Reliability Engineering and System Safety 147 (2016) 1–8

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Modeling cascading failures in interdependent infrastructures under terrorist attacks

Baichao Wu [a,b,*], Aiping Tang [a], Jie Wu [c]

[a] School of Civil Engineering, Harbin Institute of Technology, 73 Huanghe Road, Harbin 150001, PR China
[b] School of Civil Engineering, Northeast Forestry University, 26 Hexing Road, Harbin 150040, PR China
[c] College of Environmental and Chemical Engineering, Heilongjiang University of Science and Technology, 2468, Puyuan Road, Harbin 150022, PR China

ARTICLE INFO

Article history:
Received 19 May 2015
Received in revised form
7 October 2015
Accepted 12 October 2015
Available online 10 November 2015

Keywords:
Cascading failure
Critical infrastructures
Infrastructure vulnerability
Interdependencies
Terrorist attacks

ABSTRACT

An attack strength degradation model has been introduced to further capture the interdependencies among infrastructures and model cascading failures across infrastructures when terrorist attacks occur. A medium-sized energy system including oil network and power network is selected for exploring the vulnerabilities from independent networks to interdependent networks, considering the structural vulnerability and the functional vulnerability. Two types of interdependencies among critical infrastructures are involved in this paper: physical interdependencies and geographical interdependencies, shown by tunable parameters based on the probabilities of failures of nodes in the networks. In this paper, a tolerance parameter α is used to evaluation of the overloads of the substations based on power flow redistribution in power transmission systems under the attack. The results of simulation show that the independent networks or interdependent networks will be collapsed when only a small fraction of nodes are attacked under the attack strength degradation model, especially for the interdependent networks. The methodology introduced in this paper with physical interdependencies and geographical interdependencies involved in can be applied to analyze the vulnerability of the interdependent infrastructures further, and provides the insights of vulnerability of interdependent infrastructures to mitigation actions for critical infrastructure protections.

1. Instruction

With the advancement information technology, modern critical infrastructure systems are increasingly coupled and mutually depend on each other to provide essential functionality for social stabilization and economic prosperity. Most of these infrastructure systems are networked in nature and interdependent in complex ways, which means that failure of nodes in one network may lead to failure of dependent nodes in other networks, and the procedure may occur recursively, resulting in a cascade of failures of infrastructure systems. Cascading failures of critical infrastructure systems caused by recent disasters, ranging from large-scale power outages, to terrorist attacks, hurricanes and earthquakes, have exhibited highly vulnerabilities existing in interdependencies across critical infrastructure systems. Examples of significant cascading failures are the Northeast American power blackout in 2003 [1] and the terrorist attacks on the US in 2001.

In the past few years, many researchers have paid much attention to the problem of interdependencies existing in critical infrastructure systems. Several frameworks and methods for characterizing and analyzing interdependencies among critical infrastructures have been suggested. One of the most cited frameworks proposed by Rinaldi et al. identified four categories of critical infrastructure interdependencies: (1) geographical; (2) physical; (3) cyber; and (4) logical [2]. Many efforts are currently being devoted to developing models or methods attempting to capture the interdependencies among critical infrastructures. An over view of methods and models are summarized in some literatures [3–6]. Those methods are divided into two coarse categories – the empirical approaches and the predictive approaches [7]. Empirical approaches aim at studying past events in order to increase our understanding of infrastructure dependencies [8], and predictive approaches include Leontief input–output model [9–17], agent based model [18–23], system dynamics model [24] network based model [7,25–38], and others [39–49]. Although the existing methods and models based on different viewpoints have their own merits and drawbacks discussed and summarized in some literatures [5,37], they are necessary in order

[*] Corresponding author at: School of Civil Engineering, Harbin Institute of Technology, 73 Huanghe Road, Harbin 150001, PR China. Tel.: +86 18045117728.
E-mail address: wubaichao@126.com (B. Wu).

http://dx.doi.org/10.1016/j.ress.2015.10.019
0951-8320/© 2015 Elsevier Ltd. All rights reserved.

to appropriately and comprehensively address the issue of interdependencies, meaning there is no universal, all-encompassing model, which is supported by some literatures [7,40]. However some progresses have been made in modeling interdependencies among infrastructures, the challenges for modeling and understanding of interdependencies among infrastructures are immense, and the current efforts in this field are still in an early stage.

The terrorist attacks on critical infrastructures is one of the hot issues of modeling interdependencies among infrastructures, there are a few literatures attempting to capture the interdependencies based on a strategy of removing most connected node or most betweenness node or most flow edge [7,29,31,37,50]. Although the topology properties along with function properties of infrastructures and physical interdependencies among infrastructures are concerned by the previous studies, nearly all of them did not propose proper models or methods to model the geographical interdependencies among infrastructures which must be considered under terrorist attacks with specified site coordinates and specified affected ranges. There are a few literatures concerning about the geographical interdependencies among infrastructures and some meaningful frameworks are proposed [51,52]. The framework of Ref. [51] employs Monte Carlo network analysis and geographic analysis methods under a grid size to identification of critical locations across multiple infrastructures, while physical interdependencies among infrastructures have not been included which will underestimate the vulnerabilities of the coupled infrastructures. The method of Ref. [52] considers geographically localized attacks from the perspective of percolation theory and the results of the method demonstrates the potential high risk of localized attacks on spatially embedded network systems when dependencies considered, while the physical roles of nodes in individual infrastructure have not concerned, and within the range of each attack all nodes will be removed from the network which is not actual in terrorist attacks or explosions of dangerous chemicals.

To solve those problems mentioned above, a new attack model is introduced in this paper to further explore the vulnerabilities of critical infrastructures, especially when interdependencies are concerned.

This paper proposed an attack strength degradation model to model terrorist attacks, and the model not only considers the topology properties and function properties of critical infrastructures, but also includes the physical interdependencies and geographical interdependencies among critical infrastructures; a medium-sized energy system including oil network and power network is selected, the topologies of the two networks are extracted based on graph theory, and the roles or functions of different nodes of the extracted networks are also considered. To model the interdependencies between the oil network and the power network, geographical proximity is employed to establish the physical interdependencies defined by conditional probabilities of failure between the two networks before an attack, while the geographical interdependencies among critical infrastructures are provided after an attack by failure probabilities based on distance to disturbance center. Under the attack model, the vulnerabilities of the two networks are investigated under different coupling strengths among networks.

This paper is divided into five main sections. The second section introduces fundamental concepts and definitions from graph theory, as well as the definitions of the parameters used to characterize structural and functional vulnerabilities of the two networks. The third section defines the attack strength degradation model and introduces the basic topologies of the two networks. The fourth section provides the results of the two networks responses under different coupling strengths among them, and the results under different strength of interdependencies are also discussed. Finally, the last section presents the main conclusions of this study and future works are proposed.

2. Definitions for evaluations the vulnerabilities of infrastructure systems

Infrastructure systems can be modeled as a directed graph $G=(V,E)$ where V is the set of vertices $V(G)$ that represent all the individuals and E is the set of edges $E(G)$ that represent all the physical and dependency connections. The number of vertices in $V(G)$ is termed the order N of the graph or $|G|$, and the number of edges in $E|G|$ is termed its size M or $||G||$ [53]. The *vertex degree*, $d(v)$, of a vertex $vV(G)$, is defined as the number of incoming and outgoing edges connected to the vertex v. Vertex betweenness, $b(v)$, of a vertex $v \in V(G)$, is defined as the total number of shortest paths between all pairs of vertices $(i, j\ ) \in V(G)$ that pass through the vertex v, which is not an end for any path. The $d(v)$ or $b(v)$ of the network can be used for evaluation importance of a vertex of G when different removed strategy imposed.

The vulnerabilities of infrastructure networks can be learned from the decline of service rates after disturbances compared to the initial ones. Some network characteristics used in this study will be given in the next.

2.1. Service rate based on topology

The service level of an infrastructure network can be analyzed by the sum of edges based on topology of the network simply. For comparison with the initial service level, the poster service level of the network after a disturbance, the service rate based on topology, SR_t, is defined as follows:

$$SR_t = \frac{||G||_{poster}}{||G||_{initial}} \tag{1}$$

where the poster means after the disturbance, and initial means before the disturbance, obviously, $0 \le SR_t \le 1$.

2.2. Service rate based on flow

The SR_t can be used for the evaluation of vulnerability of the infrastructure network, while not detecting the differences based on the actual functions or roles of the nodes in the network. For instance, the functions or roles of the nodes in power network or oil network can be classified as generation, distribution and transmission, which must be considered in the evaluation of the vulnerabilities of the infrastructure networks. To solve the problem mentioned above, the service rate based on flow, SR_f, is defined as follows:

$$SR_f = \frac{\sum ||clusters_i^G||_{poster}}{\sum ||clusters_j^G||_{initial}} \tag{2}$$

where the $clusters_i^G$ is the ith connected subgraph of G and includes at least one generation node and one distribution node. Obviously, $0 \le SR_f \le 1$.

2.3. Service rate based on network efficency

To compare the results of vulnerabilities based on the SR_t and SR_f, the network efficiency [54], E, the mean of inverse path length, is given in this paper. Service rate based on E, SR_E, is defined as follows:

$$E = \frac{1}{N(N-1)} \sum_{i,j \in V, i \ne j} \frac{1}{d_{ij}}$$

$$SR_E = \frac{E_{poster}}{E_{initial}} \tag{3}$$

where N is the order of G, d_{ij} is the shortest path from vertice i to vertice j, $0 \le SR_E \le 1$.