation with testing data. Consequently, the static security evaluation can be managed based on the trained machine learning classifier.

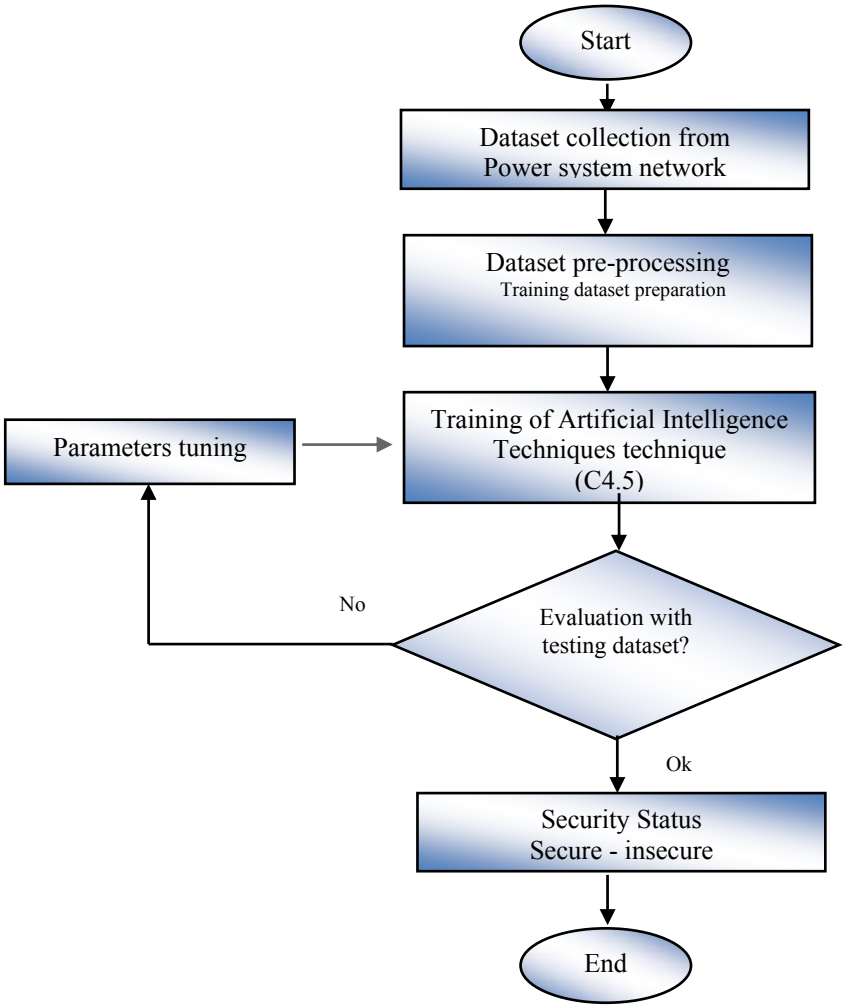

Figure 1. Artificial Intelligence Techniques procedure for static security evaluation and classification

2.1. Raw Dataset Collection

NRLF analysis is used before implementation of decision tree to solve algebraic equation which is non-linear to the system used, and collected data of all line flow and voltages of all buses. These data collected will use as input vector for training and testing the algorithms. Thus, test dataset; which is dissimilar cases from the training dataset should keep getting an acceptable accuracy results. NRLF were developed via matpower 3.0b4 program [12] and used through this study as a matrix form. In this program, the results can be shown by using the command runpf ('case Z'), where Z is the buses number. The list of attributes (features) used for the pattern vector for static security evaluation is as follows below.

$$X_{SSE} = \{| V|i , \theta i , SGi , SLi , Sij \} \quad (1)$$

The contingencies can include interruption on a transformer or the transmission line or maybe a genera-tor. Performing load flow will check all the bus voltages and line thermal power limits; (1) voltage at all buses must be within their range (0.94-1.06) p.u. [13, 14], and (2) all lines are not exceeding their power range as well (S< Smax.).

2.2. Training Dataset Preparation

To be able to put together working out information arranged, the specified options that come with the actual system tend to be obtained from the actual ready track documents. The key functions of the power system network are extracted in order to prepare the training data set. These functions tend to be transformed into the actual input/output dataset or even coaching designs needed in the coaching stage.

When the instruction dataset is ready while described previously, the actual dataset will be stabilized ap-propriately in variety [0, 1] by applying equation (2).

$$\overline{v} = \frac{v - \min_V}{\max_V - \min_V} \quad (2)$$

where v is the attribute V original value, $\overline{v}$ is the attribute V normalized value, and $\min_V$ and $\max_V$ are the minimum and maximum attribute V values.

2.3. C4.5 Classifier Training

C4.5 decision tree is one of the most broadly used and real-world approaches. In C4.5, the learned classifier is represented by a DT as sets of if-then rules to human readability improvement. Therefore, the decision tree is simple to be understood and interpreted. Besides, it can handle nominal and categorical data and perform well with large data set in a short time [15]. In C4.5 training, the decision tree is built in a top - down recursive way. Learning works of C4.5 as follows:

Primarily, all training patterns fixed at root. These patterns are divided based on features selected based on an impurity function in recursive routine. Dividing continues till all training patterns for a certain node belong to the similar class. The parameters and their settings values were used in WEKA as shown in Table 1.

Table 1. Parameters settings for C4.5 training

Parameter	Description	Value
ConfidenceFactor	The confidence factor used for pruning (smaller values incur more pruning).	0.25
minNumObj	The minimum number of instances per leaf.	2
Unpruned	Whether pruning is performed or not	False

2.4. Performance Evaluation

The correct classification rate (CCR) can be defined as one a key gauge employed for analyzing one particular or even classifier. Nevertheless, CCR only can be inadequate regarding gauging a functionality of the classifier for a static security index data set. And so, the true negative rate (TNR) and true positive rate (TPR) were used to evaluate the classifier performance. Moreover, geometric mean (GM) was addi-tionally utilized in this research to assess the actual overall performance regarding device studying tech-niques, as shown in Table 2.

Table 2. The procedures employed for assessing the efficiency of machine learning techniques

Measures name	Formula
Correct classification rate (CCR)	$CCR = \frac{TP + TN}{TP + FP + FN + TN}$ **(%)**
True positive rate (TPR)	$TPR = \frac{TP}{TP + FN}$ **(%)**
True negative rate (TNR)	$TNR = \frac{TN}{TN + FP}$ **(%)**
Geometric mean (GM)	$GM = \sqrt{TPR * TNR}$ **(%)**

where:

TP (true positive): the number positive samples classified correctly, FP (false positive): the number nega-tive samples classified incorrectly, TN (true negative): the number negative samples classified correctly and FN (false negative): the number positive samples classified incorrectly

After we initialize a pattern vector (X_{SSE}) from data collection and data pre-processing, we initialize fea-ture vector (Z_{SSE}) from cross validation and number of instances. Data samples generated are randomly split in training and testing process in approximately proportion of 75% and 25% respectively. A training pattern (Z_{SSE} vector) takes the format <x1 , x2 , x3 , x4 ,……, xn>

where x1 , x2 , x3 , x4 ,……, xn denote the input vector and denotes the security status output vector (target). This training pattern called instances (row) while the inputs are featured or attrib-utes (column). The power system condition is, in fact, known as ‘Static Secure’ (SS-Binary one) when-ever all the limitations mentioned in 3.1 are often satisfied for almost any provided backup. When somebody issues break 'is identified performing a problem, the device situation is going to be known as ‘Static Insecure’ (SI-Binary zero).

Engineering common sense occasionally may decide on the actual enter attributes. However, this kind of choices is going to be very subjective using the chance of essential factors obtaining turned down. A typ-ical approach to feature selection will be a consecutive feature choice, composed of two elements - a target function known as criterion and also a consecutive investigation formula. The real feature factors chosen through SFS technique can serve as an input data source regarding creating the actual classifier formula. The SFS technique utilized in the current function begins with an empty group of features and also encourages prospective client function subsets with the help of one attribute every time. For each prospective client perform component, SFS operates the actual 10-fold combine authorization through frequently contacting the actual qualifying criterion operate.

3. RESULTS AND DISCUSSION

Within this research, C4.5 models were properly trained by using a WEKA tool. WEKA is truly a work-bench designed to help the use of machine learning approaches to various actual difficulties. WEKA is truthfully a totally released and also free code developed in Java. In WEKA, the machine learning algorithms tend to be realists organized into programs, to allow them to become efficiently brought in and besides applied in Java's code. Right after the training, the properly trained designs had been stored just as the documents being applied in enhancing the static security stage during the test stage. About applying WEKA classifiers in Java's code, WEKA guide are available in [16].

In the steady-state, the SSE limitations are the bus voltage magnitude (V_k) and the line thermal power (S) and can be written as: $1.09 > V_k > 0.91$ and $S < S_{max}$.

The outcomes of information building and show choice stages of static security evaluation are shown in Table 3. The data samples in m-dimensional feature space are randomly split into training and test sets.

Table 3. Data generation and feature selection of different IEEE test systems

System size	Operating scenarios	Static Secure (SS)	Static Insecure (SI)	No. of pattern variables (X_{SSE})	No. of features selected (Z_{SSE})	Dimensionality reduction
30 Bus	860	595	265	170	25	**14.70%**
57 Bus	950	630	320	185	27	**14.59%**
118 Bus	1100	750	350	210	29	**13%**
300 Bus	1330	760	570	220	26	11.81%

From this table, 30, 57, 118 and 300 IEEE bus systems are used in this paper, the operation scenarios are 860, 950, 1100 and 1330 respectively. All these scenarios are classified either static secure (SS) or static insecure (SI). The impact of the feature selection approach used in this research work is mentioned in the table as dimensionality reduction which is designating by bold values.

In order to evaluate the performance of a static security evaluation approach, it is very important to measure its performance. Therefore, some common performance measures are used to evaluate the performance of a particular security status index compared with other approaches.

Four different algorithms of DT's with same train datasets and test datasets are used in a comparison. This comparison was in terms of CCR, TNR, TPR, GM and computation time and presented in table 4. For extra knowledge regarding the artificial intelligence techniques algorithms used in this study is presented in [17].

Table 4 shows the comparison between the performance's measures of proposed C4.5 and other four various DT's techniques for the two network data sets (57 and 118 IEEE test systems) in both training and testing data sets. In Table 4, the best and the worst values of the measures are highlighted in bold font and underline font, respectively. In training phase (57 bus system), BF Tree, Stump Tree, J 48 Tree and J 48 graft attained around 94.70%, 95.4%, 93.70%, 94.60% of CCR respectively, while C4.5 Tree attained of CCR around 98.64%. In testing phase, BF Tree, Stump Tree, J 48 Tree and J 48 graft attained around 93.50%, 91.2%, 92.50%, 93.40% of CCR respectively, while C4.5 Tree attained around 97.44% of CCR.

In training phase (118 bus system), BF Tree, Stump Tree, J 48 Tree and J 48 graft attained around 94.50%, 95.2%, 93.50%, 94.20% of CCR respectively, while C4.5 Tree attained around 98.44% of CCR. In testing phase, BF Tree, Stump Tree, J 48 Tree and J 48 graft attained around 93.80%, 91.5%, 92.80%, 93.70% of CCR respectively, while C4.5 Tree attained around 97.74% of CCR.

Table 4. Performance of C4.5 classifier for static security evaluation

		Proposed Classifier	**Decision Tree classifiers (DTC's)**			
		C4.5 Tree	BF Tree	Stump Tree	J 48 Tree	J 48 graft
IEEE 57 bus	Total samples, 950					
Train set	Samples	630				
	CCR (%)	**98.64**	94.70	95.4	93.70	94.60
	TPR (%)	**96.30**	93.90	95.1	93.20	94.00
	TNR (%)	**97.21**	94.30	95.00	93.30	94.20
	GM (%)	**96.75**	94.09	95.049	93.25	94.10
	Time(s)	**0.0001**	0.001	0.02	0.01	0.03
Test set	Samples	320				
	CCR (%)	**97.44**	93.50	91.2	92.50	93.40
	TPR (%)	**95.90**	93.60	95.5	93.70	94.90
	TNR (%)	**97.21**	94.15	95.70	93.30	94.20
	GM (%)	**96.55**	93.87	95.59	93.49	94.55
	Time(s)	**0.0001**	0.003	0.04	0.02	0.05
IEEE 118 bus	Total samples, 1100					
Train set	Samples	750				
	CCR (%)	**98.44**	94.50	95.20	93.50	94.20
	TPR (%)	**96.80**	94.30	95.2	93.70	94.80
	TNR (%)	**97.5**	95.00	94.90	93.10	94.10
	GM (%)	**97.14**	94.65	95.049	93.39	94.45
	Time(s)	**0.0001**	0.001	0.052	0.01	0.05
Test set	Samples	**350**				
	CCR (%)	**97.74**	93.80	91.50	92.80	93.70
	TPR (%)	**97.10**	93.75	94.7	94.10	94.10
	TNR (%)	**96.90**	94.30	94.90	93.20	94.30
	GM (%)	**96.99**	94.02	94.79	93.64	94.19
	Time(s)	**0.001**	0.002	0.055	0.015	0.08

Bold value validates that C4.5 provides great correct classification rate and minimum computation time to other DTC's classifiers.

Finally, for train mode and test mode, table 4 also demonstrates the computation time in seconds. Strongly, it can be observed that for both systems used, C4.5 got minimum computation time (0.0001) second for training and testing phases. Furthermore, for the recall (test) phase where C4.5 got computation time of 0 s. and 0.001 s. for training and testing phase respectively.

4. CONCLUSION

The results and discussions of using C4.5 and other decision tree classifiers for SSE the electric power has presented. Also, the results and discussions of using feature selection for designing classifiers for SSE the electric power grid has presented. The implementation of feature selection involved appropriateness data reduction. The implementation decision tree methods on several IEEE test systems involved appropriateness SSE and classification by using four algorithms of DT's. From this research work, it is observed that all these algorithms promise successful and alternative techniques for large scale power grid SSE. 98.7% of CCR and 0.0001 second of computation time made C4.5 is very well fit in the real-time power systems SSE. Mentioned techniques can effectively be implemented for SSE with high accuracy rate.

ACKNOWLEDGEMENTS

The authors would like to express their appreciation to Universiti Teknologi Malaysia (UTM) for the facilities and support.

REFERENCES

[1] Singh, S. and S. Srivastava, Improved contingency selection algorithm for voltage security analysis. Electric machines and power systems, 1998. 26(8): p. 855-871.

[2] Ejebe, G. and B. Wollenberg, Automatic contingency selection. Power Apparatus and Systems, IEEE Transactions on, 1979(1): p. 97-109.
[3] Verma, K. and K. Niazi, Supervised learning approach to online contingency screening and ranking in power systems. International Journal of Electrical Power & Energy Systems, 2012.
[4] Camara, F., et al., Privacy Preserving RFE-SVM for Distributed Gene Selection. 2012.
[5] Jun, S., A Clustering Method of Highly Dimensional Patent Data Using Bayesian Approach. 2012.
[6] Morison, K., L. Wang, and P. Kundur, Power system security assessment. Power and Energy Magazine, IEEE, 2004. 2(5): p. 30-39.
[7] Albuyeh, F., A. Bose, and B. Heath, Reactive power considerations in automatic contingency selection. Power Apparatus and Systems, IEEE Transactions on, 1982(1): p. 107-112.
[8] Wehenkel, L.A., Automatic learning techniques in power systems. 1998: Kluwer Academic Publishers.
[9] Marsadek, M., et al. Risk based static security assessment in a practical interconnected power system. 2008: IEEE.
[10] Mori, H. State-of-the-art overview on data mining in power systems. 2006: IEEE.
[11] Sunitha R, R. Sreerama Kumarand Abraham T. Mathew" Online Static Security Assessment Module Using Artificial Neural Networks" IEEE Transactions On Power Systems, VOL. 28, NO. 4, November 2013.
[12] 12. Momoh, J.A., Y. Xia, and G.D. Boswell. Locational Marginal Pricing for real and reactive power. 2008: IEEE.
[13] Stott, B. and O. Alsac, Fast decoupled load flow. Power Apparatus and Systems, IEEE Transactions on, 1974(3): p. 859-869.
[14] Zhou, W., Y. Peng, and H. Sun. Probabilistic wind power penetration of power system using nonlinear predictor-corrector primal-dual interior-point method. 2008: IEEE.
[15] Huang, C.J., et al., Applications of machine learning techniques to a sensor-network-based prosthesis training system. Applied Soft Computing, 2011. 11(3): p. 3229-3237.
[16] Bouckaert, R.R., et al., WEKA Manual for Version 3-6-1. 2009, The University of Waikato: Hamilton, New Zealand.
[17] Witten, I.H. and E. Frank, Data Mining: Practical machine learning tools and techniques. 2005: Morgan Kaufmann.

BIOGRAPHIES OF AUTHORS

Dr. Ibrahim Saeh received his BSc. (Electrical & Electronics) in (1997) from Bright Star University of Technology-Libya. MSc, (Electrical Power) in (2009) and Doctor of Philosophy (Electrical Power Eng.) in (2014) from Universiti Teknologi Malaysia (UTM). His research interests include power system analysis, deregulated power system, power system security and Artificial intelligence techniques. He has published as authored and co-authored a several research papers in numerous technical journals and conference proceedings Dr. Ibrahim is a director of Environmental Research & Clean Energy Centre (ERCE) and The International Society of Ocean, Mechanical and Aerospace –science and engineering (ISOMAse) member.

M.W. Mustafa he received his B.Eng degree (1988), M.Sc (1993) and PhD (1997) from University of Strathclyde. His research interest includes power system stability, FACTS, wireless power transmission and power system distribution automation, de-regulated power system, etc. He is currently a Professor and Deputy Dean (Academic) at Faculty of Electrical Engineering, Universiti Teknologi Malaysia. Dr. Mustafa is also a member of Institution of Engineers Malaysia (IEM) and a member of IEEE.

Dr. Nasir Ahmed Algeelani received the B.E. degree in electrical power system from University of Aden, Yemen, Aden, in 1997, the M.E. degree in electrical power system engineering from University Technology Malaysia in 2009 and the Ph.D. degree in high voltage engineering from University Technology Malaysia in 2014. He was a Lecturer with Industrial Technical Institute (ITI) for 25 years, where he is currently a senior lecturer of High Voltage Engineering. At the present he is a postdoctoral candidate at high voltage engineering department at University Technology Malaysia. He has published as authored and co-authored more than 30 papers in various technical journals and conference proceedings. His research interests include high-voltage instrumentation, partial discharge, detection and warning systems and condition monitoring of high power equipment.