Reliability Engineering and System Safety 169 (2018) 179–186

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A multi-uncertainty-set based two-stage robust optimization to defender–attacker–defender model for power system protection

Tao Ding [a,b,*], Li Yao [a], Fangxing Li [c]

[a] State Key Laboratory of Electrical Insulation and Power Equipment, Xi'an Jiaotong University, Xi'an 710049, China
[b] Department of Electrical Engineering, Tsinghua University, Beijing 100084, China
[c] Department of Electrical Engineering and Computer Science (EECS), University of Tennessee, Knoxville, TN 37996, USA

ARTICLE INFO

Keywords:
Analytic hierarchy process
Column-and-constrains generation algorithm
Defender–attacker–defender
Multi-uncertainty-set
Power grid protection
Robust optimization

ABSTRACT

To handle rapidly growing threats from deliberate attacks, the critical components in power grid should be identified and protected. This paper proposed a defender–attacker–defender model to deal with power grid protection problem, in which the uncertain attacks and load types are considered. Furthermore, multiple uncertainty sets are introduced to characterize the possible realizations of disruptions caused by attackers, and the probabilities of the multiple uncertainty sets are estimated using analytic hierarchy process. Then, the problem is formulated as a multi-uncertainty-set based two-stage robust optimization model which can be termed as a mixed-integer tri-level programming and solved by column-and-constrains generation algorithm with a master-subproblem framework. The test results on a standard IEEE RTS 24-bus system show the effectiveness of the proposed model by considering multiple uncertainty sets and load types.

1. Introduction

Critical infrastructure, such as power grid, serves as the backbone of health welfare, commerce, and national security. As a result, the protection of infrastructure to mitigate the impact of outage induced by attacks, has attracted much attention in recent years [1,2]. According to a report from the National Academy of Sciences of America, US electricity grid is incredibly vulnerable to terrorist attacks which may lead to several weeks or even months' large-area regional blackouts [3]. Such risk also exists in China, though power grids protection and recovery are given high priority and some measures are adopted to improve the reliability, e.g., regional power grid must satisfy $N-1$ criteria [4]. In particular, considering the diversity and severity of coordinated terrorist attacks, traditional tools are not able to guarantee correct operations under multiple contingency [5-7]. Hence, it is urgent to explore advanced tool to mitigate such vulnerability when suffered from intentional attacks. For illustrative purpose, defender hereinafter refers to security department or power grid operator to protect the power grid from deliberate attack, while attackers may be a group of terrorists.

Power grid interdicting problem, aiming at identifying the contingencies that may cause the most destructive damage to power grid, has been extensively studied [8-11]. To solve this problem, bi-level models are typically utilized which reflect the interaction between two different agents, namely attackers and defenders. Attackers intend to disable a certain number of transmission lines or substations to inflict the greatest loss on power grid, while defenders response to the attack to minimize the loss by re-dispatching power. Generally, the loss can be measured in total amount of load shedding.

However, bi-level models only consider passive defenses, i.e., defenders can only react against disruptive actions afterwards. As a complement and supplement to the bi-level model, a tri-level model, i.e., defender–attacker–defender model, is established to represent active attack defense [12-15], where countermeasures, such as patrolling localized assets, undergrounding critical targets and stockpiling spares of critical infrastructure components, may be undertaken by defender before disruption occurs. In contrast to bi-level models, the tri-level model focuses on producing optimal protection plan, which is used to deal with the Power grid protection problem. Similarly, the classic defender–attacker–defender model is proposed by Brown et al [12]. Yao et al. [13] pioneer the tri-level optimization in power network defense and describe a decomposition approach for finding an optimal solution to tri-level model, which is based on an iterative method to solve smaller nested bi-level problems. They argue that the tri-level optimization offers superior defense planning than bi-level optimization, since it captures an additional level of interaction between defender and attacker. Delgadillo and co-workers [14] formulate the electric grid defense planning problem as a mixed-integer nonlinear tri-level program, which is solved by a two-stage methodology by transforming the original problem into an equivalent bi-level programming problem in the first stage

* Corresponding author.
E-mail address: tding15@mail.xjtu.edu.cn (T. Ding).

http://dx.doi.org/10.1016/j.ress.2017.08.020
Received 15 July 2016; Received in revised form 4 August 2017; Accepted 29 August 2017
Available online 31 August 2017
0951-8320/

Nomenclature

Indices and sets

m	index of generator m
l	index of line l
n	index of bus n
s	index of uncertainty set s
Λ_n	set of generators at bus n

Parameters

N_s	number of assets disrupted in uncertainty set s
R	defense budget
S	uncertainty sets budget
w_s	probability of uncertainty set s
ρ_n	penalty coefficient of load at bus n.
$P^g_{j,\max}$	upper limit of generator's power output
$P^f_{l,\max}$	maximum power flow on line l
D_n	demand at bus n
M_l	sufficiently large number for line l
χ_l	reactance of line l
$\delta_{n,\max}$	maximum value of phase angle at bus n, equal to $\pi/2$ in this paper
$\delta_{n,\min}$	minimum value of phase angle at bus n, equal to $-\pi/2$ in this paper
$O(l)$	origin bus of line l
$D(l)$	destination bus of line l

Decision variable

$p^{g,s}_j$	power output of generator j in set s
$p^{f,s}_l$	power flow of line l in set s
ΔP^s_n	load shed at bus n in set s
x_l	binary protection decision for line l
y^s_l	binary attack decision for line l in set s
δ^s_n	value of phase angle at bus n in set s
LS	totally load shed in the power grid
CLS	shedding amount of critical load
θ_s	auxiliary variable for uncertainty set s
Q_s	optimal value of subproblem for uncertainty set s

and solving the bi-level programming via the implicit enumeration algorithm. Although this methodology can obtain global optimality in finite time, it is difficult to be applied to large scale power system due to its expensive computation cost. Yuan et al. [15] propose a column-and-constrains generation algorithm, a recent solution strategy for two-stage robust optimization, to solve the tri-level defender–attacker–defender model. This approach outperforms the existing exact algorithm significantly with respect to computational time.

It is noted that in existing literatures, the number of out-of-service components is determined before the defense decision-making. Nevertheless, in practical, uncertain information of attackers, such as the number of attack sources and the main target of attackers, is difficult to foresee accurately. Hence, it motivates us to fully leverage the existing information and make a systematic decision considering uncertain factors of attackers. This idea is based on the fact that intelligence gathering and information sharing play increasingly important role in preventing terrorist attack in several countries according to a recent report [16]. It is possible for security department to provide alert information to system defenders [17], and moreover, defense strategy can be performed with a tradeoff among possible scenarios accordingly.

To address this issue, we introduce multiple uncertainty sets for simulating uncertainties, where each uncertainty set contains possible realizations of uncertain factors and different uncertainty sets have different probabilities [18]. It is worth mentioning that the probabilities of uncertainty sets rely on existing information as well as decision-maker's risk preference of power systems.

Moreover, the impact of load types is neglected in all the previous works which is very critical for the power system protection. In fact, the electricity loads are practically divided into several types with respect to their importance, so different penalty for load shedding should be adopted according to the load types [19]. Meanwhile, the attacker agent prefers causing social panic and worries through interrupting power supply of public facilities and transportation systems which closely relate to residents livings [3]. Thus, attaching different types to loads has an effect on protection decision. To address this problem, penalty coefficients, revealing the significance of electricity loads in proportion to importance, are customized in the model we propose.

According to the study in reference [20], our research studies the attack against multiple elements in network, and uses protection as defense measure. Compared with above references and some closely related literature such as [21-36], our study has the following major contributions:

(1) A defender–attacker–defender problem is presented as a flexible mechanism to make the optimal protection decision. Uncertainty from attackers is considered in the model by multiple uncertainty sets, whose probabilities are obtained through analytic hierarchy process. Unlike the previous related research ignoring the existing information regarding attacks, the proposed approach considers the attacks' strength, risk management, etc. to yield a comprehensive protection plan.
(2) The effect of load types on decision-making is investigated by comparing the protection with and without the consideration of load types. The load types take the customer priorities into consideration, and therefore lead to more practical protection decision.
(3) The defender–attacker–defender model is solved by the column-and-constrains generation algorithm, which can obtain the global optimal solution by proper mathematical transformations. Since the subproblems have a very similar mathematical structure and are mutually independent in the structure, we propose that the group of subproblems can be solved in a parallel manner, which will accelerate the solution procedure.

The paper is organized as follows. In Section III, the analytic hierarchy process constructs multiple uncertainty sets and the two-stage robust optimization model is set up for defender–attacker–defender problem. Section IV introduces a mathematical transformation to reformulate the proposed model, so that the column-and-constraints generation algorithm can be employed to solve the proposed model. In Section V, numerical results are provided and summarized. Section VI draws main conclusions and discussions in future research directions.

2. Model formulation

2.1. Analytic hierarchy process

In this section, we will construct multiple uncertainty sets and assign corresponding probabilities to them. Therein, each uncertainty set includes several attack scenarios and only the quantity of out-of-service assets is specified, while the location of disrupted assets by attacks is uncertain. To better recognize the probability of each uncertainty set, analytic hierarchy process (AHP) is used to find a probability that best suits decision requirements [37-39]. The probabilities determination problem is decomposed into a hierarchy including several elements, each of which characterizes an aspect of deciding problem [39]. Considering the intrinsic interactions of these elements, AHP partitions all elements into 3 layers, namely goal layer, criteria layer and scenario layer.

Such a hierarchy structure is depicted in Fig. 1, with the goal at top, a number of scenarios at the bottom, and four criteria between the top and bottom. Therein, the criteria include attackers' strength, risk preference, existing defense plans, and valuable intelligence information. Meanwhile, uncertainty sets with the specified number of disrupted assets are modeled in the scenario layer.