Electrical Power and Energy Systems 99 (2018) 594–602

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

# An optimization model for power grid fortification to maximize attack immunity

Alberto Costa[a,b,*], Dionysios Georgiadis[b], Tsan Sheng Ng[a], Melvyn Sim[c]

[a] National University of Singapore, Department of Industrial Systems Engineering and Management, Singapore
[b] ETH Zurich, Future Resilient Systems, Singapore
[c] National University of Singapore, Department of Decision Sciences, Business School, Singapore

ARTICLE INFO

*Keywords:*
Interdiction
Power grids
Robust optimization
Stackelberg game
Trilevel programming

ABSTRACT

This paper studies the problem of allocating fortification resources in an electric power grid with the aim of maximizing its immunity against malicious attacks. An attacker of the grid allocates his attack resource budget to destroy targeted transmission lines in the network. The attacker is successful if the power load shed after attack exceeds a specified permissible level. On the other hand, the grid defender allocates his fortification budget to the lines in a manner to deter as many such attacks as possible, in particular to maximize the budget required by the attacker to be successful. This is termed as the *attack immunity* in our work. We formulate this as a two-stage optimization problem that generalizes several of other network fortification problems and propose an exact algorithm for its solution. Numerical studies are performed using test instances from the literature. A graphical representation of the results is also proposed as a tool for analyzing the immunity of power grids under malicious attacks.

## 1. Introduction

The vulnerability and fortification analysis of power systems is an important research topic motivated by real-world power failure catastrophes, e.g., the huge blackout in the U.S.A. in August 2003 [1], and the September 2003 incident affecting more than 50 million people in the south of Switezrland and almost the entire Italy [2], just to cite a few.

Many such incidents are triggered by random isolated failures in grid components which cascaded into large scale disruptions, as also empirically observed [3]. This suggests that power grids may collapse as a result of random disruptions, for example those produced by a natural disaster. The mechanisms via which the disturbances propagate through the system, as well as the most prominent ways that have been used to tackle them, are summarized in [4].

Power grid disruptions can also be a consequence of malicious attacks (e.g., by terrorists), which is the focus of this paper. Malicious attacks are generally not random, and the goal of intelligent adversaries is to maximize the damage produced. Therefore, vulnerability assessments based on the random disruption assumption are not appropriate in this case. [5] remarks that planned attacks on grids can maximize impacts by exploiting the specific network structure. [6,7] analyze the topological aspects of the power system to show the malignant potential of such attacks. However, approaches relying only on topology to assess vulnerability are not sufficient for power grids, since important engineering design information like the capacity and reactance of the lines are not taken into account.

Attacks to the power system can propagate via fast electromagnetic transient phenomena that trigger protective equipment. Typically, this mechanism is a key driver of cascading blackouts and a crucial component to a malicious threat assessment. However, we focus on capturing the effects of equipment capacities and power angle constraints, not the threat of cascading failures - a goal achieved via the DC Power Flow approximation (DCPF). While this decision affects the realism of the model, it is still a significant improvement over the purely topological approach. Moreover, the choice of employing a static power flow based model allows us to obtain a good computational tractability even with an exponentially increasing number of attacks to the system, as show in Section 4. As a matter of fact, unlike many of the previous works that consider an upper threshold of attacked components [7,6,8,9], we remove this restriction thus the attacker is allowed to attack an arbitrary number of component simultaneously.

In this context, the vulnerability of power grids subject to malicious attacks can be conceptualized as a game where the attacker's goal is to maximize the system damage, while the defender seeks to minimize the consequences of such attacks when they occur, via available mitigation actions. Mathematically, this is formulated as a bilevel optimization problem (termed here as *disruption-mitigation* problem). If the mitigation problem has the structure of a linear programming model (and this is the case when employing the DCPF approximation), a complete single

* Corresponding author at: National University of Singapore and ETH Zurich, Future Resilient Systems, Singapore.
*E-mail addresses:* costa@lix.polytechnique.fr (A. Costa), dionysios.georgiadis@frs.ethz.ch (D. Georgiadis), isentsa@nus.edu.sg (T.S. Ng), melvynsim@nus.edu.sg (M. Sim).

https://doi.org/10.1016/j.ijepes.2018.01.020
Received 19 May 2017; Received in revised form 4 January 2018; Accepted 13 January 2018

level optimization problem can be derived and solved directly [10,11], as often done for network interdiction problems [12]. It is also possible to obtain a single level problem by replacing the inner optimization problem with its Karush-Kuhn-Tucker optimality conditions [13]. Other approaches involve decomposition schemes, like Benders decomposition and its variants [14,15]. In some cases, the mitigation problem may also involve integer variables, for example when line switching is considered. In practice, line switching allows the defender to disconnect additional lines after an attack as a defensive measure, with the purpose of exploiting the Braess' paradox [16,17]. The presence of binary variables in the inner problem prohibits the application of strong duality, hence specific algorithms have been designed [9,18]. A further step in the analysis of power grids under malicious attacks concerns the fortification of the grid to reduce its vulnerability. This yields a trilevel min−max−min (*fortification-disruption-mitigation*) model, that is clearly harder to solve than the bilevel problem in general. A heuristic algorithm has been introduced in [19] to address this type of problems. In [20], starting from the model presented in [10], a decomposition approach has been proposed. An implicit enumeration algorithm was then presented in [21] to improve the performance of [20], and [22] proposed a column-and-constraint generation algorithm for the same problem. In addition, a model based on a trilevel formulation including transmission expansion and line switching has been put forward in [23]. A common feature of many of these works is that the vulnerability is usually improved by making some components of the system impervious to attacks.

This paper studies a generalization of the aforementioned 'fortification-disruption-mitigation' problem, which can be described as a nested Stackelberg game of two players (the defender and the attacker). This type of game has been used to address various leader–follower problems on power grids, for example in the context of demand-response models involving utility company and users [24], or for vulnerability analysis of power grids based on the concept of susceptibility [25]. In our problem each player has a budget that is not known to one another, and the defender allocates his budget to harden selected transmission lines, forming a fortification plan that practically makes it more expensive for the attacker to destroy those lines. The attacker learns of this, and invests his budget in a disruption plan calculated to inflict maximum damage. The attack may result in load shedding, which the defender then tries to mitigate through optimal load balancing. Finally, because the defender does not know exactly the budget level of the attacker, i.e., the 'strength' of the attacker, he seeks a fortification plan that defends against all attacks capable of compromising the power grid in some sense (this is defined later), from *as strong an attacker as possible*. We say that the *attack immunity* of the grid system is that strength of the attacker that can be fended off. Our methodology consists of solving iteratively two optimization problems: the fortification problem, i.e., looking for a grid fortification plan which makes the attacks of the enemy as expensive as possible, and the attacker problem, i.e., finding new ways to attack the system given the fortification. The process stops when either there is no other feasible attack given the fortification plan, or no feasible fortification plan can be found. This approach results in the following contributions:

- Previous works assume that the defender can simply make transmission lines completely impervious to any attack - a very strong assumption as complete invulnerability is unlikely to be achieved in reality. In contrast, our fortification model is much more general and flexible, where the cost of destroying individual grid components can be controlled, hence permitting the modeling of a wide range of network fortification schemes in practice.[1]
- Our formulation allows the attacker to destroy any number of lines, as long as he has sufficient budget to do so. This is a generalization of previous works, that assume a fixed number of line removals. In this work the overall objective is to maximize the attacker's budget level required to compromise the power system, and hence we consider all possible attacks with a cost smaller than the defender's budget.[2]
- As a consequence of the above-mentioned attacker budget model in this work, our resulting two-stage optimization problem, although sharing some similarities to existing approaches such as in the area of robust optimization (e.g., [26]), contains non-trivial structural differences that introduces additional complications. This is further explained in Section 2.2. As a consequence, this requires a specialized solution approach, and is not simply a straightforward application of standard robust optimization methods.

Related to the first point above, we remark that a primary motivation of this work is to present an alternative to the binary fortification assumption that is prevalent in the literature. Thus, for clarity of exposition, additional constraints such as cascades, ramp rates, dynamic stability, voltage collapse, and unit commitment are out of scope and not considered in this paper.[3]

The rest of the paper is organized as follows. In Section 2, after introducing the notation, we develop the mathematical formulations of the 'fortification-disruption-mitigation' problem. Section 3 presents the algorithmic framework of the solution methodology. Some numerical studies are then performed using case instances in the literature, in Section 4. Finally, Section 5 concludes the paper.

## 2. The 'fortification-disruption-mitigation' model for power grids

### 2.1. Nomenclature

We introduce here the notation used in the rest of the paper. Notice that symbols in bold are used to represent vectors.

*Sets and symbols*

| | |
|---|---|
| $N$ | buses; |
| $J$ | generating units; |
| $J_n$ | generating units connected to bus $n \in N$; |
| $L$ | transmission lines; |
| $O(l)$ | origin bus for line $l \in L$; |
| $D(l)$ | destination bus for line $l \in L$; |
| $\delta_n^+$ | forward star of bus $n \in N$, i.e., the set $\{l \in L \mid O(l) = n\}$; |
| $\delta_n^-$ | backward star of bus $n \in N$, i.e., the set $\{l \in L \mid D(l) = n\}$; |
| $W$ | set of feasible fortifications; |
| $U(\Gamma, \boldsymbol{w})$ | set of feasible attacks. |

*Parameters [units]*

| | |
|---|---|
| $\overline{P}_l^f$ | power flow capacity of line $l \in L$ [MW]; |
| $\overline{P}_j^g$ | capacity of generating unit $j \in J$ [MW]; |
| $P_n^d$ | demand at bus $n \in N$ [MW]; |
| $x_l$ | reactance of line $l \in L$ [Ω]; |
| $\overline{\Delta P}$ | maximum load shed after worst-case attack [MW]; |
| $\varepsilon$ | percentage of maximum load shed permissible; |
| $F$ | fortification budget, set to 100; |
| $M$ | big-M constant for the linearization of $v_l \mu_l$. |

*Variables [units]*

[1] For example, instead of making a line invulnerable, the operator can invest gradually more in monitoring or structural integrity. This is a better analogy to the real world problem.

[2] Please note that going above that would be trivial as the attacker would be capable of destroying the entire network.

[3] That being said, some of these mechanisms can be introduced by expanding the list of constraints in the respective optimization problem.