Electrical Power and Energy Systems 77 (2016) 372–384

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A mixed integer programming model for optimal fault section estimation in power systems

Aécio L. Oliveira *, Olinto C.B. de Araújo, Ghendy Cardoso Jr., Adriano P. de Morais, Lenois Mariotto

Energy and Power Systems Research Center, Federal University of Santa Maria, Santa Maria, Rio Grande do Sul, Brazil

ARTICLE INFO

Article history:
Received 16 March 2015
Received in revised form 24 June 2015
Accepted 25 November 2015
Available online 11 December 2015

Keywords:
Alarm processing
Fault diagnosis
Fault section estimation
Mixed integer programming
Power system protection

ABSTRACT

This paper proposes a methodology to deal with the fault section estimation problem in electrical power systems. The main motivation for this study lies in the fact that operators of control centers usually are subject to information overload during great contingencies. The fault diagnosis is formulated as an optimization problem and solved through two stages: classification of events at equipment level and the fault section estimation. The first stage consists of a heuristic based on Bayes' theorem that provide the input to the second stage where a mixed integer programming model is solved by commercial package in order to determine the faulted section. Several fault scenarios from a real Southern Brazilian subsystem were considered to validate the methodology. The results show that the proposed method can correctly identify the faulted section even in case of multiple faults or in case of improper operation of protective devices.

Introduction

During normal system configuration, it is expected that protective relays detect fault disturbances and, if necessary, the circuit breakers (CB) open in order to isolate the defective part of the system. It is known that due the complexity of the fault and size of the outage area, the protection reliability tends to decrease. Poor protection performance is usually caused by more than one factor. Multiple faults, power swing, incorrect relay setting, human errors are some examples of events that can cause improper operation of protective devices. In these cases, the fault analysis in control centers become a challenge, even to skillful engineers, who prioritize some records because, in general, there is not enough time to examine all of them.

The fault section estimation problem (FSE) is related to the identification of the faulted section from the analysis of alarm messages sequence provided by Supervisory Control and Data Acquisition (SCADA) during power system disturbances. The fault diagnosis aims to assist Control Center operators with required information to understand the fault disturbance and to perform corrective actions to restore the service as soon as possible [1]. Thus, diagnosis assists the operators to complete the message analysis in a shorter period of time assuring more effective decisions.

In the last two decades, a large number of methodologies to solve the FSE problem have been proposed in the literature. According to [2], FSE methodologies are divided in two categories: one infers the faulted sections from reported alarm by means inference rules and the other models fault diagnosis as a combinatorial optimization problem. In this respect, Expert Systems (ES) [1], Artificial Neural Networks (ANNs) [3], hybrid systems based on the combination of features of ES and ANNs [4] are the most conventional inference-based approaches, even though these techniques have some disadvantages. Expert systems need a formalized knowledge that represents the operator expertise, process that may require an extensive interviewing effort, whereas ANNs require an appropriate number of samples for training process and thus provide a good generalization capability. Other important inference-based approaches include fuzzy logic [5,6] and cause–effect networks [7,8]. These methodologies can handle incomplete and uncertain information, however they still require engineers experience and historical data to create inference rules.

In [9], the authors present the first attempt in the formulation of the FSE problem as a combinatorial optimization problem, where they employed a Genetic Algorithm (GA) to find out the most likely hypothesis that better explain the issued alarms. A critical analysis of recent research shows an inclination for the use of metaheuristics approaches to solve the FSE problem. The most commonly used metaheuristics for fault diagnosis are GA [10,11] and Tabu

---

* Corresponding author. Tel.: +55 55 3220 6110.
E-mail addresses: aecio.oliveira@ufsm.br (A.L. Oliveira), olinto@ctism.ufsm.br (O.C.B. de Araújo), ghendy@ufsm.br (G. Cardoso Jr.), adriano@ctism.ufsm.br (A.P. de Morais), mariotto@ufsm.br (L. Mariotto).

http://dx.doi.org/10.1016/j.ijepes.2015.11.090

Search (TS) [12,13], wherein [13] combines the global search features of the GA with the TS ability in local searching. Besides, several bio-inspired metaheuristics have been developed and applied to estimate the faulted section including Particle Swarm Optimization [14], Immune Algorithms [15] and Artificial Bee Colony [16]. Although metaheuristics usually provide a sufficiently good solution to large-size problems in a limited time, there is often some parameter tuning issues that need to be carefully addressed and most of these methods are not deterministic. In real operational situations, the lack of conviction in a right answer may lead the operator to abandon a software solution just to prevent future errors of decision.

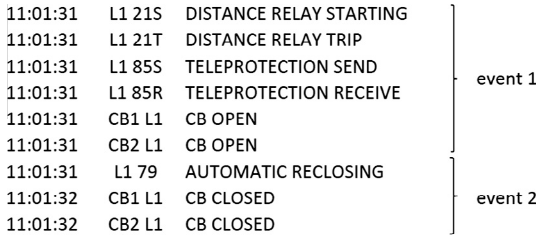
In Ref. [12], the FSE problem is formulated as an unconstrained binary integer programming problem and employing a TS algorithm to minimize the discrepancy between the reported and expected alarms of protective devices. The proposed approach is based on a temporal constraint network to handle temporal information provided by sequence of events. The methodology proposed by [17] consists of a two-level analysis that classifies the issued alarms with the intention of accelerating the problem solution. A constructive heuristic is developed to process the information provided by SCADA employing event patterns characterized by expected status of protective devices in each power system component. The FSE problem is formulated as a Binary Integer Programming model (BIP) using processed information of the constructive heuristic together with statuses of circuit breakers to estimate the faulted section and the improper operation of protective devices. The instances of the BIP model were solved using a commercial optimization solver.

In this work it is intended to develop a new approach that combines probabilistic analysis at equipment level of report alarms using the Bayes' theorem and a systemic analysis using pre-processed information and circuit breakers status. The FSE problem is formulated as a Mixed Integer Programming model (MIP) and it is able to estimate the faulted section and to identify the improper operation of protective devices. Several tests were performed on large Southern Brazilian power system using a real monitoring system of the power utility. Complex events with multiple faults and multiple malfunctions of PRs and CBs were considered in the simulations.

Methodology

Some questions regarding to alarm processing should be addressed by operators before any further fault analysis. During real-time operation, engineers must pay attention to the reported alarms in SCADA in order to understand what happened, as well as identify the faulted section and the malfunctioned devices, such as protective relays (PR) and CBs malfunctions. These questions are the basis for the development of the proposed methodology to solve the FSE problem.

The proposed fault diagnosis approach is based on two interconnected modules: classification of events and fault section estimation. The time is a variable not included as part of the model, which means that the optimization model analyzes the fault as if all alarms have triggered at the same instant. For the purpose of experimental, we split a real alarm log, provided by a transmission network operator from Brazil, into fixed size of one minute time windows. This time size was defined heuristically, considering a reasonable interval to separate the fault events from independent alarms that have no apparent causal relation to the disturbance. Note that it is possible the occurrence of several events in a time window. In this case, it is essential to extract pieces of information that represent a transition from a triggering event (e.g., fault) to a consequence event (e.g., automatic reclosing). As an example, Fig. 1 shows a small real alarm log composed of two different events where the reclosing alarm is the information that distinguish the event 1 (fault in line L1) from event 2 (line reclosing). Other examples of window breaker considered may be cited such as: power swing blocking relay (68), repetitive alarm with undefined status (noise) and repeated alarm with opposite status.



```
11:01:31   L1 21S   DISTANCE RELAY STARTING
11:01:31   L1 21T   DISTANCE RELAY TRIP
11:01:31   L1 85S   TELEPROTECTION SEND            event 1
11:01:31   L1 85R   TELEPROTECTION RECEIVE
11:01:31   CB1 L1   CB OPEN
11:01:31   CB2 L1   CB OPEN
11:01:31    L1 79   AUTOMATIC RECLOSING
11:01:32   CB1 L1   CB CLOSED                      event 2
11:01:32   CB2 L1   CB CLOSED
```

Fig. 1. Example of alarm log.

A network topology processor procedure proposed by [18] is applied to determine the topology model of the power system using real-time status of circuit breakers and switches. The network topology is always determined prior to the beginning of a new event. Each component belonging to the energized topology that is a reported in the event must be analyzed by the classifier of events. The classification determines the fault direction analyzing each protection performance after the disturbance, whose answers are potentially valuable information for the optimization model. Finally, a mathematical programming model analyzes pre-processed classifications together to CBs statuses to estimate the faulted section, as well the malfunctioned protective devices. Fig. 2 shows the concept of the system.

When faults occurred, protections must detect them and trip circuit breakers. This cause–effect relationship during disturbances is described as a rule. This rule represents a plausible event pattern of the protection operation that is stored into a database, which will be used by an inference engine to correlate well-known events with issued alarms to a diagnose the fault. Every event pattern is modelled according to a possible operation of the protective schemes of each section in the power system. Note that it is not necessary that an event has already happened to be in the database. Five types of protective sections (line, busbar, transformer, synchronous generator and capacitors bank) are considered in this paper and their protection schemes are illustrated in Figs. 3–7. Protection schemes are based on real schemes employed by a large Southern Brazilian power utility and the supervised digital points associated with each equipment protection follows the ANSI/IEEE C37.2 standard. Tables 1–5 present the set of event patterns elaborated for each type of equipment.

Every protection scheme is composed of two redundant protection systems where the back-up protection operates in case of failure of the main protection. It is usual to choose different measuring principles which monitor different system criteria for duplicate phase and ground fault protections. In this work, the different protection functions are grouped together with other functions that have the same application of protection (main, local back-up, remote back-up). Each row in the tables above corresponds to a protection application, which data is fed by corresponding protective devices. For example, the transmission line protection is divided in seven input data as follows:

- Selective protection: includes differential relay (87L) and first zone of distance relay (21-1) at both line ends.
- Backup protection installed at substation S1: includes a directional earth overcurrent relay (67N), second (21-2) and third (21-3) zones of distance relay. Both distance zones are composed of starting and tripping alarms.