Electrical Power and Energy Systems 82 (2016) 29–36

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A game theory approach to vulnerability analysis: Integrating power flows with topological analysis

Maggie X. Cheng [a,*], Mariesa Crow [b], Quanmin Ye [c]

[a] Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65409, United States
[b] Department of Electrical and Computer Engineering at Missouri University of Science and Technology, Rolla, MO 65409, United States
[c] Nokia Networks, Mountain View, CA 94043, United States

ARTICLE INFO

Article history:
Received 10 July 2014
Received in revised form 24 December 2015
Accepted 25 February 2016
Available online 17 March 2016

Keywords:
Vulnerability analysis
Topological analysis
Power flow
Instability
Game theory
Linear programming

ABSTRACT

This paper presents a new framework for vulnerability analysis. Under this framework, we can identify the vulnerable components and the critical components of a power grid. Distinct from previous work, our model considers the interaction between the components of the power system, and models the dynamic evolving process of cascading failures. The impact of a component failure on the system is dynamically changing as the failure propagates. We analyze the vulnerability of a power grid using an optimization model based on game theory, and use linear programming method to solve it. Since instability is the reason of power outage, we use an instability index to measure the negative impact to the system. The results from this optimization problem suggest which component of the system is critical since its failure can most negatively impact the cyber-physical system.

Introduction

The electrical power grid nowadays is well connected. As the grid connectivity increases, we will have fewer power outages since the high demand in one region can be satisfied by not only the local generation, but also remote generation from other regions. However, connectivity is a double-edged sword—multiple independent small-scale power outages may be mitigated, fewer but larger-scale power outage is more likely to happen. Large-scale power outage is typically the consequence of cascading failures propagated through a power system. To avoid cascading failure, it is important to identify the critical points or critical lines in the power system and protect them from failure. As the physical system is coupled with the cyber system, additional threats are introduced. Our job is not only to protect the grid from natural failure but also adversarial attacks. This is the scope of vulnerability analysis.

To take preventive action against potential attacks, it is important to identify the vulnerability as early as possible so that grid operator can enhance the security and robustness of those identified components. In this paper, we present an analytical framework to identify the security holes of a power grid. It is analytical in the sense it identifies the most vulnerable and the most critical components of the system without deliberately probing the system to discover its weaknesses. Previous work on power grid vulnerability analysis is mainly on the SCADA system [1,2], and/or based on attack graphs or attack trees ([3,4], etc.). The proposed method uses a different approach for network vulnerability analysis and can be extended beyond the SCADA system to consider the control and monitoring devices and communication links in a smart grid.

To show the cascading failure propagation in a power grid, we study a simple six-bus three-machine system in Fig. 1. Suppose instantaneous high load at bus 2 causes power oscillation at bus 2. If transient instability cannot be dampened timely and it may cause power outage in this area. This "fault" may be propagated to bus 3 and the extra load may also cause system instability in that area. If the instability is high and it can continue to increase the power flow in more lines and faults may propagate through the whole power grid and cause large-scale power outage. The more the power grid is connected, the more vulnerable it is. An isolated area can only have small scale power outage, but will have it more often; a highly connected power grid will have fewer but larger power outage.

To identify the component that is prone to failure is important since failure of one component may cause chain reaction of more

* Corresponding author.
E-mail addresses: chengm@mst.edu (M.X. Cheng), crow@mst.edu (M. Crow), quanmin.1.ye@nsn.com (Q. Ye).

http://dx.doi.org/10.1016/j.ijepes.2016.02.045
0142-0615/

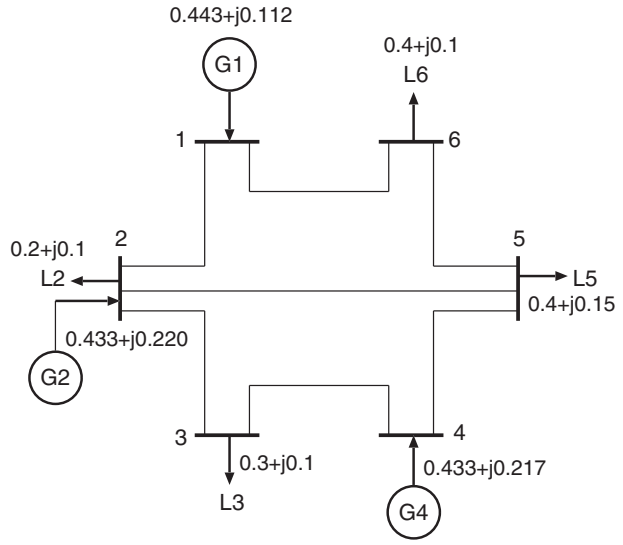

Fig. 1. A six-bus three-machine system.

components, and therefore the robustness or reliability of the vulnerable component should be improved. On the other hand, to identify the component whose failure can cause the largest degree of damage to the system is also very important in a security context since the hacker would target at such components to attack. The identification of the vulnerable components and the critical components help the grid operator in long term planning. The operator can reconfigure the generators, power lines or enhance security protection of some components to keep the grid in a reliable and secure state.

A purely topological approach that is based on the metrics of network connectivity alone will not do a satisfactory job in power grid vulnerability analysis [5–8]. The reason is that power flow dynamics is not considered, and the interaction between different components of the system is not considered. The cascading propagation of failure cannot be captured in such a model. Due to the heterogeneity in load distribution and source capacity, a more sophisticated method is needed than the purely topological approach.

Bompard et al. [9] extended the purely topological approaches to consider the real power flow allocation and line flow limits in transmission grids, and introduced a new metrics called "net-ability"—the ability of the transmission grid to function properly under normal operating conditions. In [9] critical components are identified according to the relative drop in net-ability caused by the failure of each component. As we will show later, the method in [9] is what we called "Static Analysis" in this paper by using a different metrics from our work.

The key idea of this paper that distinguishes itself from previous work is to consider the evolving process of system instability after component failure. System vulnerability is quantified in terms of the cost to the power system, which is related to system instability. When system instability is low, power oscillation caused by load disturbance can be quickly stabilized and no further damage will occur; when system instability is high, power oscillation cannot be dampened timely, so it may cause the tripping of a power line. The tripping of a power line will cause power oscillation in other areas so the chain reaction will continue.

The scope of this paper does not include the countermeasures of potential attacks; it only identifies the vulnerable components and the critical components. It is up to the grid operator to decide what to do with the result of vulnerability analysis. Countermeasure or protection is the next step after vulnerability analysis.

Graph model

We can use a multi-source multi-sink flow network to represent a power grid as follows: source nodes represent generators, denoted by set G; sink nodes represent loads, denoted by set L; and intermediate nodes represent buses, denoted by set B. Directed edges are added from generators to buses and from buses to loads; bidirectional edges are added between buses to represent the physical connectivity among them. Let E be the set of bidirectional edges connecting buses. A directed edge from a generator to a bus or from a bus to a load has no capacity limit, and therefore the edge has capacity set to ∞. Such edges are not subject to failure. A bidirectional edge between two buses represents the power line with a capacity limit, and therefore we set the edge capacity $c(i,j) = T^*_{ij}$ in both directions, $\forall (i,j) \in E$. If the power flow $S_{i,j}$ exceeds T^*_{ij}, the line will trip off.

The graph model for the example in Fig. 1 is shown in Fig. 2.

If the subgraph induced by the bus nodes is fully connected (i.e., there is a path from every node to every other nodes), then every source node has a connected path to every sink node. When there are multiple sources available, a load may be satisfied by drawing power from multiple sources. Intuitively, every sink node would draw power from its *nearest* (in terms of impedance) source node. If the nearest source cannot satisfy its demand, then the second nearest, and so on. This is because the nearest source has the lowest impedance on the power line; it is also because if there is increase in demand, the power supply can ramp up quickly if it is near the sink node so that the power oscillation can be quickly stabilized.

To compute the power flow on power lines with given load condition, we can formulate the problem as a flow network problem. When computing the power flow, we ignore the capacity constraint since the real power flow does not change its path because of the capacity limit of the power line. The problem can be cast as an optimization problem with the constraints that (1) flow conservation is satisfied, (2) the total load demand is satisfied, and (3) the AC version of Ohm's Law is approximately satisfied.

Let $f(i,j)$ denote the power flow from bus i to bus j, θ_i denote the phase on bus i, $X_{i,j}$ the reactance of the power line between bus i and bus j. We define the cost of a power line as the absolute error of the power flow solution:

$$cost(i,j) = |\theta_i - \theta_j - X_{i,j} f(i,j)|, \quad \forall (i,j) \in E$$

Then the optimization problem is to find a power flow solution that minimizes the total cost. X_{ij} is given as input; θ and $f(i,j)$ are variables whose values will be solved from the linear program.

Let N_v denote the neighbors of node v connected by undirected edges, N^-_v denote the neighbors of v connected by out-edges of v, and N^+_v denote the neighbors of v connected by in-edges of v. For a power system with n generators (sources) and m loads (sinks), the linear program is given as follows:

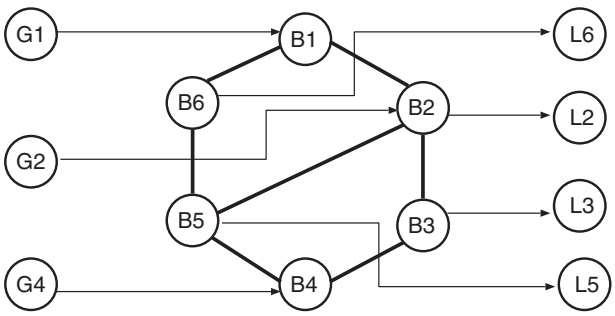

Fig. 2. The flow network model for the system in Fig. 1.