International Journal of Environmental Research & Clean Energy
30nd April 2016. Vol.2 No.1

ISSN: 2502-3888 http://isomase.org/IJERCE1.php

Feature Selection for Static Security Evaluation and classification Classifier Design

Ibrahim Sae h[a], Walid Nabgan[b], Tuan Amran Tuan Abdullaha,[b*], Bahador Nabgan[b], Ramli Mat[b], Yahya Gambo[b], Kamal Moghadamian[b]

[a)] *Environmental Research and Clean Energy Centre (ERCE), Libya.*
[b)] *Centre of Hydrogen Energy, Faculty of Chemical Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia*

*Corresponding author: tuanamran@utm.my

Paper History

Received: 25-March-2106
Received in revised form: 16-April-2016
Accepted: 30-April-2016

ABSTRACT

This paper proposes feature selection approach (FSA) for static security evaluation (SSE) and classification. Data are generated on (30, 57, 118 and 300) bus IEEE test systems used to design the classifiers. 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.

KEY WORDS: *Feature Selection, Classifier design, Static Security Evaluation and classification.*

1.0 INTRODUCTION

Since 1920s, Power system security has been known as an important condition in preparing pattern and also procedure levels. Security means the capability of the power system in order to endure impending disruptions (contingencies) with no disturbance in order to customer support. It requires the sturdiness from the program and also depends upon the actual working situation along with depending likelihood of disruptions [1]. To be a certain dependable procedure of the power system, it should be correctly built to be able to protect and also constantly supervised to make sure that a security procedure is available constantly.

Through simulation, 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 perfor-mance index (PI) basis. In [2-4], numerous PI based methods have been reported. Artificial intelligence (AI) can be divided into two types of techniques, clustering techniques and classification techniques, and its powerful of reducing the data complexity, made it to use in various areas like medical and engineer-ing [5, 6].

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 [1].

In the literature, several keys have been suggested as standards for static security classification and evaluation [3, 7-10] include lines overloaded or \ and bus voltages collapse which let the system devi-ate from normal operating state limits. However, violations are not in the same level of the same signifi-cance.

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 equa-tions (1), and (2) are fulfilled. In case of one

ISOMAse
International Society of Ocean, Mechanical and Aerospace Scientists and Engineers
International Journal of Environmental Research & Clean Energy
30nd April 2016. Vol.2 No.1

ISSN: 2502-3888
http://isomase.org/IJERCE1.php

limitation is identified subsequent a contingency, the state of the system is categorized as static insecure (SI-Binary 0).

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.

Generally, most of the data mining 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 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.

1.2 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 [11] and used through this study as a matrix form. In this pro-gram, 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.

XSSE = {| V|i , θi , SGi , SLi , Sij }

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. [12, 13], and (2) all lines are not exceeding their power range as well (S< Smax.).

2.0 METHODOLOGY

After we initialize a pattern vector (XSSE) from data collection and data pre-processing, we initialize feature vector (ZSSE) 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 (ZSSE 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) whenev-er all the limitations mentioned in 3.1 are often satisfied for almost any provided backup. When some-body 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. The actual qualifying criterion operates is really a reduction calculate determining the amount of misclassification studies within the mix affirmation of every prospect feature part. This method has actually continued before the inclusion of many more characteristics produced absolutely no further reduction in the actual qualifying criterion operate.

3.0 RESULTS

The outcomes of information building and show choice stages of static security evaluation are shown in Table 1. The data samples in m-dimensional feature space are randomly split into training and test sets.

Table 1. 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%**

IJERCE | Received: 5 April 2016 | Accepted: 30 April 2016 | February-March 2016 [(2)1: 5-8]
Published by International Society of Ocean, Mechanical and Aerospace Scientists and Engineers, www.isomase.org.

ISSN: 2502-3888 http://isomase.org/IJERCE1.php

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.

3.0 CONCLUSION

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. Mentioned techniques can effectively be implemented for SSE with high accuracy rate.

Acknowledgement
The authors would like to express their appreciation to Environmental Research and Clean Energy Centre (ERCE) for the facilities and support.

REFERENCE

1. Morison, K., L. Wang, and P. Kundur, Power system security assessment. Power and Energy Magazine, IEEE, 2004. 2(5): p. 30-39.
2. Singh, S. and S. Srivastava, Improved contingency selection algorithm for voltage security analysis. Electric machines and power systems, 1998. 26(8): p. 855-871.
3. Ejebe, G. and B. Wollenberg, Automatic contingency selection. Power Apparatus and Systems, IEEE Transactions on, 1979(1): p. 97-109.
4. 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.
5. Camara, F., et al., Privacy Preserving RFE-SVM for Distributed Gene Selection. 2012.
6. Jun, S., A Clustering Method of Highly Dimensional Patent Data Using Bayesian Approach. 2012.
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. Momoh, J.A., Y. Xia, and G.D. Boswell. Locational Marginal Pricing for real and reactive power. 2008: IEEE.
12. Stott, B. and O. Alsac, Fast decoupled load flow. Power Apparatus and Systems, IEEE Transactions on, 1974(3): p. 859-869.
13. 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.