Computers and Electrical Engineering 68 (2018) 513–525

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Synchronized measurements-based wide-area static security assessment and classification of power systems using case based reasoning classifiers☆

Venkatesh T*, Trapti Jain

Discipline of Electrical Engineering, Indian Institute of Technology Indore, Indore 453552, India

ARTICLE INFO

Keywords:
Case-based reasoning
Class imbalance
Composite security index
Feature selection
Phasor measurement unit
Power system monitoring
Rule based expert systems
Static security assessment
Synchronized measurements
Wide-area security

ABSTRACT

This paper proposes a human intuition-based concept of Case-Based Reasoning (CBR) for Static Security Assessment (SSA) of power systems. Prior to security assessment, a composite Security Index *(SI)* defined in terms of line overload and voltage violation, is computed for each training pattern to label them into either secure or insecure class. Out of all phasor measurements obtained using Phasor Measurement Units (PMUs), only the real and reactive power flows, which are identified as relevant features are given as inputs to the proposed CBR system. The proposed approach has been implemented on IEEE 14 bus, IEEE 30 bus and Indian 246 bus networks and the results have been compared with those obtained using Support Vector Machine (SVM) and Artificial Neural Network (ANN) based classifiers. The results indicate that the proposed approach is more efficient, reliable and outperforms the above said classifiers in terms of classification accuracy at a comparable computation cost.

1. Introduction

Security assessment of power systems has always been a major concern, but their changing operational paradigm makes it more challenging now. The penetration of renewable energy generations and flexible loads tend to change the operating conditions more rapidly in comparison to the traditional power systems. The persistent increase in load demand has forced the utilities to operate the power systems closer to their operating limits. Early detection of the post-contingency problems can help the operator in taking the corrective actions timely and thus avoiding a blackout. This can be achieved by developing an approach for fast and reliable security assessment.

The traditional approach for security assessment is based on the data provided by Supervisory Control And Data Acquisition (SCADA), which is not necessarily synchronized across the system. This may cause significant error in the state estimation results considering the dynamic nature of the power system. On the other hand, PMUs which provide fast and accurate synchronized measurements help in obtaining updated information of the system being monitored at a particular time. Thus, the application of phasor measurements can significantly improve the possibilities for real time monitoring of power systems even during small disturbances. Hence, PMUs are widely employed for monitoring and control of power systems in a wide geographical area.

In recent years, various PMU based security analysis methods have been proposed in the literature. The authors in [1] have proposed a new voltage stability index calculated using the real time measurements from PMUs installed at the two ends of the

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. B.V. Manikandan.

* Corresponding author.
E-mail addresses: phd12120203@iiti.ac.in (V. T), traptij@iiti.ac.in (T. Jain).

https://doi.org/10.1016/j.compeleceng.2018.05.008
Received 14 April 2017; Received in revised form 4 May 2018; Accepted 7 May 2018

branches. These measurements include terminal end voltages and the power flows of the branches, provided that the PMUs are placed at the terminals of the transmission lines. A similar work reported in [2] calculates the stability index based on the voltage and current phasor measurements, which are obtained using the PMUs installed at high voltage level buses. Finally, this index is used to identify the high voltage buses that are vulnerable in case of occurrence of contingencies. A real-time voltage security monitoring framework has been presented in [3]. The line flow and bus voltage measurements-based sensitivity indices are computed at each substation using the PMU measurements. These indices from each substation are collected at the control center to provide a comprehensive voltage security index. The authors in [4] have proposed a distributed linear algorithm for online computation of voltage collapse sensitivity indices, which are calculated iteratively at each bus using the real and reactive power flows measured by the PMUs. In [5], PMU measurements have been used to compute Thevenin equivalent matrix to assess voltage security of a wind power plant.

Since the evolution of machine learning algorithms, they have been extensively applied for power system security assessment to overcome the drawbacks of traditional techniques. The authors in [6] have applied decision trees to evaluate power system security assessment. The decision tree follows a natural course of events by tracing relationships between events. However, they are prone to errors in classification, owing to differences in perceptions and the limitations of applying statistical tools. Over the past few years, several approaches using ANN have been used for static security assessment [7]. But, its major concerns are exhaustive training process and its complicated design procedure [8]. Since, power system security evaluation is a complex non-linear separability problem, the authors in [8,9] have applied SVM for power system security assessment as it is considered to be an effective tool for non-linear classification problems. However, the performance of the SVM classifier depends on the proper selection of kernel parameters and the choice of margin parameter *(C)* which is a more challenging task when the underlying distribution of the data is not known.

Case based reasoning approach is a reasoning methodology, which works on prior experience and examples. It solves the new problem by retrieving similar past examples and adapting their solutions. It has been predominately used in the field of life sciences, where the sufficient knowledge for parameter estimation is not available [10]. Some of its major applications include prediction and classification [11,12], knowledge-inference and evaluation [13,14], etc., In these applications, CBR systems are built for the classification problems mainly to determine whether a problem is a member of a class or not or which of the several classes it may belong to. The authors in [15] have used CBR technique and Naive Bayes learner for the design and development of an intelligent report system for forensic-autopsy. Inspired by the successful application of CBR in other technical domains, an attempt has been made in this paper to implement the CBR-based approach for power system security assessment. This paper also aims to utilize the knowledge extracted from the previous disturbances for predicting the system status of the present situation. The power system parameters changes continuously due to the dynamic nature of loads connected to it. Hence, the online learning property of the classifier is a critically required phenomena for the continuous monitoring of power systems. With the use of CBR, an online learning system can update its knowledge base with the data which is additionally acquired during learning. Thus, the knowledge base is continuously updated in real-time and their weights are updated. In addition, further studies have revealed that the performance and the application of CBR systems can be much improved with the development of different case adaptation techniques [16].

This paper proposes the use of CBR-based classifiers for power system static security classification using phasor measurements. Further, a novel case adaptation strategy using fuzzy clustering thresholding and minimum criterion methods has been proposed to make the CBR approach more reliable for security assessment. The proposed approach consists of four case based reasoning classifiers. The classifier I is used to predict the security status of the system as secure or secure during a specific loading condition whereas, classifier III is used to classify the system security status of the loading pattern with respect to its next contingency. The steady state variables such as voltage magnitude and voltage angle of the buses where PMUs are installed, real and reactive power flows of the branches measured by the PMUs form the components of the training pattern vector (Block I). Out of all phasor information obtained from PMUs, only the outgoing real and reactive power flows of the PMU buses are given as inputs to the classifiers I and II, as these measurements are identified as the relevant features by the feature selection technique (Block II). Thus, after successful training, classifier I predicts the system security status as secure or insecure (Block III) and classifier II gives the type of violation in terms of line overload, voltage violation or both in the insecure patterns (Block IV). The line outage contingency number and its respective pre-contingent power flows are provided as inputs to the classifiers III and IV. Similarly, the classifier III can accurately predict the security status of the system with respect to its next contingency (Block V) and classifier IV determines the type of violation in terms of either line overload or voltage violation or both in the insecure patterns (Block VI). The effectiveness of the proposed approach has been tested on IEEE 14-bus, IEEE 30-bus and a practical 246-bus Indian systems and their results are compared with the results of other classifiers.

The present paper is organized into 6 sections. The current section provides the importance of phasor measurements and also presents the relevant state-of-the-art survey on recent security assessment studies and various machine learning techniques. Section 2 presents the details of static security index used for classifying the training patterns into secure or insecure class. Section 3 proposes a new framework for SSA of power systems using synchronized measurements obtained from PMUs. The details regarding input data generation, selection of input features and methods to improve the class imbalance problem are also presented in this section in detail. Section 4 illustrates the application and design of CBR classifiers for security assessment of power systems. Simulation results obtained on various test systems have been presented in Section 5. Finally, Section 6 concludes the important finding of the work presented in this paper.