J Syst Sci Syst Eng (March 2016) 25(1): 102-118 ISSN: 1004-3756 (Paper) 1861-9576 (Online)
DOI: 10.1007/s11518-016-5295-3 CN11-2983/N

MODELING AND SIMULATION OF THE VULNERABILITY OF INTERDEPENDENT POWER-WATER INFRASTRUCTURE NETWORKS TO CASCADING FAILURES

Yanlu Zhang[1] Naiding Yang[1] Upmanu Lall[2]

[1]*School of Management, Northwestern Polytechnical University, Xi'an, 710072, China*

zhangyanlu@nwpu.edu.cn (✉), *naidingy@nwpu.edu.cn*

[2]*Columbia Water Center & Department of Earth and Environmental Engineering, Columbia University, New York, NY 10027, USA*

ula2@ columbia.edu

Abstract

Critical infrastructures are becoming increasingly interdependent and vulnerable to cascading failures. Existing studies have analyzed the vulnerability of interdependent networks to cascading failures from the static perspective of network topology structure. This paper develops a more realistic cascading failures model that considers the dynamic redistribution of load in power network to explore the vulnerability of interdependent power-water networks. In this model, the critical tolerance threshold is originally proposed to indicate the vulnerability of network to cascading failures. In addition, some key parameters that are important to network vulnerability are identified and quantified through numerical simulation. Results show that cascading failures can be prevented when the values of tolerance parameter are above a critical tolerance threshold. Otherwise interdependent networks collapse after attacking a critical fraction of power nodes. Interdependent networks become more vulnerable with the increase in interdependence strength, which implies the importance of protecting those interconnected nodes to reduce the consequences of cascading failures. Interdependent networks are most vulnerable under high-load attack, which shows the significance of protecting high-load nodes.

Keywords: Interdependent infrastructure networks, vulnerability, cascading failures, complex network, numerical simulation

1. Introduction

Critical infrastructures, such as electric power grids, natural gas pipelines, water distribution networks, transportation networks, and Internet communication networks, play a fundamental role in providing essential services to the society (de Bruijne and van Eeten 2007). However, such infrastructures are becoming more and more vulnerable to some disturbances (e.g., earthquake, severe weather, terrorist attacks or components deterioration) because of their increasing interdependences (Rinaldi et al.

2001, Eusgeld et al. 2011). The failures of a small fraction of nodes in one network may spread within the whole network and then propagate to another dependent network. This recursive process is called cascading failure, which leads to a breakdown of interdependent networks and cause severe consequences to the society (Little 2002, Buldyrev et al. 2010). In this context, it is necessary to explore the vulnerability of interdependent infrastructure networks to cascading failures.

Electric power and water distribution networks are typical examples of interdependent infrastructure networks (Bagchi et al. 2010). Their interdependences are illustrated by the fact that pump stations, control units, and storage tanks in water network depend directly on substations in the power network to function well. One example of cascading failures in interdependent networks is the power blackout that happened in many parts of the eastern USA on 14th August 2003. The blackout subsequently caused a shortage of water supply and affected other critical infrastructures. Another example is the power blackout resulting from Hurricane Sandy in 2012, which led to a loss of water supply in New York City. These examples motivate a study on the vulnerability of interdependent power-water networks to cascading failures.

So far, current models and methods for analyzing the vulnerability of interdependent infrastructure networks can be divided into two categories: empirical approach (Restrepo et al. 2006, Zimmerman and Restrepo 2006, Chang et al. 2007, McDaniels et al. 2007) and predictive approach (Ouyang et al. 2009, Buldyrev et al. 2010, Parshani et al. 2010, Johansson and Hassel 2010, Huang et al. 2011). The empirical approach is a kind of method that is using past real cases or collecting data through questionnaire survey to explore general rules and verify hypothesis of the vulnerability of interdependent networks to cascading failures. The predictive approach is another kind of method that is building models after extracting some significant parameters that can reflect real cascading failures phenomena in interdependent networks to explore rules of the vulnerability of interdependent networks to cascading failures through simulation. McDaniels et al. (2007) pointed out that empirical approaches can provide important information regarding the vulnerability of general interdependent infrastructures to make policies and decisions. Predictive approaches can provide important information to facilitate the proactive risk management of specific interdependent infrastructure networks. This paper considers the predictive approaches. Ouyang et al. (2009) introduced a methodological approach to analyze the structural and functional vulnerabilities of an artificial interdependent electric power network and gas pipeline network. Buldyrev et al. (2010) proposed a theoretical framework to study cascading failures in interdependent networks under random attack, and found that the failure of a small fraction of nodes can result in complete fragmentation of all the networks, while a significant number of nodes must be randomly removed before degradation of a single network. But Buldyrev et al. (2010) assumed that each node in one network is interconnected to one node in the other network by establishing one-to-one bidirectional links, which is not always the case

in the real world. Parshani et al. (2010) then studied the vulnerability of partially interdependent networks under random attack, and found that reducing interdependence improves the robustness of networks against random attack. Johansson and Hassel (2010) studied the vulnerability of interdependent technical infrastructure networks and the functional and geographic interdependences among them. Huang et al. (2011) studied the vulnerability of interdependent networks under intentional attack on high-degree and low-degree nodes, and found that interdependent scale-free networks are still significantly vulnerable even if high-degree nodes are protected and have a low probability of failure.

However, the studies mentioned above do not consider the dynamic load redistribution of nodes within a power network when modeling the cascading failures of interdependent infrastructure networks. In fact, overload of node is one of key factors that trigger cascading failures in many real-world networks, especially in electric power networks. Each node in power network has its own maximum capacity. When the load of a power node exceeds its capacity, this node will malfunction and its load will be distributed to neighboring operating nodes, which will trigger cascading failures within the power network. Such cascading failures may then propagate to the dependent water network through the interdependences and potentially cause the water network to break down. Therefore, this study will introduce the dynamic redistribution of load in power network, and then establish a realistic model of cascading failures in interdependent power-water networks to better explore the vulnerability of interdependent networks to cascading failures.

2. Generation of Interdependent Power-water Networks

Prior to modeling cascading failures, the first step is to generate interdependent power-water networks (i.e., what is described as node and what is described as edge). Since most infrastructure networks usually have different owners, data are not easily available (Johansson and Hassel 2010). Terrorist attacks over the last decade have also resulted in various governments treating all information regarding a city's infrastructure layout as classified (Bagchi et al. 2010). Therefore, we will generate fictional interdependent power-water networks.

2.1 Generation of Individual Networks

For simplicity, we hypothesize that the electric power network and the water distribution network are unweighted and undirected graphs respectively. Let $G_A(V_A, E_A)$ denote the electric power network and $G_B(V_B, E_B)$ denote the water distribution network, where $V_A = \{1, 2, \cdots, N_A\}$ is the set of all power nodes and $V_B = \{1, 2, \cdots, N_B\}$ is the set of all water nodes. Two types of nodes are considered for the two networks, namely source nodes (i.e., supply nodes) and demand nodes (i.e., sink nodes). For the electric power network, we take generators that produce power as source nodes, substations that deliver power to users or other systems as demand nodes, and electric wires as edges. For the water distribution network, we take pumps that supply water as source nodes, storage tanks that deliver water to users or other systems as demand nodes, and water pipelines as edges according to the assumptions made by Hwang et

al. (1998) and Dueñas-Osorio et al. (2007).

Afterwards, we assume that the two networks are generated based on the spatial proximity of nodes in the same two-dimensional area. This assumption causes the two networks to show the remarkable properties of a small-world network during the growth (Watts and Strogatz 1998). Furthermore, the two networks are assumed to have the same generation algorithm, which is given as follows:

(1) Initially, the network starts with N_1 isolated and randomly distributed source nodes. Their coordinates are N_1 pairs of independent random numbers within the interval [0, 1], i.e., $< x_1, y_1 >, < x_2, y_2 >, \cdots, < x_{N_1}, y_{N_1} >$.

(2) Next, a new node i with a randomly distributed coordinate $< x_i, y_i >$ $(i = N_1 + 1, N_1 + 2, \cdots, N)$ is connected to m existing nodes in the network at each time step. Here, the probability Π_{ij} that a new node i links to an existing node j is given as follows (Xu et al. 2007, Ouyang et al. 2009):

$$\Pi_{ij} \sim k_j^{\lambda} / D_{ij}^{\mu}, \quad i = N_1 + 1, N_1 + 2, \cdots, N, \qquad (1)$$

where k_j is the degree of node j (i.e., the number of links directly connected to node j); D_{ij} is the Euclidean distance between node i and j (i.e., $D_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$); λ ($\lambda \geq 0$) and μ ($\mu \geq 0$) are the respective parameters governing the preferential attachment and the cost of distance between nodes. Obviously, a high value of λ will favor linking to nodes with high degrees, whereas increasing the value of μ will discourage longer distance. Based on the assumption above, we set λ=0 to exclude the influence of preferential attachment, and set $\mu = \infty$ to make sure a new node is linked to the geographically nearest existing nodes.

(3) After N-N_1 time steps, a network with N nodes is finally generated.

2.2 Building the Interdependences across Two Networks

So far, several methods and frameworks to identify and characterize different kinds of interdependences among infrastructure networks have been proposed (Rinaldi et al. 2001, Restrepo et al. 2006, Zimmerman and Restrepo 2006, Lee et al. 2007, McDaniels et al. 2007, Johansson and Hassel 2010). Rinaldi et al. (2001) proposed a framework where interdependences are classified into physical (an output from a system is an input to another system), cyber (the state of a system is dependent on information transmitted through an information infrastructure), geographic (two or more geographically proximate systems are affected by the same local event) and logical dependency (all other types of interdependences, for example, related to human behavior). Lee et al. (2007) then proposed five types of relationships among infrastructures: input dependence, mutual dependence, shared dependence, exclusive-or dependence and co-located dependence.

For interdependent power-water networks, we assume that each pump in the water network depends on the geographically nearest substation in the power network to supply and deliver water to storage tanks, and each storage tank in the water network depends on the geographically nearest substation to deliver water to the ultimate users. Interdependences across the two networks are modeled with the dependence matrix $I_{A \to B} = [I_{ij}]_{N_A \times N_B}$, which describes the directional relationships from

specific nodes in power network G_A to the dependent nodes in water network G_B. The dependence matrix $I_{A\to B}$ is expressed as follows:

$$I_{A\to B}: I_{ij} = \begin{cases} 1, \text{ if node } j(j \in V_B) \text{ is dependent,} \\ \quad \text{on node } i(i \in V_{A_2}), \\ 0, \text{ otherwise,} \end{cases} \quad (2)$$

where V_B is the set of all nodes in the water network, and V_{A2} is the set of all substations in the power network. Clearly, the matrix $I_{A\to B}$ can provide a brief representation of physical coupling between the two networks. However, the opposite dependence matrix $I_{B\to A}$ may not be valid because of real topological and operational factors (Wu and Dueñas-Osorio 2013). For example, a pump may depend heavily on the local substation for power, whereas this substation may not rely on this pump for cooling, but rather on the local river.

3. Modeling Cascading Failures in Interdependent Networks

On the basis of the interdependences across power and water network, we assume that cascading failures in interdependent power-water networks originate from an attack on some power nodes. Then, the failures of these attacked power nodes can spread within the power network and potentially cause other substations to malfunction. Subsequently, the failures of some substations will lead to a malfunction of the dependent water nodes (pumps or storage tanks) through the interdependences, which may further cause other water nodes to malfunction. Therefore, the cascading failures in interdependent power-water networks will be modeled to describe how failures spread within the power network and then propagate to the dependent water network.

The first step is to model how cascading failures spread within the power network. For the electric power network, each node carries a dynamic power load when functioning, and each power node has its own maximum load that it can handle. When the load of some node exceeds its own maximum load that it can handle, this node will malfunction because of overload. First, we assume that the initial load of each power node is the number of shortest paths that pass through this node (Goh et al. 2001; Newman 2001). Therefore, the initial load $L_k(0)$ of node $k\,(k = 1, 2, \cdots, N_A)$ at time 0 is given by the following equation:

$$L_k(0) = \sum_{i\neq j} L_k^{(i,j)}(0), \quad k = 1, 2, \cdots, N_A, \quad (3)$$

where $L_k^{(i,j)}(0)$ is a Boolean variable that indicates whether the shortest path connecting nodes i and j passes through node k or not at time 0. If $L_k^{(i,j)}(0)$ =1, the shortest path connecting nodes i and j passes through node k at time 0, or not if $L_k^{(i,j)}(0)$=0.

The maximum load that a node can handle is called the capacity of this node. For real electric power network, the capacity of a node is severely limited by cost. Thus, it is natural to assume that the capacity of a node is proportional to its initial load. Therefore, the capacity C_k of node k is assumed to be linearly proportional to its initial load, which is also justified by Motter and Lai (2002), Kinney et al. (2005), Wang and Rong (2009), Lan et al. (2012), Jia et al. (2014). Therefore, C_k is given as follows:

$$C_k = (1+\beta)L_k(0), \quad k = 1,2,\cdots,N_A, \qquad (4)$$

where $\beta(\beta \geq 0)$ is a tunable variable called the tolerance parameter of network. As we can see, the capacity of each node is not infinite owning to the high correlation between β and the limited cost invested into the network. Investing excessive cost into the whole network to build extremely robust nodes would be unrealistic if they do not have to carry high loads.

Next, we will explore the cascading failures mechanism within the power network. We assume that cascading failures originate from an attack on some power nodes. Here, the initial attack on the power network is interpreted as the removal of those attacked nodes from the network (Albert et al. 2000, Holme et al. 2002). The loads of removed nodes will then be redistributed to their neighboring nodes based on the following rule, which is shown in Figure 1.

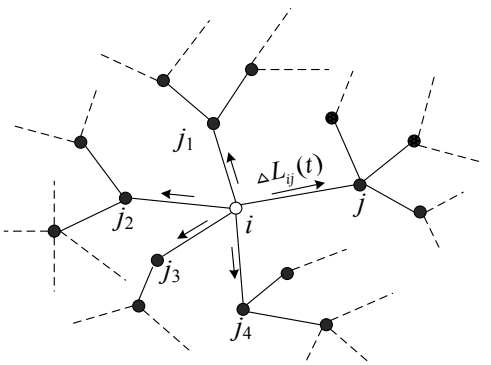

Figure 1 Preferential redistribution of the failed node's load in the power network

In Figure 1, according to the rule of preferential redistribution, the extra load $\triangle L_{ij}(t)$ of the neighboring node j from the failed node i at time t is defined as follows:

$$\triangle L_{ij}(t) = L_i(t)\frac{L_j(t)}{\sum_{k\in\Gamma_i(t)} L_k(t)}, \qquad (5)$$

where $\Gamma_i(t)$ is the set of neighboring operating nodes of node i at time t. Therefore, the load $L_j(t+1)$ of operating node j at time $t+1$ is given by the following equation:

$$L_j(t+1) = L_j(t) + \sum_{i\in\Psi_j(t)} \triangle L_{ij}(t), \qquad (6)$$

where $\Psi_j(t)$ is the set of neighboring failed nodes of node j at the end of time t. Next, if the load $L_j(t+1)$ of node j at time $t+1$ is larger than its capacity, this load $L_j(t+1)$ will then be distributed to its neighboring operating nodes and potentially cause them to fail.

After modeling cascading failures within the power network, the next step is to describe how failures in the power network propagate to the water network. To explore the interdependent response of the water network more precisely, we propose a parameter $P_{B_j|A_i}$ to measure the interdependence strength between the two networks. This parameter is the probability that the relationship between two nodes in different networks enables failure to propagate from one node to the other one (Hernandez-Fajardo and Dueñas-Osorio 2011, Wu et al. 2013), which is expressed as follows:

$$P_{B_j|A_i} = P(\text{failure of water node } j \mid \text{failure of power node } i), \qquad (7)$$

where A_i means the failure of node i ($i \in V_{A_2}$) in the power network; B_j means the failure of dependent node j ($j \in V_B$) in the water network; $P_{B_j|A_i}$ is the conditional probability of B_j given A_i ranging from independence $P(B_j \mid A_i) = P(B_j)$ to complete interdependence $P(B_j \mid A_i) = 1$. The

reason why there is a conditional probability of failure can be explained with the working performance of back-up power for any power node. For instance, when $P(B_j|A_i)=P(B_j)$, the interdependence strength between power and water network is extremely weak. In this case, even if power node i fails to function, dependent water node j could still work well because of the good performance of back-up power to timely supply power. But when $P(B_j|A_i)=1$, the interdependence strength between power and water network is extremely strong. In this case, when power node i fails to function, dependent water node j will malfunction due to poor performance or inexistence of back-up power.

Cascading failures may stop after a few steps or spread and finally cause all the interdependent networks to break down. Hence, it is necessary to develop an indicator to quantitatively measure the consequence of cascading failures to interdependent networks. For real networks, there is a general hypothesis that the flow between any two nodes in network always takes the shortest path connecting them. So Watts and Strogatz (1998) proposed the average shortest path length $L=\sum_{i\neq j\in V}d_{ij}/N(N-1)$ to measure the efficiency of network. In order to avoid the infinity caused by the disconnection between two nodes, the average reciprocal shortest path length E has been used generally (Latora and Marchiori 2001, Crucitti et al. 2003). It is shown as follows:

$$E=\frac{1}{N(N-1)}\sum_{i\neq j}\frac{1}{d_{ij}}, \tag{8}$$

where d_{ij} is the shortest path length connecting node i and j. If nodes i and j are not connected or become disconnected because of an attack, then $d_{ij}=\infty$ and then $1/d_{ij}=0$. If the E of a network is smaller than that of other network, the d_{ij} of most pairs of nodes of this network will be larger than that of other network, then the flow between any two nodes in this network will take longer path and more time or resources, so the efficiency of this network is lower than that of other network. In this sense, it is reasonable to use the E for indicating the efficiency of interdependent power-water networks.

4. Analysis of Simulation Results

Before exploring the vulnerability of interdependent power-water networks to cascading failures through numerical simulation, the values of some parameters in the simulation model must be fixed. We set the number of all power nodes as N_A=100, the number of all generators as N_{A1}=10, the number of all water nodes as N_B=80, and the number of all pumps as N_{B1}=15. Considering the average node degree $\langle k\rangle$=2.78 of the North American grid (Albert et al. 2004) and $\langle k\rangle$=2.36 of grid in an area of China (Chen et al. 2007), we set m=2 in the generation algorithm. Next, we can generate a graph of interdependent power-water networks with $\langle k\rangle$=3.6 of the power network and $\langle k\rangle$=3.25 of the water network, which is shown in Figure 2.

Subsequently, we will utilize numerical simulation to explore the vulnerability of interdependent networks to cascading failures under the tolerance parameter β and fraction f_A of initially attacked power nodes, interdependence strength $P_{B_j|A_i}$, and different attack strategies.

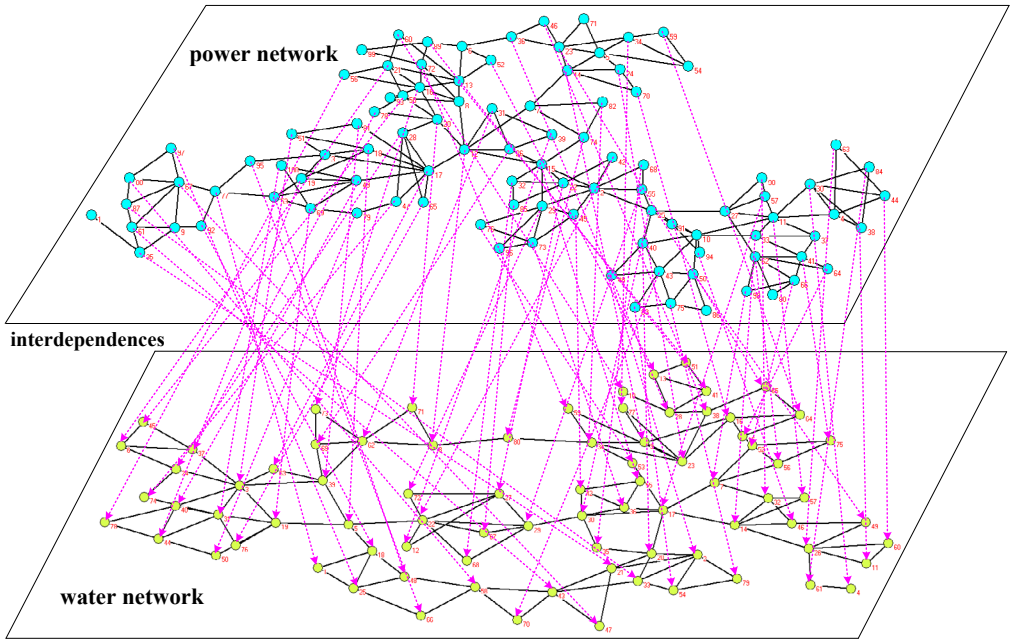

Figure 2 The graph of interdependent power-water networks topology

4.1 Impact of Tolerance Parameter β and Fraction f_A on Vulnerability

As stated in the cascading failures model, the capacity C_i of node i is linearly proportional to its initial load. Hence, if the value of β is large enough, the capacity of any operating node is large enough to accommodate extra loads from its neighboring attacked nodes. In other words, cascading failures will not spread within the power network and will not propagate to the dependent water network when the value of β is large enough. In this sense, we introduce a new parameter called the critical tolerance threshold β^*, which is used to indicate the vulnerability of interdependent networks to cascading failures. Specifically, when $\beta \geq \beta^*$, most of nodes will function well and cascading failures can be prevented; However, when $\beta < \beta^*$, cascading failures will spread within the power network and propagate to the water network because most power nodes will be unable to accommodate extra loads from their neighboring attacked nodes. Next, we will explore how the efficiencies E_A of the power network and E_B of the water network vary with values of β under random attack on some given fraction f_A of power nodes, which is shown in Figure 3. Here, E_A (E_B) is the ultimate efficiency of the power (water) network when cascading failures come to an end.

In Figure 3, the efficiencies E_A and E_B always stay at 0 when the values of β are below a certain threshold under random attack on a given fraction of power nodes. For example, $E_A \equiv 0$ and $E_B \equiv 0$ when the values of β are below 0.34 under random attack on 5% of power nodes. That is, all the power (water) nodes failed when the values of β are below 0.34 under random attack on 5% of power nodes. Next, E_A and E_B rise sharply when the values of β

exceed this threshold, and then remain at a stable value along with the increase of β. For example, E_A (E_B) rises to 0.218 (0.167) rapidly and then remains stable along with the increasing values of β above the threshold 0.34 under randomly attack on 5% of power nodes. In this study, this remarkable threshold is the so-called the critical tolerance threshold β^*. Additionaly, a positive correlation is found between the critical tolerance threshold β^* and the fraction f_A for both networks. For example, β^*=0.34 under f_A=5%, β^*=0.52 under f_A=15%, β^* =1 under f_A=25%, and β^* =1.04 under f_A=35% for the two networks. Therefore, cascading failures in interdependent power-water networks can be prevented completely when the values of β are above a certain β^* under attack on a given fraction of power nodes. Furthermore, increasing the value of β to decrease the vulnerability of interdependent power-water networks to cascading failures is always effective.

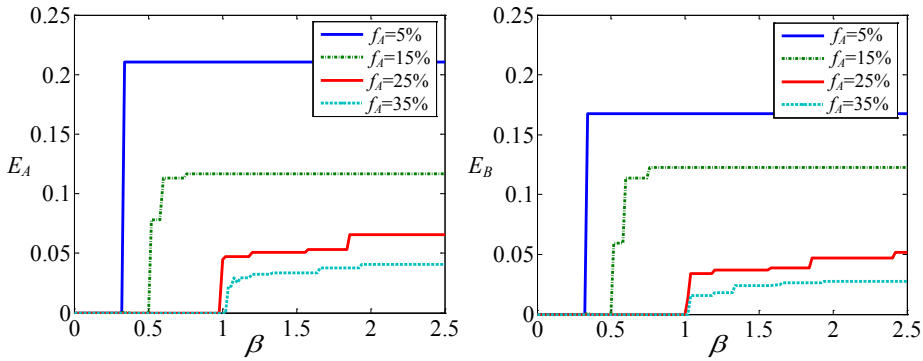

Figure 3 Relationship between E_A (E_B) and β under random attack on different fractions f_A ($P_{B_j|A_i}$ =100%)

For any given value of β, a significant relationship also exists between the efficiency E_A (E_B) and fraction f_A, as illustrated in Figure 4. For example, when β=0.20, the efficiencies E_A (E_B) first decrease slightly from 0.2314 (0.2376) to 0.2088 (0.2025) after 1% of power nodes are randomly attacked, and then plummets suddenly from 0.2088 (0.2025) to 0 after 2% of power nodes are randomly attacked. Similarly, when β=0.50, E_A (E_B) plummets from 0.2314 (0.2376) to 0 after 6% of power nodes are randomly attacked. Here, these two significant fractions (i.e., f_A=2% under β =0.20 and f_A=6% under β =0.50) are called the critical fractions f_A^* (Dorogovtsev et al. 2008, Buldyrev et al. 2010, Johansson and Hassel 2010). Therefore, cascading failures spread within the power network and then propagate to the water network after attacking a certain critical fraction f_A^* of power nodes under a relatively small value of β. However, under β=0.80 and 1.10, E_A (E_B) falls smoothly from 0.2314 (0.2376) to 0 along with the increase of fraction f_A from 0% to 100%. The reason for this results is that, when the value of β is large enough, the capacity of each operating power node can accommodate extra loads, as well as prevent cascading failures from spreading within the power network and further

propagating to the water network. At this moment, only the increasing number of attacked power nodes (or the dependent failed water nodes) account for the smooth reduction of efficiency E_A (E_B) when the value of β is large enough.

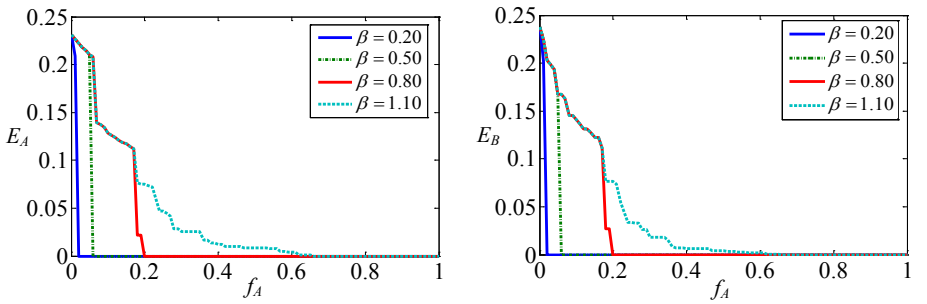

Figure 4 Relationship between E_A (E_B) and f_A under different values of β ($P_{B_j|A_i}$=100%)

4.2 Impact of Interdependence Strength $P_{B_j|A_i}$ on Vulnerability

Water network is dependent on power network when $P(B_j \mid A_i) > P(B_j)$. In the extreme case of $P(B_j \mid A_i) = 1$, the failure of node $i (i \in V_{A_2})$ in the power network will certainly make water node $j (j \in V_B)$ fail if it depends on this substation, as illustrated briefly in Figure 5. Assuming that power node A_1 is attacked initially and causes the nodes A_2, A_3, A_4, and A_5 to malfunction because of overload, only the power nodes A_1, A_2, A_3, A_4, and A_5 are failed in the end when $P(B_j \mid A_i) = P(B_j)$. However, when $P(B_j \mid A_i) = 1$, the water nodes B_1, B_2, and B_3 will also fail because of the interdependences between the two networks. Therefore, the interdependences between the two networks may enlarge the consequences of cascading failures and increase the vulnerability of interdependent networks.

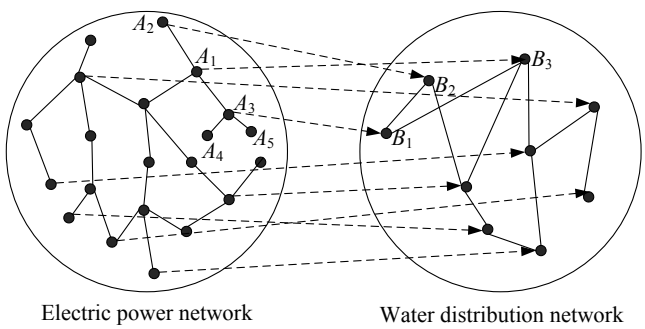

Figure 5 Example of cascading failures in interdependent networks after attacking power node A_1

To explore the precise impact of interdependences on the vulnerability of interdependent networks, we will study how the efficiencies E_B of the water network vary indirectly with the fractions f_A under different levels of interdependence strength $P_{B_j|A_i}$, which is shown in Figure 6.

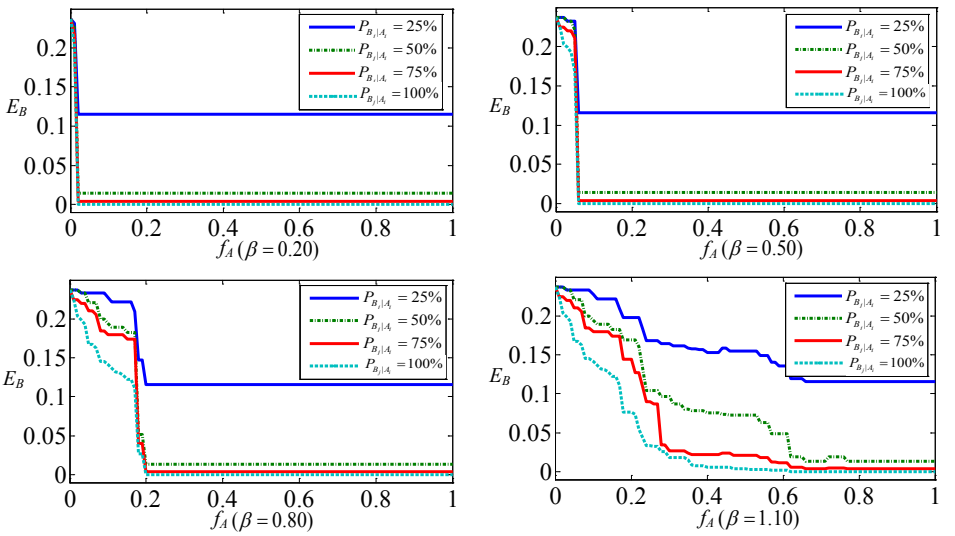

Figure 6 Relationship between E_B and f_A under different values of $P_{B_j|A_i}$ (when β=0.20, 0.50, 0.80, 1.10)

In Figure 6, we assume that all pairs of interconnected nodes have the equal conditional probability. This figure illustrates that for any value of β, the efficiencies E_B always decrease along with the increase of interdependence strength $P_{B_j|A_i}$ under attack on any given fraction f_A. For example, when β =0.8, the efficiencies E_B=0.2274 under $P_{B_j|A_i}$ =25%, E_B=0.1944 under $P_{B_j|A_i}$=50%, E_B=0.1801 under $P_{B_j|A_i}$=75%, and E_B=0.1411 under $P_{B_j|A_i}$=100% after attacking f_A=10% of power nodes. These simulation results validate the previous conclusion that the interdependences between interdependent networks can significantly increase their vulnerability to cascading failures (Buldyrev et al. 2010, Parshani et al. 2010). Therefore, it is crucial to protect those pairs of interconnected nodes in interdependent networks for reducing the consequences of cascading failures.

4.3 Impact of Attack Strategies on Vulnerability

Subsections 4.2 and 4.3 present the hypothesis that cascading failures in interdependent networks are triggered by randomly attacking power nodes, which means each node in the power network has an equal probability of being attacked. Different nodes play different roles in keeping the network functional. Thus, some attackers (e.g., terrorists) are more likely to attack more critical nodes of infrastructure networks. Only in this way can they destroy the infrastructure completely by attacking a small number of critical nodes. Considering that the degree and load of a node are the two important

indicators of its characteristics, we propose two types of intentional attack strategies, namely high-degree and high-load attacks. Under high-degree attack, the nodes with high degrees are preferentially attacked. Under high-load attack, the nodes with high initial loads are preferentially attacked. Next, we will explore the different impacts of the three attack strategies (i.e., random, high-degree, and high-load) on the vulnerability of interdependent networks by studying how the average efficiencies $\bar{E}$ vary with values of β under three attack strategies, which are shown in Figure 7. Here, $\bar{E}=(E_A+E_B)/2$ is the ultimate average efficiency of two networks at the end of cascading failures.

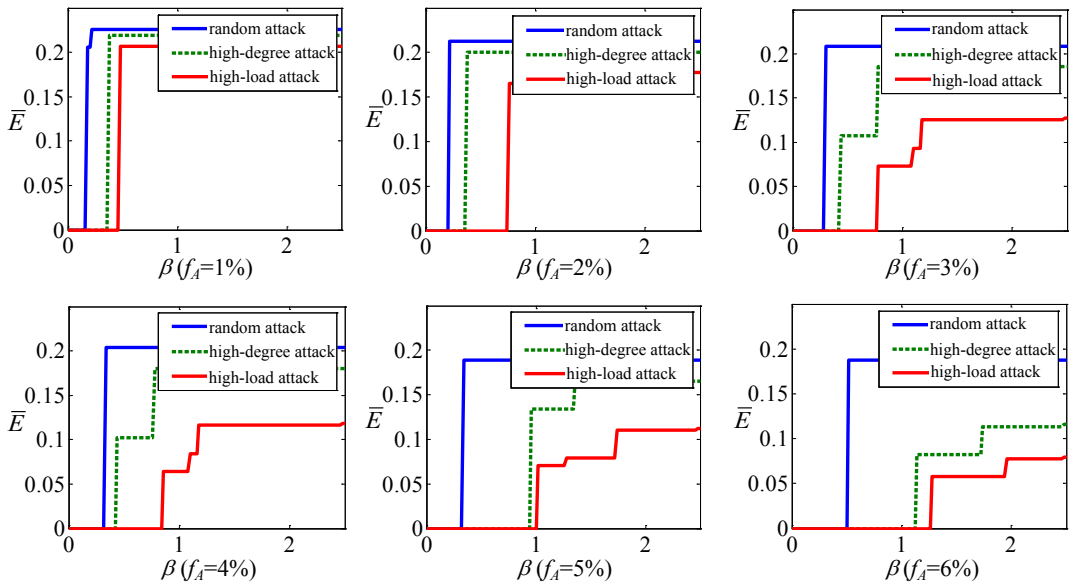

Figure 7 Relationship between $\bar{E}$ and β under the three attack strategies (when f_A =1%, 2%, 3%, 4%, 5%, 6%, and $P_{B_j|A_i}$ =100%)

In Figure 7, for any value of β, the critical tolerance threshold β^* under high-load attack is always larger than those under high-degree and random attacks. For example, when f_A=1%, β^*=0.48 under high-load attack, β^*=0.38 under high-degree attack and β^*=0.18 under random attack. Therefore, interdependent power-water networks under high-load attack are most vulnerable to cascading failures. In other words, the largest amount of cost needs to be invested into interdependent networks to prevent cascading failures under high-load attack rather than under high-degree and random attacks. The reason for such investment is that β^* is mainly determined by the highest initial loads of all attacked nodes, so β^* under high-load attack is the largest one. In addition, Figure 8 shows that the nodes with high degrees are more likely to be ones with high initial loads according to the definition of node load. Therefore, β^* under high-degree attack is between β^* under high-load attack and β^* under random attack.

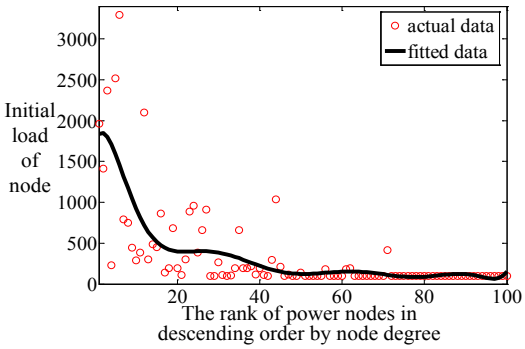

Figure 8 Relationship between initial load and rank of power nodes in descending order by node degree

The simulation results in subsection 4.1 reveal that E_A (E_B) of the power (water) network will fall rapidly to 0 after f_A increases to the critical fraction f_A^* under a relatively small value of β, but will decreases smoothly along with the increase of f_A when the value of β is large enough. Here, we will study the impact of three attack strategies on this relationship, which is shown in Figure 9. This figure illustrates that the critical fraction f_A^* under high-load attack is always the least one under the three attack strategies when the value of β is relatively small. For example, when β=0.5, f_A^*=2% under high-load attack, f_A^*=5% under high-degree attack and f_A^*=6% under random attack. In other words, only 2% of power nodes with the highest loads can trigger cascading failures in interdependent networks under high-load attack when β =0.5. However, when β =1.0, cascading failures are prevented completely and just the initially attacked nodes account for the reduction of $\overline{E}$ under random attack, and f_A^*=5% under high-load attack and f_A^*=6% under high-degree attack. When β =1.5, cascading failures are prevented under high-degree and random attacks, while f_A^*=7% under high-load attack. When β =2.0, cascading failures are prevented completely under the three types of attacks. Therefore, we should identify those critical nodes with high loads, and then preferentially invest sufficient resources to protect them from increasing the vulnerability of interdependent networks to cascading failures.

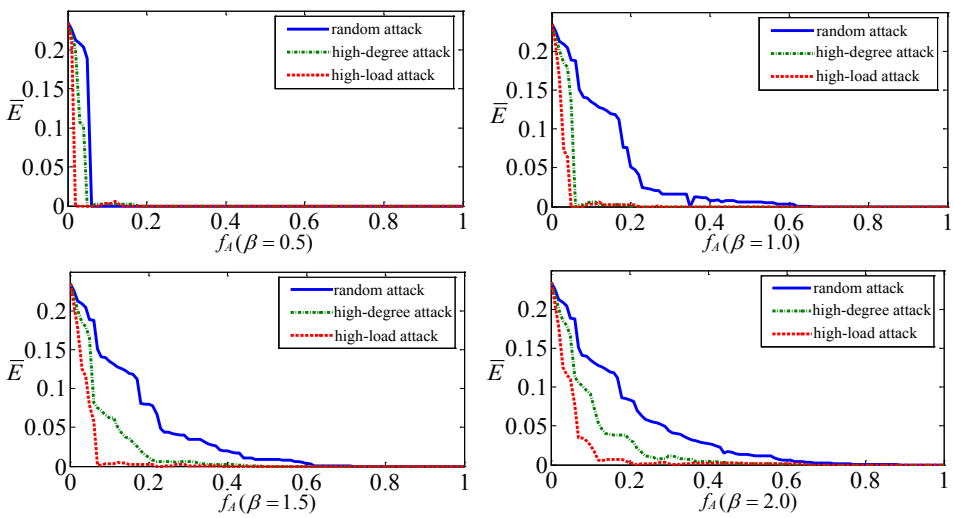

Figure 9 Relationship between $\overline{E}$ and f_A under three attack strategies (when β =0.5, 1.0, 1.5, 2.0, and $P_{B_j|A_i}$ =100%)

5. Conclusions

Critical infrastructures are becoming increasingly interdependent and susceptible to exposure to cascading failures. This study takes power and water networks as an example of interdependent infrastructure networks, and then develops a more realistic simulation model that considers the dynamic redistribution of load in power network to explore the vulnerability of interdependent networks through numerical simulation. In this model, fictional power and water networks are generated based on the spatial proximity among nodes, and their interdependences across the two networks are built based on the physical dependency. Moreover, critical tolerance threshold β^* is originally proposed to indicate the vulnerability of the network to cascading failures. Finally, the vulnerability of interdependent networks under some key parameters is explored through numerical simulation.

The results of the study are as follows: 1) Cascading failures can be prevented completely when the values of β are above a certain β^* under attack on a given fraction f_A of power nodes. Otherwise, cascading failures spread in interdependent networks after attacking a certain critical fraction f_A^* of power nodes under a relatively small value of β. This results shows that increasing the values of β is always effective for reducing the vulnerability of interdependent networks to cascading failures. 2) The efficiencies E_B always decrease with the increase of interdependence strength $P_{B_j|A_i}$. This finding validates the conclusion that interdependences in interdependent networks increase their vulnerability to cascading failures. Therefore, protecting those pairs of interconnect nodes is crucial to reducing the consequences of cascading failures. 3) Interdependent networks under high-load attack are more vulnerable to cascading failures than those under high-degree and random attacks, showing the significance of protecting those high-load critical nodes to prevent cascading failures proactively.

This work will help governments proactively protect interdependent infrastructures under cascading failures in the real world. Note that the cascading failures model proposed in this study may not describe thoroughly what happens to real interdependent power-water networks under cascading failures. For instance, different attacks such as natural and man made hazards, may have different influences on different infrastructures and even on different nodes within an infrastructure. As such, this direction will be the focus of our future work.

6. Acknowledgments

This work is supported by National Natural Science Foundation of China (No. 71501158; 71471146) and "the Fundamental Research Funds for the Central Universities". The authors would like to thank the referees for their efforts to improve the quality of this paper.

References

[1] Albert, R., Albert, I. & Nakarado, G.L. (2004). Structural vulnerability of the North American power grid. Physical Review E, 69(2): 025103(R).

[2] Albert, R., Jeong, H. & Barabási, A.L. (2000). Error and attack tolerance of complex networks. Nature, 406: 378-382.

[3] Bagchi, A., Sprintson, A., Guikema, S.,

Bristow, E. & Brumbelow, K. (2010). Modeling performance of interdependent power and water networks during urban fire events. Paper presented at the 48th Annual Allerton Conference on Communication, Control, and Computing: 1637-1644.

[4] Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E. & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464: 1025-1028.

[5] Chang, S.E., McDaniels, T.L., Mikawoz, J. & Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. Natural Hazards, 41(2): 337-358.

[6] Chen, X., Sun, K. & Cao, Y. (2007). Structural vulnerability analysis of large power grid based on complex network theory. Transactions of China Electro-technical Society, 22(10): 138-144.

[7] Crucitti, P., Latora, V., Marchiori, M. & Rapisarda, A. (2003). Efficiency of scale-free networks: error and attack tolerance. Physica A: Statistical Mechanics and Its Applications, 320: 622-642.

[8] de Bruijne, M. & van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of Contingencies and Crises Management, 15(1): 18-29.

[9] Dorogovtsev, S.N., Goltsev, A.V. & Mendes, J.F.F. (2008). Critical phenomena in complex networks. Reviews of Modern Physics, 80(4): 1275-1335.

[10] Dueñas-Osorio, L., Craig, J.I. & Goodno, B.J. (2007). Seismic response of critical interdependent networks. Earthquake Engineering & Structural Dynamics, 36(2): 285-306.

[11] Eusgeld, I., Nan, C. & Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures. Reliability Engineering & System Safety, 96(6): 679-686.

[12] Goh, K.-I., Kahng, B. & Kim D. (2001). Universal behavior of load distribution in scale-free networks. Physical Review Letters, 87(27): 278701.

[13] Hernandez-Fajardo, I. & Dueñas-Osorio, L. (2011). Sequential propagation of seismic fragility across interdependent lifeline systems. Earthquake Spectra, 27(1): 23-43.

[14] Holme, P., Kim, B.J., Yoon, C.N. & Han, S.K. (2002). Attack vulnerability of complex networks. Physical Review E, 65(5): 056109.

[15] Huang, X., Gao, J., Buldyrev, S.V., Havlin, S. & Stanley, H.E. (2011). Robustness of interdependent networks under targeted attack. Physical Review E, 83(6): 065101(R).

[16] Hwang, H., Lin, H. & Shinozuka, M. (1998). Seismic performance assessment of water delivery systems. Journal of Infrastructure Systems, 4(3): 118-125.

[17] Jia, S.M., Wang, Y.Y. & Feng, C. (2014). Cascading failures in power grid under three node attack strategies. Intelligent Computing Methodologies, 8589: 779-786.

[18] Johansson, J. & Hassel, H. (2010). An approach for modeling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety, 95(12):

1335-1344.

[19] Kinney, R., Crucitti, P. & Albert, R. (2005). Modeling cascading failures in the North American power grid. The European Physical Journal B, 46(1): 101-107.

[20] Lan, Q., Zou, Y. & Feng, C. (2012). Cascading failure of power grids under three attack strategies. Chinese Journal of Computational Physics, 29(6): 943-948.

[21] Latora, V. & Marchiori, M. (2001). Efficient behavior of small-world networks. Physical Review Letters, 87(19): 198701.

[22] Lee, E.E., Mitchell, J.E. & Wallace, W.A. (2007). Restoration of services in interdependent infrastructure systems: a network flows approach. IEEE Transactions on Systems, Man, and Cybernetics, 37(6): 1303-1317.

[24] Little, R.G. (2002). Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructure. Journal of Urban Technology, 9(1): 109-123.

[25] McDaniels, T., Chang, S., Peterson, K., Mikawoz, J. & Reed, D. (2007). Empirical framework for characterizing infrastructure failure interdependencies. Journal of Infrastructure Systems, 13(3): 175-184.

[26] Motter, A.E. & Lai, Y.C. (2002). Cascade-based attacks on complex networks. Physical Review E, 66(6): 065102(R).

[27] Newman, M.E.J. (2001). Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. Physical Review E, 64(1): 016132.

[28] Ouyang, M., Hong, L., Mao, Z.J., Yu, M.H. & Qi, F. (2009). A methodological approach to analyze vulnerability of interdependent infrastructures. Simulation Modeling Practice and Theory, 17(5): 817-828.

[29] Parshani, R., Buldyrev, S.V. & Havlin, S. (2010). Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. Physical Review Letters, 105(4): 048701.

[30] Restrepo, C.E., Simonoff, J.S. & Zimmerman, R. (2006). Unraveling geographic interdependencies in electric power infrastructure. Paper presented at the 39th Hawaii International Conference on Systems Sciences, Hawaii, USA.

[31] Rinaldi, S., Peerenboom, J. & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6): 11-25.

[32] Wang, J.W. & Rong, L.L. (2009). Cascade-based attack vulnerability on the US power grid. Safety Science, 47(10): 1332-1336.

[33] Watts, D.J. & Strogatz, S.H. (1998). Collective dynamics of 'small-world' networks. Nature, 393(6684): 440-442.

[34] Wu, J. & Dueñas-Osorio, L. (2013). Calibration and validation of a seismic damage propagation model for interdependent infrastructure systems. Earthquake Spectra, 29(3): 1021-1041.

[35] Xu, X., Zhang, X. & Mendes, J.F.F. (2007). Impacts of preference and geography on epidemic spreading. Physical Review E, 76(5): 056109.

[36] Zimmerman, R. & Restrepo, C.E. (2006). The next step: quantifying infrastructure interdependencies to improve security.

International Journal of Critical Infrastructures, 2(2-3): 215-230.

Yanlu Zhang is a lecturer of School of Management, Northwestern Polytechnical Unversity, Xi'an, China. He received his PhD in management science and engineering from Northwestern Polytechnical University. His research interests focus on complex systems modeling and simulation, risk management of complex systems. He currently published many high-level papers in Reliability Engineering & System Safety, Safety Science, Systems Engineering – Theory & Practice, Chinese Journal of Management Science, etc.

Naiding Yang is a professor and doctoral mentor of School of Management, Northwestern Polytechnical University, Xi'an, China. He received his PhD in management science and engineering from Xi'an Jiaotong University. His research interests include management system engineering, risk management, decision analysis. He is the executive director of Emergency Management Institute of Northwestern Polytechnical University, and a member of Systems Engineering Society of China, Management Science and Engineering Society of China, Project Management Research Committee China, etc.

Upmanu Lall is the Alan and Carol Silberstein Professor of Engineering at Columbia University and the Director of the Columbia Water Center. He is a world-renowned expert in statistical and numerical modeling of hydrologic and climatic systems and water resource systems planning and management. His research areas include hydro-climatology, nonlinear dynamics, applied statistics, natural hazards, water systems and risk management, etc. He has pioneered statistical methods and their application to the prediction of hydrologic and climate conditions, and advanced tools for decision analysis and risk management.