Electric Power Systems Research 141 (2016) 344–353

Contents lists available at ScienceDirect

Electric Power Systems Research

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

Decomposed algorithm for risk-constrained AC OPF with corrective control by series FACTS devices

Dmitry Shchetinin*, Gabriela Hug

ETH Zurich, Physikstrasse 3, Zurich, Switzerland

ARTICLE INFO

Article history:
Received 29 February 2016
Received in revised form 11 July 2016
Accepted 9 August 2016

Keywords:
Optimization
Power system security
Flexible AC transmission systems
Risk-based optimal power flow
Corrective control

ABSTRACT

Maintaining a desired level of security in a power system while maximizing its efficiency is a cornerstone of system operation. In recent years, system security has been jeopardized by increasingly variable power flow patterns caused by renewable generation and market liberalization. One potential solution is to employ corrective power flow control by means of series FACTS devices. However, this requires solving a complex optimization problem, which is difficult to do quickly for large-scale power systems. While several decomposition strategies have been proposed to address this issue, existing approaches rely on a DC approximation of a power system model and thus do not fully capture system's behavior. This paper presents a decomposed iterative algorithm for the probabilistic security-constrained OPF problem, which is formulated for an AC model of a power grid with series FACTS devices and outages of more than one element as credible contingencies. The algorithm is based on so-called locational security impact factors, which represent sensitivities of the security index to changes in generator outputs. The IEEE 24-bus and 118-bus systems are used to examine the effectiveness of the proposed method and to analyze the effect that series FACTS devices have on security and efficiency of system operation.

1. Introduction

With the liberalization of electricity markets and higher penetration of renewable generation the problem of balancing security and efficiency of power system operation is becoming increasingly challenging. Excessively rigorous security criteria may lead to a sub-optimal generation dispatch, reducing social welfare, whereas sacrificing security for efficiency may result in major blackouts. Hence, quantifying security of power systems and enhancing it while keeping the total supply cost as low as possible are important aspects of system operation.

Traditionally, system security has been quantified by deterministic approaches such as the $N-1$ criterion [1–3]. Despite its simplicity, this criterion treats all outages equally in terms of both their probability to occur and their effect on the system, which does not reflect reality and may lead to inefficient operation. To overcome this drawback, probabilistic approaches to system security, based on a notion of risk [4–7], have been proposed. Risk-based security indices can be used for both increasing operators' awareness of the system state [8,9] and optimizing power system performance [10–12], e.g. by formulating the Risk-Constrained OPF (RCOPF) problem [13–18].

Power system security can be enhanced by generation re-dispatch [2], load shedding [19,20], or power flow control [21,22], e.g. by means of FACTS devices [23]. The latter is preferable as its cost is limited to the procurement and maintenance cost of control devices, whereas the other two reduce social welfare and should be ideally avoided. Since FACTS devices are fast-acting, they enable the implementation of corrective power flow control [24], i.e. the set-points of the devices can be changed quickly according to the state of the system. While FACTS devices are not widely used due to their high cost, recent developments such as Distributed FACTS [25] are promising as they offer potentially reduced installation and maintenance costs, which can lead to their extensive use.

Both the deterministic and probabilistic security-constrained OPF problems are notorious for their difficulty because each is a large-scale, nonlinear, non-convex optimization problem that usually has to be solved as quickly as possible. Due to its practical importance, the security-constrained OPF problem has received a lot of attention from the research community and a number of formulations and solution algorithms can be found in the literature. An extensive overview of major challenges and existing endeavors in this field has been presented in [26] and, more recently, [27].

This paper focuses on the RCOPF problem, which has the objective of minimizing the total supply cost in the system while keeping

* Corresponding author.
E-mail addresses: shchetinin@eeh.ee.ethz.ch (D. Shchetinin), hug@eeh.ee.ethz.ch (G. Hug).

http://dx.doi.org/10.1016/j.epsr.2016.08.013
0378-7796/

the risk below a given value and, due to its size, becomes difficult to solve in a centralized fashion for real-world grids. Existing approaches for decoupling this problem include using Benders decomposition [14] or so-called locational security impact factors (LSIFs) [15,28,29]. However, studies [14,15,28] are based on a DC approximation of a power system, and the problem formulation in [29] does not include corrective control. In addition, only single-element outages are considered in these studies and communication overhead between parallel processors is not taken into account when analyzing the potential acceleration of the algorithm with parallelized computations.

The main contributions of this paper are threefold. First, it presents a decomposed iterative algorithm for solving the RCOPF problem for a full AC model of a power system with corrective control. The utilization of the AC model poses certain challenges, e.g. some contingencies may have no steady-state solution. The paper discusses a possible strategy of dealing with such contingencies. Second, the paper considers outages of more than a single element in the system, which might help capture potential danger posed by cascading outages and provide system operators with a better risk estimate. For the sake of presentation simplicity, the paper is focused only on $N-1$ and $N-2$ outages, but the proposed algorithm can be straightforwardly extended to include any $N-k$ outages as credible contingencies. The last focus of the paper is to examine what the best way of parallelizing the proposed algorithm is and how communication overhead influences the simulation time. In addition, the paper analyses the impact that series FACTS devices have on the risk and cost of system operation as well as on the computation time.

The rest of the paper is structured as follows: Sections 2 and 3 provide an overview of steady-state models of series FACTS devices and risk-based security indices, respectively. In Section 4, locational security impact factors are described. In Section 5, the centralized formulation of the AC RCOPF is presented and Section 6 provides the description of the proposed iterative algorithm for solving the AC RCOPF problem. In Section 7, simulation results are provided, and Section 8 concludes the paper.

2. Series FACTS modeling and control

In general, security of a power system depends on both voltage magnitudes at buses and currents in transmission lines and transformers. However, in this paper only the effect of the line flows on reliability is taken into account, which is why series FACTS devices are considered as a means of power flow control. Examples of such devices include the Thyristor Controlled Series Compensator (TCSC), Static Synchronous Series Compensator (SSSC) [12], and recently developed distributed FACTS (DFACTS) [25] devices. For steady-state analysis, all aforementioned devices can be modeled as a variable reactance inserted in series into the transmission line. By changing the value of X_{FACTS}, the susceptance of a transmission line with a series FACTS device can be changed, which in turn causes the change in the line flow, thus enabling power flow control. All power electronics-based FACTS devices are fast-acting, which provides an opportunity of quickly adjusting line flows after the occurrence of a disturbance to eliminate possible violations of operational constraints. This may allow the operator to choose a generation dispatch with a lower total supply cost while still satisfying security requirements. Such a control strategy, which is called corrective power flow control, is considered in this paper.

3. Risk-based security indices

As was mentioned in Section 1, probabilistic approaches to system security are based on a concept of risk, which for a certain event is defined as the product of its probability to occur and the consequences that will ensue. The events are represented by outages of various elements in the system called contingencies and the total risk is the sum of individual risks of all considered contingencies along with the normal state. The value of the total risk provides a quantitative measure of system security, as opposed to a binary $N-1$ criterion. The risk value can be used as a constraint in OPF to determine the most cost-efficient generation dispatch that still satisfies security requirements.

Unfortunately, at this point there is no benchmark method of selecting the contingencies to be included in the risk calculation as well as quantifying the consequences of considered contingencies. Proposed risk metrics vary substantially and are often designed for different purposes and time-scales. Please note that this paper does not aim at developing a new risk index and comparing this index with others found in literature. Rather, it adopts already existing metrics that are deemed well suited for the main focus of this study, which is the real-time optimization of power system operation.

Existing approaches to quantifying the consequences of contingencies can be divided into two groups. The first group determines the economic effect of contingencies [5,12] using various indices such as expected energy not served (EENS), loss of load probability (LOLP), etc. This approach assumes certain actions from a system operator and its main application is in medium and long-term planning. The second group [9,4] uses a purely technical definition of consequences as functions of the loadings of system elements. Here, the risk index is independent of any assumptions regarding the actions of a system operator, but rather reflects the level of danger to the system if no such actions are undertaken. This approach is well suited for short-term planning or system operation and, therefore, it is employed in this paper.

Contingencies for the risk calculation can be chosen either by the Monte-Carlo approach [5] or from a pre-determined list of outages that are deemed credible [4]. In this paper, the latter approach is employed with considering all $N-1$ and $N-2$ outages to be credible. This is done in order to capture the risk pertaining to cascading outages, which may occur if the outage of a single element leads to high loadings of other elements, making them more likely to become disconnected and cause further exacerbation of the system state.

To compute the risk of a certain contingency, the following procedure is used. First, the operational constraints such as line flow limits are relaxed by adding slack variables:

$$h_{p,q}(P_G, x_q) \le k_p \cdot \bar{h}_p + s_{p,q}, \quad s_{p,q} \ge 0 \tag{1}$$

where $h_{p,q}$ is the operational constraint of element p in contingency q, which is a function of generator outputs P_G and control variables x_q, $\bar{h}_p$ is the limit on this constraint, and $s_{p,q}$ is the corresponding slack variable. The slack variable represents the part of the loading of the corresponding element that is considered to be unsafe. Coefficient $0 < k_p \le 1$ controls the loading level at which the slack variable becomes non-zero and starts to contribute to the risk index.

To quantify the consequences of a contingency, so-called severity functions introduced in [9] are used. For a certain element, the severity function, shown in Fig. 1a, is a quadratic function of its loading. The consequences value for a given system state is determined as the sum of the severity functions values for all elements that are still in operation in this state:

$$c_q = \sum \hat{c}_p(s_{p,q}) \tag{2}$$

The probability of element p to fail and create contingency q, shown in Fig. 1b, is chosen based on [15] to have two components. The first is constant and represents the outage probability obtained from historical records, and the second is a quadratic function of the element's loading before the outage. This allows capturing a