Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online
CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-27 (2016) 445–450

Machine Learning Techniques for Power System Security Assessment ⋆

Nikita V. Tomin, Victor G. Kurbatsky, Denis N. Sidorov, Alexey V. Zhukov

Melentiev Energy Systems Institute, Irkutsk, 664033 Russia (e-mail: tomin@isem.irk.ru).

Abstract: Modern electricity grids continue to be vulnerable to large-scale blackouts. As all states leading to large-scale blackouts are unique, there is no algorithm to identify pre-emergency states. Moreover, numerical conventional methods are computationally expensive, which makes it difficult to use for the on-line security assessment. Machine learning techniques with their pattern recognition, learning capabilities and high speed of identifying the potential security boundaries can offer an alternative approach. The purpose of this paper is not to suggest that one particular kind of machine learning technique for security assessment would be more appropriate than others. We start from the premise that almost every method may be useful within some restricted context. Based on this idea, we developed an automated multi-model approach for on-line security assessment. The proposed method allows us to automatically test the different state-of-art techniques in order to find both the best algorithm and its top performance tuning for particular analyzed power system. A case study using the IEEE RTC-96 system demonstrates the effectiveness of the proposed approach.

Keywords: smart grid, power system, security assessment, blackout, machine learning.

1. INTRODUCTION

The security of a power system is related to the ability of a power system to continue normal operation despite unplanned casualties to operating equipment, known as contingencies. A failure of security can cause equipment damage, low frequency or low voltages, and localized loss of power to customers, but the most severe, spectacular, costly and therefore most interesting security failures result in blackouts. During the past ten years events in North America, European Union and Asia have clearly demonstrated an increasing likelihood of large blackouts. This indicates that the security monitoring and control of power systems may need to be improved IEEE (2007), Wang et al.(2005), Syktyvkar (2010), Wehenkel (1995).

Most power plants and transmission lines are overseen by a supervisory control and data acquisition (SCADA) system. SCADA technology goes back 40 years. Much of it is too slow for todays challenges and does not sense or control nearly enough of the components around the grid. The result is that no single operator or utility can stabilize or isolate a transmission failure. However, at the transmission level, phasor measurement units (PMUs) have been introduced to improve grid reliability. One of the issues of applying and using the large amounts of PMU datasets are rapid decision making. Even if a lot of data was available, the operators at different control centers did not take the proper actions in time to prevent the blackouts. The decision making and onus is usually still with the expertise of the grid operators.

For the time being there is a wide spectrum of approaches and tools for the assessment of security. The primary objective of security assessment techniques, then, is to measure the vulnerability of the system to blackouts. Unfortunately. real-time evaluation of this measure is not within the capabilities of current conventional technology. This is due to the fact that numerical conventional methods are computationally expensive, which makes it difficult to use for the on-line security assessment. Managing a modern grid in real-time requires much more automatic monitoring and fast security assessment measures. Machine learning techniques with their pattern recognition, learning capabilities and high speed of identifying the potential security boundaries can potentially offer such on-line solution.

Many researchers deem that machine learning (ML) methods such as artificial neural networks (ANNs), decision trees (DTs), deep learning models etc. are indeed able to provide interesting security information in power systems, Syktyvkar (2010), Wehenkel (1995), Diao et al. (2009), Tomin et al. (2014). Actually, in their philosophy machine learining-based approaches are quite similar to existing practices in power system security studies, where limits are derived from simulations, though in a manual fashion. But machine learning approaches are more systematic, easier to handle and master, in short more reliable and powerful. An important asset of machine learning methods lies in the explicit and logical representation they use for the induced classification rules, which, together with simplicity, provide a unique explanatory capability, Sidorov (2015).

⋆ This work was supported by the Russian Scientific Foundation under Grant No. 14-19-00054 and the 2015 Endeavour Scholarship and Fellowship program.

10.1016/j.ifacol.2016.10.773

This work outlines some experience obtained at the Melentiev Energy Systems Institute, Russia in developing machine learning-based approaches for detecting potential dangerous states in power systems before they lead to major emergencies and blackouts. The proposed method allows us to automatically test the different state-of-art techniques in order to find both the best algorithm and its top performance tuning for particular analyzed power system. The calculations involved the different machine learning-based models, such as Multilayer Perceptron (MLP), Support Vector Machine (SVM), self-organized Kohonen network (SOM), Extreme Learning Machine (ELM), Random Forest (RF), Classification and Regression Tree (CART). A case study using the IEEE RTC-96 system demonstrates the effectiveness of the proposed approach. The suggested approach is implemented in the free software environment R intended for calculations with an open-source code.

The paper is organized as follows. Section 2 consists of two subsections. First subsection provides the problem statement in the field of modern security assessment problem. Second subsection presents the state-of-art in the field of on-line security assessment technologies. In section 3 a novel automated multi-model approach based on machine learning is developed for for online security assessment in power system. Section 4 presents the experimental results and discussion.

2. BACKGROUND

2.1 Problem Statement

Practical experience demonstrates that most blackouts begin with a large disturbance (a disturbance, which may or may not cause cascading failures), which leads to a slow deterioration of the system conditions, IEEE (2008), Muller et al. (2012), Lachs (2002). The system parameters may still remain within specified limits, but many of these parameters are on the boundary of stability; even a small additional disturbance can cause a simultaneous violation of several system parameters, and as a result, fast deterioration of the system state. If such conditions are identified as pre-emergency, preventive actions can be taken, and major events avoided. Unfortunately, in current competitive environment, such conditions may not be easily detected because different problems may simultaneously occur in different parts of a large network within different jurisdictions. The liberalisation process in power systems has created an additional interface which can adversely impact communication and coordination activities between operators on both sides. The past blackout events reveal that underlying causes are also partly linked to the liberalisation trends due to missing incentives to invest in reliable infrastructures.

To monitor that the power system is within its limit, determined either online or offline, the primary measurement tools are SCADA systems and post processing by a state estimator, Morison (2004). The ENTSO-E network code on operational security requires each TSO to classify its system according to the system operating states ENTSO(2013). Figure 1 shows the different operating states of a power system as identified by Dy Liacco and adopted by authors of this paper.

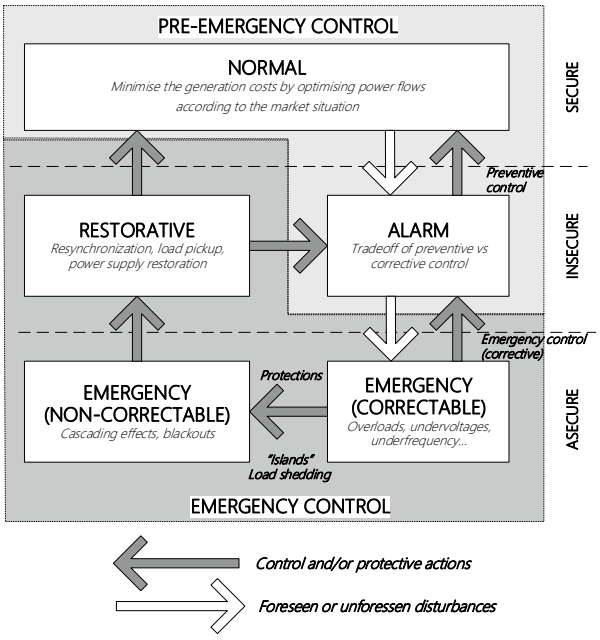

Fig. 1. Operating states and transitions. Adapted from [Fink (1978)]

2.2 The state-of-art

In the last few years significant advances have been made in the field of on-line security assessment technologies, CIGRE (2007). In this report, there are reported 19 tools for dynamic security assessments in use, under testing and under development. A review of 15 of these state-of-the-art tools shows a wide variety of implementations. The range of assessment capabilities includes determination of critical contingencies, transfer limits, and determination of remedial measures necessary to ensure security. The computational methods used for each type of security assessment is varied, and depends on the specific requirements, power system characteristics and, in some cases, the techniques available in the state-of-the-art tools used.

However, conventional numerical techniques are usually time consuming and therefore are not always suitable for real-time applications. Also, these methods suffer from the problem of misclassification or/and false alarm. Misclassification arises when an active contingency is classified as critical.

A great many studies show that the effective solution to this problem can be found on the basis of machine learning methods which normally include ANNs, DTs, deep learning models, etc. In the mid-eighties, it has already been demonstrated that machine learning is indeed an efficient and effective way to generate reliable and interpretable security rules from very large bodies of simulated examples, Wehenkel(1994), even for as complex systems as are real large-scale power systems. The extracted rules are found to express explicitly problem specific properties, similarly to human expertise, and hence may be easily appraised, criticized and eventually adopted by engineers in charge of security studies. The flexibility of the machine learning framework allows one to tailor the resulting information to analysis, sensitivity analysis and control applications.