Reliability Engineering and System Safety 165 (2017) 144–154

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Mitigating electric power system vulnerability to worst-case spatially localized attacks

Min Ouyang[a,b], Min Xu[a], Chi Zhang[c,*], Shitong Huang[a]

[a] School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China
[b] Key Lab. for Image Processing and Intelligent Control, Huazhong University of Science and Technology, Wuhan 430074, China
[c] Department of Industrial Engineering, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Keywords:
Power system
Vulnerability
Spatially localized attacks
Defender-attacker-defender
Tri-level optimization

ABSTRACT

This paper proposes an approach to mitigate power system vulnerability against worst-case spatially localized attacks (SLAs), which are defined as the failure of a set of system components, distributed in a spatially localized area, due to natural hazards or malicious attacks, while other components outside of the area do not directly fail. This problem is mathematically formulated as a tri-level defender-attacker-defender model, where the inner level optimizes the power dispatch to minimize system vulnerability (quantified as power demand drop), the middle level identifies the most disruptive spatially localized attack, and the outer level makes an optimal mitigation decision, including protecting vulnerable components and building new lines, to reduce the SLAs-induced vulnerability. This model is exactly solved by a proposed decomposition algorithm. Case studies on the IEEE 14 bus test system demonstrate the effectiveness and efficiency of the proposed approach.

1. Introduction

Modern society and its economy depend on critical infrastructures, such as electric power, water, gas and oil, and telecommunication systems. Among them, electric power systems are particularly critical, because most of the other infrastructures need electricity for their operation and management. However, contemporary power systems are subject to many types of hazards, such as extreme weather, natural hazards, terrorisms, component aging, human errors, animals and so on, which can cause severe and widespread societal and economic disruption, as demonstrated by 2.5 million customers experiencing power outage in the 1994 Northridge earthquake that struck Los Angeles, and 50 million customers affected in the 2003 North America blackout. Examples of these events call for better protection of power systems, which requires modeling their component fragilities under different types of hazards and then analyzing their vulnerability. Here, the term “vulnerability” has many different definitions [1,2], without a broadly accepted one.

This paper interprets that “vulnerability” is associated with a specific initiating event and the vulnerability of a system to a specific initiating event is quantified as its performance drop. Hence, defining the initiating event is the first step for vulnerability analysis. According to the types of the initiating events, the vulnerability studies on power systems in the literature can be grouped into three types. The first type is power system vulnerability analysis under random failures, which is a series of initiating events, such as equipment failures, downed limbs, animals, human errors and so on, with large variety and uncertainty. These failures can be modeled by randomly removing a certain fraction or number of system components [3–5]; or by assigning a failure probability to each component and then comparing this probability to an uniformly distributed random number within [0,1] to judge the component state [6–8]; or by first selecting the number of failed components according to a given distribution and then randomly removing a set of components with the selected number [9–11]. The second type is power system vulnerability analysis under natural hazards [12–15], such as earthquakes, hurricanes, floods and lightning. These hazards can cause system components distributed within an influence area to fail simultaneously. The impact of these natural hazards on system components are usually modeled according to fragility curves, which provide the probability of exceeding a certain damage state threshold conditional on a selected hazard intensity measure, such as peak ground acceleration or peak ground velocity or permanent ground deformation for seismic hazards [12–14], 3s gust wind speed for hurricane hazards [11–15].

The third is power system vulnerability studies under malicious attacks, where an attacker tries to maximally disrupt the system of concern by intentionally attacking some system components. Some scholars studied power system vulnerability by attacking components

[*] Corresponding author.
E-mail addresses: min.ouyang@hust.edu.cn (M. Ouyang), czhang@tsinghua.edu.cn (C. Zhang).

http://dx.doi.org/10.1016/j.ress.2017.03.031
Received 6 December 2016; Received in revised form 11 February 2017; Accepted 22 March 2017
Available online 23 March 2017

with the largest degree [16–18], betweenness [19,20], and load levels [16]. But the failure of local important components is not necessarily the worst-case disruption at the system level, so some other scholars studied power system vulnerability under the worst-case disruptions. This type of problems can be described as mixed integer programming problems. To solve this type of problems, Salmeron et al. proposed a heuristic algorithm to identify the worst-case attack scenarios; Bier et al. introduced a “Max Line” greedy method when only transmission lines can be attacked [38]; Salmeron et al. further proposed a global Benders decomposition for large scale power systems [22]; Motto et al. generalized Salmeron's model and formulated a Mixed Integer Linear Programming model for exact solution of the problem [23].

Note that system defender may also take defense measures before the malicious attacks, hence, many scholars studied the interactions between the defender and the attacker to identify the best defense strategy and the worst-case attack under the optimum defense [24–26]. A review of systems defense and attack models were conducted by Hausken and Levitin [39]. For those systems that the consequences of attacking a set of components can be determined in a straightforward manner, the interactions between the defender and the attacker are usually modeled by min-max approaches [40], where the inner level describes how the attacker maximizes the worst-case damage or the expected damage under all possible attack strategies, and the outer level describes how the defender minimizes the damage. But for electric power systems, the defender can also manipulate component flow after any attacks to minimize system damage. The interactions between the attacker and the defender for power systems are usually modelled by min-max-min approaches [24–26], where the outer level describes how the defender takes the defense measures, the middle level simulates how the attacker disrupts the systems and the inner level describes how the defender manipulates component flow to minimize system damage.

Actually, the above mentioned studies and many other studies on malicious attacks, such as those by Hausken and Levitin [40], and Levitin et al. [41], should belong to the non-proximity-based attacks, where the geographical coordinates of the attacked components are not considered. In reality, there also exists another type of malicious attacks, belonging to proximity-based attacks and called spatially localized attacks (SLAs), which are defined as the hazards that can cause direct damage or interruption of system components distributed over a localized area, and other components outside the area do not fail directly. For example, on September 11, 2001, the New York terrorist attack caused the full collapse of the WTC1 and the WTC2, and the debris caused the damage of some neighboring buildings. These damaged buildings further caused the damage of many power system components within 0.21 km from the attack center. On August 12, 2015, the Tianjin chemical explosion event caused the damage or interruption of many power system components located within 1 km from the attack center. For these spatially localized attacks, they need to be modeled by considering all system components’ geographical coordinates. Berezin et al. [27] and Nicholson et al. [28] modeled the localized area by a circle shaped area with a random attack center to analyze network vulnerability, but these modeling approaches cannot identify the worst-case attack. Patterson and Apostolakis modeled the localized areas by dividing the system map into a generic hexagonal grid with a small radius and each hexagon was a localized area [29]. Johansson and Hassel [30] made a similar analysis by dividing the system region into a square grid and each square was a localized area. These studies enable identifying the worst-case attack, but the results depend on how the system map is partitioned into small localized areas. Ouyang et al. modeled the localized areas by circle shaped area and then proposed an algorithm to identify the worst-case attack [31,32], but these works do not study the mitigation strategies.

Based on the above literature review, this paper investigates the vulnerability mitigation of electric power systems under spatially localized attacks. From the above example events, it can be found that the SLAs can be triggered in various ways and some of which may be unexpected and cannot be identified until they occur. Hence, different from many existing studies in the literature that adopt probabilistic frameworks to model the actions and outcomes of the attacker and defender [40,42,43], where the defender minimizes the maximal expected damage that an attacker can inflict, this paper uses the worst-scenario approach and the defender minimizes the damage given that the attacker selects the worst-case attack. The main contribution of this research lies in two-fold. Firstly, a tri-level decision-making model is formulated to determine the defense strategy that can minimize power system vulnerability under the worst-case SLA. Secondly, a decomposition algorithm is proposed to identify the optimal defense and the associated worst-case SLA. The rest of the paper is organized as follows: Section 2 introduces the mathematical model. Section 3 provides the solution algorithm and Section 4 applies the proposed method to the IEEE 14 test system. Section 5 gives conclusions and future work.

2. Problem formulation

This paper interprets that vulnerability is associated with a specific initiating event and the system vulnerability to a specific event is quantified as its performance loss. Mitigating power system vulnerability to spatially localized attacks needs to introduce a virtual attacker and a defender. The attacker seeks the most disruptive strategy to attack the system, and the defender can take ex-ante (i.e., protect vulnerable components, build new lines) and ex-post actions (i.e., re-dispatch power flow), to minimize the performance loss. The interactions between the attacker and the defender lead to a tri-level defender-attacker-defender model. In this model, the inner level optimizes the power dispatch to minimize the performance loss, the middle level identifies the most disruptive spatially localized attack on power systems, and the outer level makes an optimal mitigation decision. Before presenting the mathematical formulation, some assumptions and simplifications are stated as follows:

(1) This paper models a power system by a network $G(\boldsymbol{B}, \boldsymbol{L})$, described by a collection of buses $\boldsymbol{B}$ and transmission lines $\boldsymbol{L}$ connecting the buses. Note that some bus may contain multiple generating units, which can be considered to be destroyed all together once the bus is destroyed by a spatially localized attack, since these units are usually deployed nearby the bus. Thus, these generating units are not separately modeled and are all together regarded as a single generator bus, which can produce electricity. To model spatially localized attacks on a power system, the system geographical layout information is required for analysis. For buses, their locations can be described by *xy*-coordinates for systems embedded in two-dimensional plate or latitude and longitude for systems embedded in earth surface; for power lines, they are assumed to be straight lines between two adjacent buses. This may not be true in practice for some lines. In this case, the line can be divided into a series of short segments, and each of them is a straight line. Then the proposed approach can still work.

In the power network, this paper approximates active power flows with a DC optimal power flow model (shortened as DC-OPF) [21,44–46], which neglects reactive power effects and nonlinear losses and is normally acceptable in the context of long-term, “coarse-grained” security analysis [21,44]. Also, the DC power flow model is a commonly adopted simplification in power network planning [45,46]. In the DC-OPF model, associated with each bus $i \in B$ are P_i^{Gen} and P_i^{Load} representing its power supply and demand. $\hat{P}_i^{Gen}$ is the maximum output and $\hat{P}_i^{Load}$ is the required demand for the bus i. If $\hat{P}_i^{Gen}$>0 and $\hat{P}_i^{Load}$=0, bus i is a source or generator node; if $\hat{P}_i^{Gen}$=0 and $\hat{P}_i^{Load}$=0, bus i is a transshipment node; if $\hat{P}_i^{Gen}$=0 and $\hat{P}_i^{Load}$>0, bus i is a demand or load node; if $\hat{P}_i^{Gen}$>0 and $\hat{P}_i^{Load}$>0, bus i is both generator and load node.