Chaos, Solitons and Fractals 117 (2018) 21–29

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

A methodological framework for vulnerability analysis of interdependent infrastructure systems under deliberate attacks

Shuliang Wang[a,b,*], H. Eugene Stanley[b], Yachun Gao[c,b]

[a] School of Electrical Engineering and Automation, Jiangsu Normal University, Xuzhou 221116, China
[b] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[c] School of Physical Electronics, University of Electronic Science and Technology of China, Cheng Du 610054, China

ARTICLE INFO

Article history:
Received 5 February 2018
Revised 26 August 2018
Accepted 5 October 2018
Available online 10 October 2018

Keywords:
Critical areas
Deliberate attacks
Interdependent systems
Vulnerability analysis

ABSTRACT

In this paper, we give a methodological framework to analyze vulnerability of interdependent infrastructure systems under deliberate attacks. Meanwhile, the intelligence of attackers is considered and a method of critical attack area identification according to community detection is proposed as well. The Interdependent power and gas system in Wuhan, China is taken as the example. We determine the vulnerabilities of different critical areas in both independent and interdependent scenarios. In the meantime, percolation theory are utilized and different coupling strengths are considered to further analyze the vulnerabilities. It is found that the disruption of only a few vertices may lead to complete collapsing for some critical areas and the vulnerabilities increase when systems become interdependent. Therefore, greater protection should be given to critical areas of a network in order to reduce the vulnerabilities when deliberate attacks occur. The proposed method could help decision makers develop mitigation techniques and optimal protection strategies.

1. Introduction

Real-world networks are critical infrastructure systems (CISs) which function collaboratively and synergistically to produce essential services and facilitate human interaction [1–3]. Examples include electrical power systems, telecommunication systems, water supply systems, natural gas supply systems, and transportation systems, all of which are essential in maintaining the economy of a nation and the well-being of its citizens.

Due to the expansion of information technology, CISs are now highly connected and mutually interdependent [4–7]. Although these interdependencies increase operational efficiency, social disruptions caused by recent disasters, ranging from hurricanes to large-scale power outages and deliberate attacks, indicate that they also increase system vulnerability. Small failures in a subsystem can initiate cascading failures across an entire network, and increasing the level of interconnections among CISs have increased their vulnerability.

Scholars in different fields define vulnerability differently [8–11]. The glossary of the Society for Risk Analysis (SRA) defines vulnerability as the degree to which a system can be affected by a source of risk [12]. Zio [13] defines vulnerability as a global flaw or weakness in the design, implementation, operation, or management of an infrastructure system. In this paper we define vulnerability as the decrease in performance of the system when it is disturbed.

To understand how vulnerability of interdependent CISs differs under different failure scenarios we examine both interdependency and modes of failure. In recent years, a number of different ways of characterizing CISs interdependency have been proposed. The widely-cited framework proposed by Rinaldi et al. defines the interdependency as a bidirectional relationship between two CISs and distinguishes four types: physical interdependency, cybernetic interdependency, geographic interdependency, and logical interdependency [14].

Earl et al. define five types of infrastructure dependencies, including input dependence, mutual dependence, shared dependence, exclusive-or dependence, and co-located dependence [15]. There are currently many efforts to develop models to capture the interdependencies among critical infrastructures, and these efforts have been summarized by Ouyang [16]. Identifying interdependencies enables us to analyze the mechanism of fault propagation.

Depending on the failure scenarios, we classify the failure modes into three types, (i) random failures, (ii) natural hazards, and (iii) deliberate attacks, such as terrorist or military attacks. When modeling the vulnerability of a CIS to random failure, the

* Corresponding author at: School of Electrical Engineering and Automation, Jiangsu Normal University, Xuzhou 221116, China.
E-mail addresses: shuliang0820@sina.com, 6020150035@jsnu.edu.cn (S. Wang).

https://doi.org/10.1016/j.chaos.2018.10.011
0960-0779/

usual approach is to randomly remove a fraction of system components. When analyzing vulnerability of CISs under natural hazards, impacts of natural hazards on system components is usually modeled according to fragility curves, which provide the probability of exceeding a certain damage state threshold conditional to a selected hazard intensity measure. When modeling the vulnerability of a CIS to deliberate attacks, we identify the important components that would be probable attack targets.

CISs have exhibited high vulnerabilities under deliberate attacks, and thus it is a topic of great interest. Most research on deliberate attacks has ignored high network density factors. There are only a few literatures attempting to capture the vulnerabilities of the systems under disruptions in a localized area where components are distributed in close proximity [5,17], Yet, with the studies considering proximity factors, usually a random attack center or randomly diluted square lattice or generic hexagonal grid is selected as the attack area, which does not necessarily reflect the importance of the region in the systems.

Research indicates that attackers have access to a large amount of information [18] and usually target densely connected areas to maximize infrastructure damage. These dense areas have been defined as network structures that are "relatively densely connected to each other but sparsely connected to other dense groups in the network" [19–20], and are more likely to become the targets. The task is to identify these areas, and to measure the vulnerability of the systems in these areas.

We study the vulnerability of interdependent systems under terrorist attacks by focusing on the interdependent power and gas systems in Wuhan, China and—because the two systems are in close proximity—examining their physical and geographic interdependency. We also introduce a way of identifying critical attack areas that takes into account levels of attacker intelligence and examine regional deliberate attacks on both independent and interdependent infrastructure components.

Section 2 of this paper proposes a methodological framework for analyzing vulnerability of interdependent CISs, introduces the fundamental concepts and definitions used to characterize the structural and functional characteristics of power and gas infrastructure systems, and introduces the relevant interdependencies, vulnerability models, performance metrics, and corresponding vulnerability metrics. Section 3 gives a case study, and Section 4 analyzes the results that capture the vulnerabilities of independent and interdependent systems. Section 5 gives a further discussion, vulnerabilities of the networks under different coupling strengths are analyzed using percolation theory. Section 6 presents conclusions and prospects for future research.

2. A methodological approach

Fig. 1 shows the methodological framework for the vulnerability analysis of interdependent infrastructure systems under deliberate attacks.

2.1. Development of adequate system understanding

We first clarify the topological and geographical features of subject of our research. The function role of nodes in the power network includes generation, substation and distribution. The distribution network has 135 transmission lines and 111 nodes, including 11 power plants and 100 substations. On the other hand, the nodes in the gas system represent compressors, storage facilities, delivery facilities, receipt facilities, and pipeline junctions. The edges are gas pipeline segments. They constitute three component parts, (i) the gathering system, (ii) the transportation system, and (iii) the distribution system. The gas storage facilities and the gas receipt facilities are source nodes, the connection points and gas compressors are transmission nodes, and the gas delivery facilities are load nodes. The geographical distribution of the selected networks which is obtained from our previously work is shown in Fig. 2 [21]. Table 1 lists their topological properties, where $N$is the number of nodes, $E$is the number of edges, $G$is the number of generators, $< k >$ is the average degree, $C$is the average clustering coefficient, $< d >$ is the characteristic path length, $B$is the nodes average betweenness.

Table 1
General properties of the power and gas pipeline systems.

Network	N	E	G	$\langle k \rangle$	C	$\langle d \rangle$	B
Power	111	135	11	2.432	0.047	8.247	797
Gas	30	38	4	2.533	0.126	4.313	96

2.2. Selection of vulnerability models and vulnerability metrics

2.2.1. Vulnerability models

To analyze the vulnerability of interdependent systems, we present the models to simulate the dynamical processes of the power and gas networks. There are basically three types of models for the power networks, i.e., the Purely Topological Models (PTM) [22], the Real Alternative Current Power Flow Model (ACPFM) [23], and the Artificial Flow Model (AFM) [24]. As the PTM cannot capture the dynamics of particles and the overload-induced cascading failures, in the meanwhile, the nonlinear feature of the ACPFM makes it is not feasible on power grids vulnerability analysis. We adopt the Artificial Flow Model (AFM) in this paper.

It is assumed that gas transmission in the gas pipeline network follows shortest paths. We use a generalized betweenness centrality model.

In a gas pipeline network $G_G = (V_G, E_G)$ with nodes set $V_G$and edges set E_G, we assign $T_{K,L}$ to be the flow from the source subgraph (V_K, E_K) to the sink subgraph (V_L, E_L). The generalized betweenness centrality of $e_{ij} \in E_G$ is defined as$G_{ij} = \sum_{\substack{\in V_K \\ \in V_L}} \frac{T_{K,L}}{|V_K||V_L|} \frac{\sigma_{s,t}(e_{ij})}{\sigma_{s,t}}$.

Here, $e_{ij} \in E_G$,$\sigma_{s,t}$ is the number of shortest paths from node s to node t and $\sigma_{s,t}(e_{ij})$ is the number of paths that pass through linke_{ij}. We denote b_j^g to be the decision variable which designates the flow of node j. Its mathematical formulation is

$$b_j^g = \sum_i G_{ij} - \sum_m G_{jm} \tag{1}$$

2.2.2. Vulnerability metrics

After identifying the vulnerability models, the simulation of the dynamical processes is then carried out on power and gas networks. Vulnerability of the power network is defined as the quantified performance drop of the power network when experiencing a disruptive event, expressed as

$$V_P = \frac{P_{\text{norm}} - P_{\text{damg}}}{P_{\text{norm}}} \tag{2}$$

Where P_{norm} is the performance index of the power network under normal operating conditions, and P_{damg} is the performance index after a deliberate attack. The source-demand efficiency which considers the shortest path between the source nodes and the demand nodes is adopted as performance index.

2.2.3. Cascading process

It is assumed in artificial flow model that the particles run along the shortest paths between generator nodes and load nodes, and betweenness is used as a proxy for the load of the nodes. Capacity is defined as the maximum load that a node can handle. We

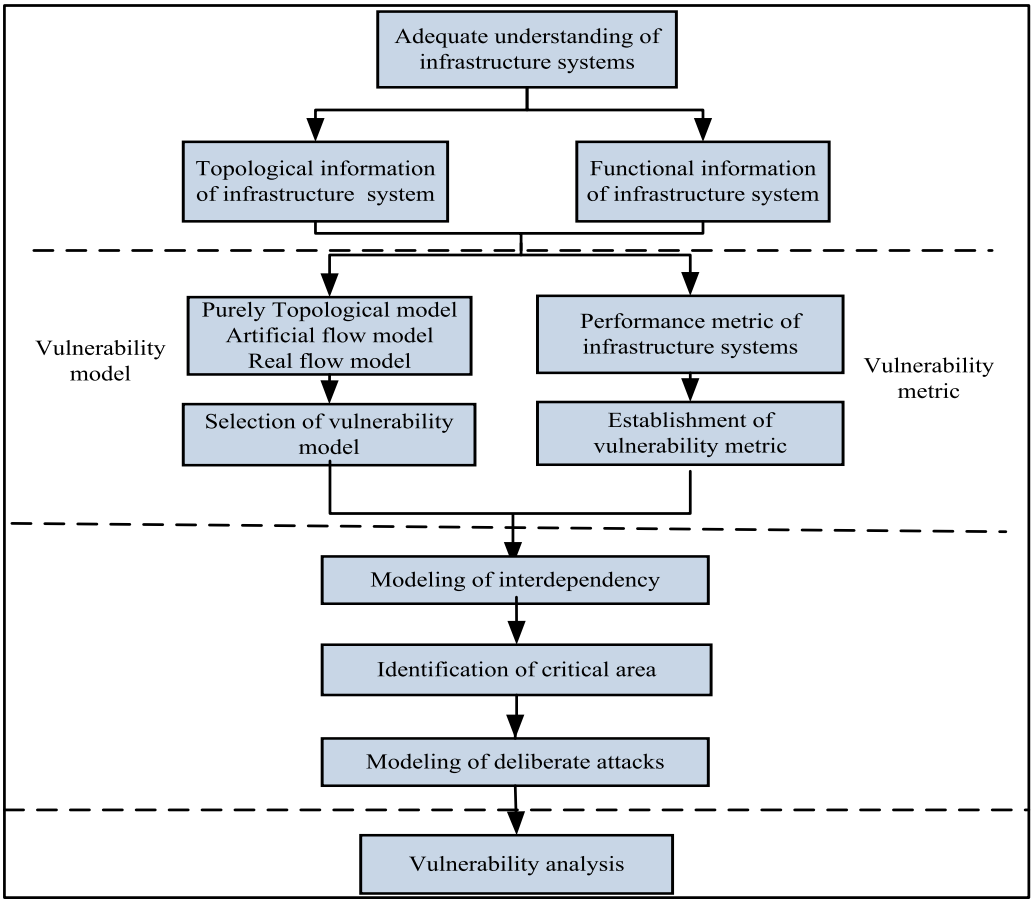

Fig. 1. Methodological framework of the interdependent CISs vulnerability.

assume that the capacity C_j of node j is proportional to its initial load L_j, i.e., $C_j = (1+\alpha)L_j$, where the constant α is the tolerance parameter.

The cascading process is as follows: A disruptive event can cause some components failed and alter the power grid topology, which further changes all components' betweennness values. It may push other nodes beyond their capacity limit and cause their failure. When the loads of the remaining nodes in the network fall below their safety thresholds, the cascading failure stops and the power network reaches a new stable state.

If the gas pipeline network nodes cannot get power supply to ensure their normal operation since the power nodes linking the gas components are destroyed, it will be removed. Then flows in the gas network will be redistributed according to the proposed model. When the gas pipeline node for power production cannot supply sufficient gas, the corresponding gas-fired generator will be removed, and load of the power network will be redistributed again. The cycle goes on until the whole system reaches a stable state.

2.3. Identification of critical areas

Attackers use their collected intelligence to select the most densely connected areas as attack targets. Research indicates that many networks have community structures, defined as a group of elements that are "densely connected to each other but sparsely connected to other dense groups in the network." Since these dense network communities are the most likely targets of deliberate attacks, we use the concept of community to identify probable targets for attacks.

Here we use the fast modularity algorithm to detect community structure. The modularity Q of a set of k communities is defined

$$Q = \sum_{i=1}^{k} \left(\frac{e_i}{m} - \left(\frac{d_i}{2m} \right)^2 \right) \tag{3}$$

where k and e_i define the number of communities and the number of links in community i, respectively, d_i is the degree sum of all nodes in community i, and m is the total number of links in the network. In this community detection strategy we (i) designate each node in the power network a single community, (ii) calculate the change in modularity ΔQ_{ij} when creating a new community from communities i and j, (iii) merge the two communities with the highest ΔQ_{ij} value, and (iv) repeat steps (ii) and (iii) until $\Delta Q_{ij} \leq 0$.

2.4. Modeling of deliberate attacks

In our model we assume probable attack targets will be locally dense community areas, and we collect data on the density of communities to identify these critical attack areas. We then determine the sequence of failure for components within an area. We first identify the system elements with the maximum load or degree in a community area to be the attack center, and we assume that all components connecting to this attack center are directly affected by the attacks. The attack strength of node i connected to the attack center is

$$\text{Attack}_{\text{node}_i}^{\text{strength}} = \text{Attack}_{\text{center}}^{\text{strength}} * (I_i / I_{\text{center}}). \tag{4}$$

Here I_{center} and I_i quantify the importance of the attack center and of node i connected to the attack center, respectively. Note that

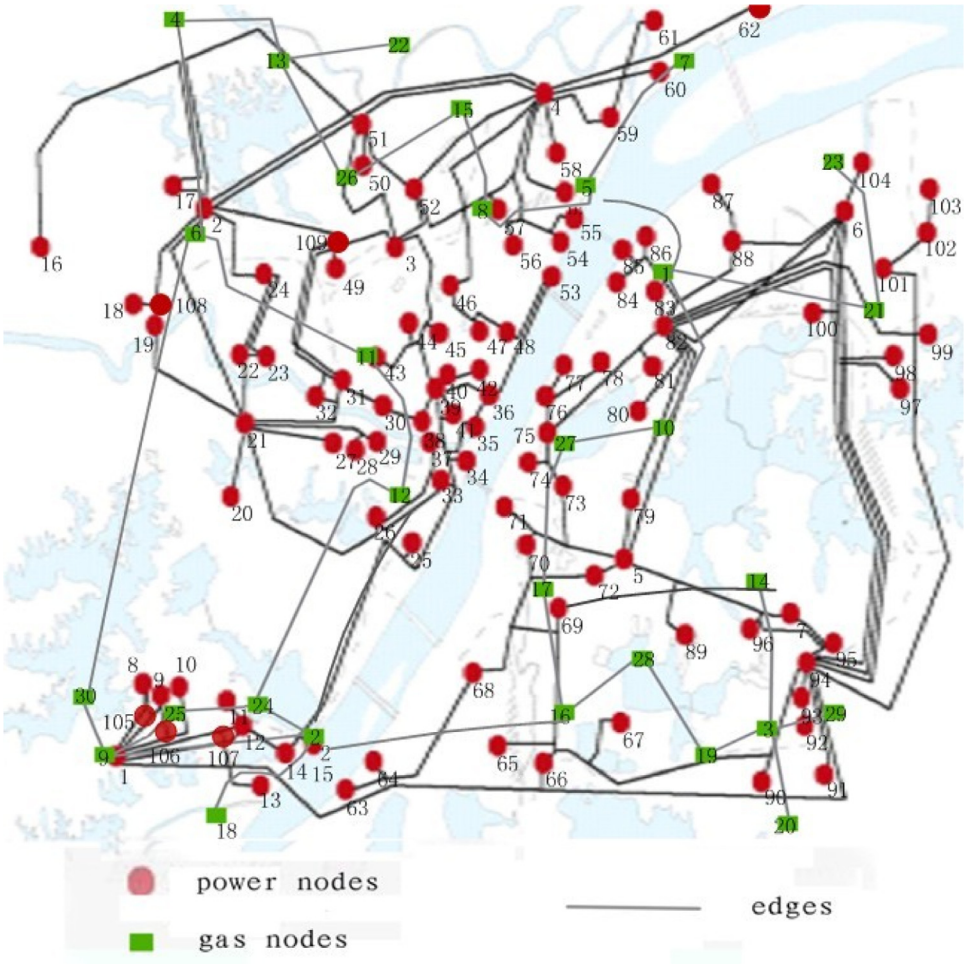

Fig. 2. Topological and geographical information of the power and gas systems in Wuhan [22].

we measure node importance by node degree or load. If node i in the community is not directly connected to the attack center, the attack on node i has strength $\text{Attack}_{\text{node}_i}^{\text{strength}} = 0$, i.e., the node is not directly affected by the attack. In this model both the center attacked and its neighbor nodes are directly affected, and a portion of them fail and are removed from the network. Then, the dynamical processes and performance response can then be simulated using the vulnerability model.

2.5. Modeling of interdependency

Previous literatures provide a variety of approaches to modeling the interdependency of CISs, including those based on system dynamics [25], empirical observation [26], and economic theory [27], and those focusing on agents [28] or the entire network [29]. In current paper, a network-based approach is utilized to determine the topological structure and get geographical information, due to the networked structure of the power-gas interdependent infrastructure systems. The power and gas systems of Wuhan are located in the same region, and thus they have co-located interdependencies. The nodes in the gas transmission system depend on electrical power supply for normal operation and some electrical generators are fueled by gas, there are physical interdependencies. They constitute a network of two partially interdependent networks.

Define P and G as the power and gas pipeline networks. Let P_j^{failure} denote failures of the nodes in the power network upon which the gas network depends, G_i^{failure} denote failures of the gas node which depends on the power network, the conditional probability is set to be $P(G_i^{\text{failure}}|P_j^{\text{failure}})$. Let G_s^{failure} denote failures of the nodes in the gas network upon which the power network depends, P_t^{failure} denotes failures of the power node which depends on the gas nodes, the conditional probability that element P_t will fail when element G_s fails is defined as $P(P_t^{\text{failure}}|G_s^{\text{failure}})$.

3. Case study

Our case study is of the interdependent power and gas systems in Wuhan, China. We analyze the vulnerability of these systems to deliberate attacks. Using the community detection method based on the modularity algorithm, we generate the community structures and identify the critical attack areas. Fig. 3 shows the power network partitioned into nine communities.

After identifying the critical areas, we analyze their vulnerability, measuring them in terms of how much their performance declines after being attacked. We examine both independent and interdependent cases. We first analyze the vulnerability of a single power network to deliberate attacks by (i) examining the influence of deliberate attacks on different critical areas, (ii) identifying the vulnerability of each critical area, and (iii) comparing the vulnerability of each critical area using different tolerance parameters.

We then analyze the vulnerability of interdependent systems. Since the gas pipeline networks are usually underground, we begin by examining the vulnerability to attack of the electrical power network. The electrical network supplies power for gas compressors, storage regulators, and control systems, and the gas pipeline supplies fuel for electrical generators, thus the physical interdepen-

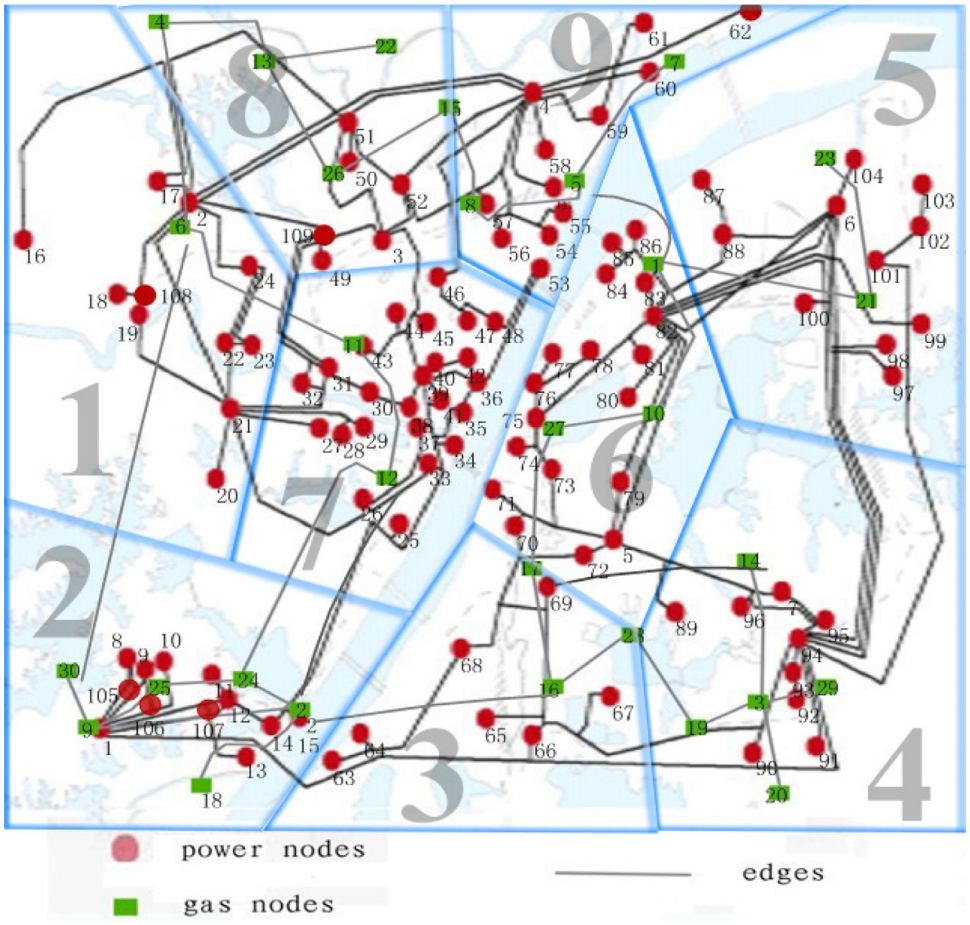

Fig. 3. Communities of power network in Wuhan, China.

dency is bidirectional. We examine (i) the attack times that can collapse a critical area, and (ii) the vulnerabilities of critical areas when they are interdependent.

4. Simulation results

4.1. Independent network vulnerability

To analyze the vulnerability of an independent power network to deliberate attack, we first examine how deliberate attacks affect each critical area. Based on the importance of node, the center of attack is designated to be the node with maximum degree or maximum load. Here the attack strength to the center is denoted as 1, i.e., when it is attacked, it breaks down completely. We use Eq. (4) to quantify the intensity of the attacks on the nodes connected to the attacked center node. Our performance metric is the Source-demand considered efficiency, the betweeness-based artificial flow model (AFM) is adopted, and the tolerance parameter$\alpha$is set to be 0.2 here as an example.

Attackers first aims at the community and choose the vertex with maximum degree or load in the community area as targets. This affects both the center of attack and the nodes with $\text{Attack}_{\text{node}_i}^{\text{strength}} \neq 0$ and may trigger a cascading propagation. When the power network reaches a steady state, the vertex with the recalculated maximum degree or load in the community area of the remained network is attacked. This process is continued until the critical area collapses, and whole process is repeated for ten times to determine the average results. Figs. 4 and 5 show the vulnerabilities of different critical areas as a function of attack times, with maximum degree and maximum load vertices denoted as the center of attack, respectively.

It is observed that Figs. 4 and 5 share similar variation tendency. The vulnerability curves of different attack areas increase as the attack times increase. With the increase of attack times in the critical area, more vertex fails, leading to a decrease of the performance and an increase of the vulnerability values. Note that some of the critical areas, e.g., Area-8 and 9, collapse after only a few vertices are disrupted. There are relatively small amount of nodes and edges for the Area-8 and 9, so they collapse after only a small fraction of vertices fail. These two areas are most easily to collapse, but they do not generate the most amount of vulnerability values. Breakdown of the Area-2 generate highest vulnerability to the whole system. As from Fig. 2, there are many high load nodes in this area. Failures of the high load nodes will generate a load redistribution and easily cause other nodes overload. It leads to a cascading failures and increases the vulnerabilities of the whole system.

Then, vulnerabilities of different critical areas are also acquired. The results are illustrated in Figs. 6 and 7. As from the figures, vulnerability of different critical area can be identified and compared clearly. Some areas are highly vulnerable to deliberate attacks and may collapse after a small number of attacks while disruption of some other critical areas may generate high vulnerability to the whole system. To reduce their vulnerability, these critical areas should be given prioritized protection.

We next compare and analyze the vulnerability of different critical areas under different tolerance parameters. The attack strength equals to 1. The tolerance parameter values vary with a step 0.1

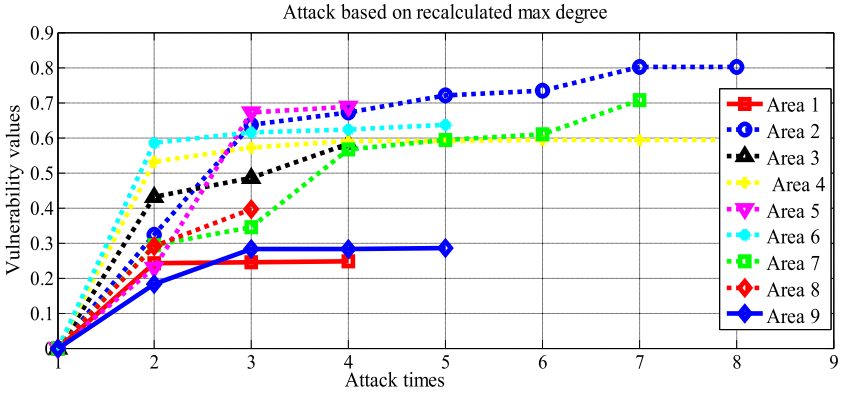

Fig. 4. Vulnerabilities produced by different areas as a function of attack times with maximum degree based center.

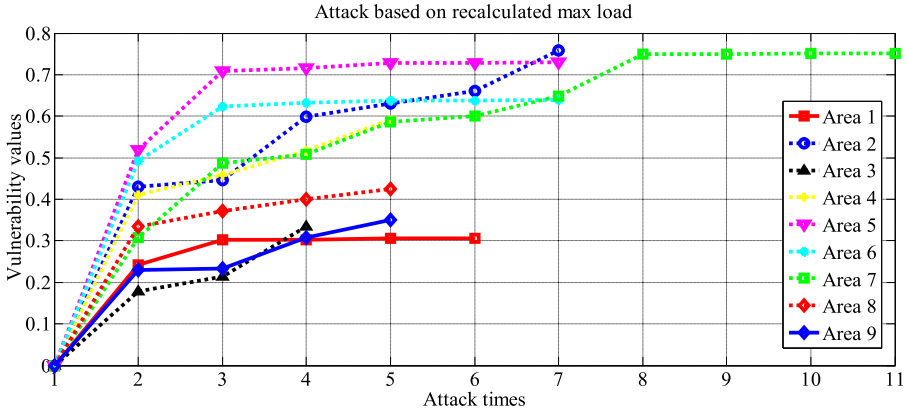

Fig. 5. Vulnerabilities produced by different areas as a function of attack times with maximum load based center.

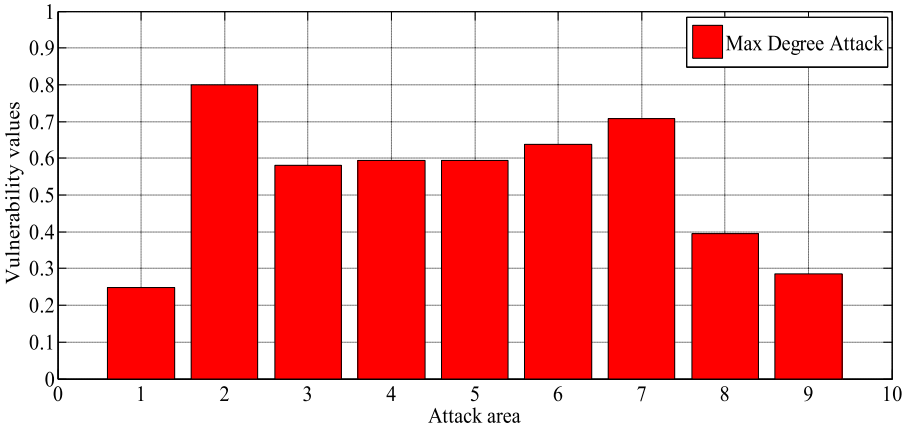

Fig. 6. Vulnerability values of different areas with maximum load based center.

from 0.1 to 0.5. The results are illustrated in Figs. 8 and 9, with maximum degree attack center and maximum load attack center respectively.

When α is low, the power network operates close to its limit state, and most of the node failures cause an overload of the other elements. The efficiency of the source-demand decreases and the vulnerability values increase. The figure shows that the values are relatively high when the tolerance parameter is low. When the tolerance parameter is high, the vulnerability values are low. The variation in the vulnerability values generated by different large tolerance parameters is very small. This is mainly because large tolerance parameters increase the capacity such that the failure of one element is less likely to overload other elements and less likely to trigger cascading failure.

4.2. Interdependent network vulnerability

The conditional probability $P(G_i^{\text{failure}}|P_j^{\text{failure}})$ is set to be 1 when analyzing interdependent vulnerability. Namely, when power nodes are unable to supply power for gas nodes, the corresponding gas node will break down. When the gas node can no longer provide fuel for generators due to failures, there is a probability that the gas-based generators may fail. We examine values of the conditional probability $P(P_t^{\text{failure}}|G_s^{\text{failure}})$ ranging from 0.2 to 0.6 with a step of 0.2.

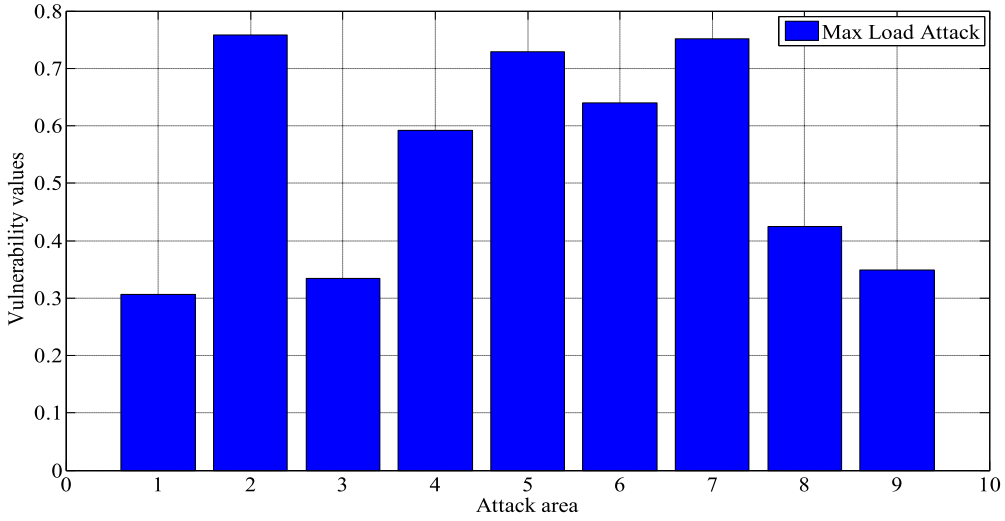

Fig. 7. Vulnerability values of different areas with maximum degree based center.

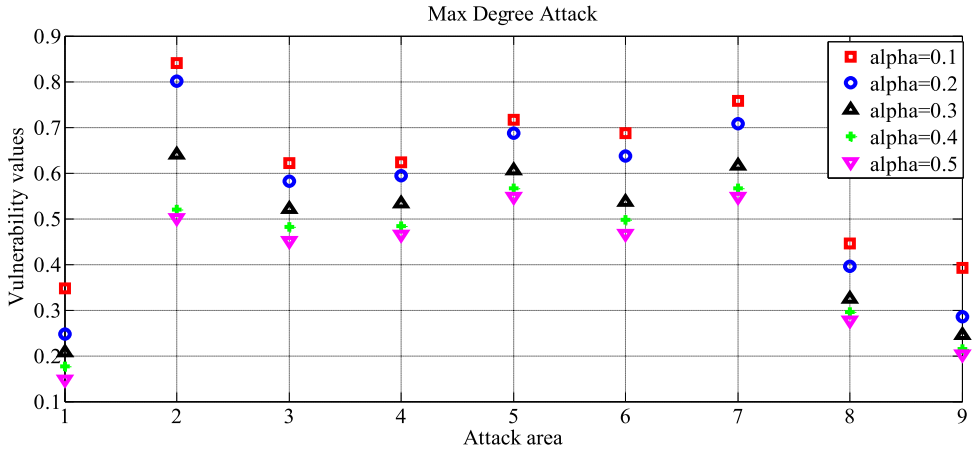

Fig. 8. Vulnerabilities of different areas under different tolerance parameter with maximum degree based center.

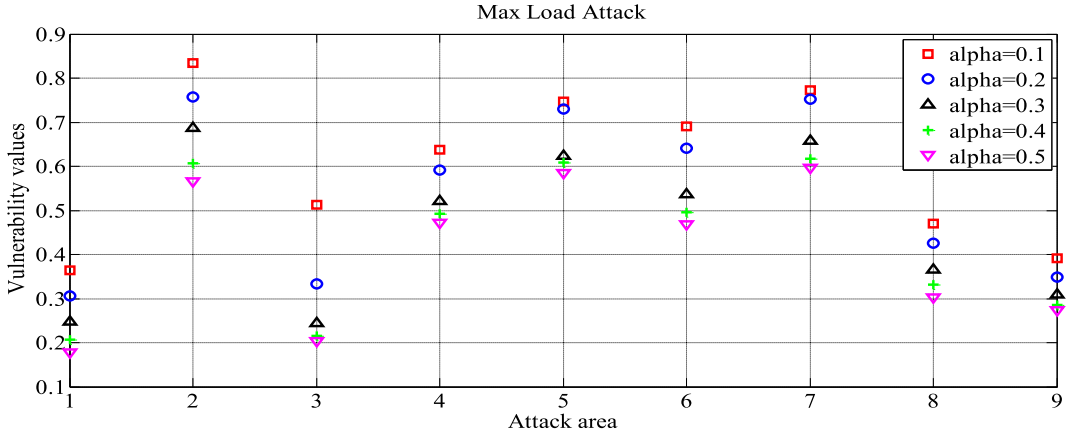

Fig. 9. Vulnerabilities of different areas under different tolerance parameter with maximum load based center.

Since gas pipelines are usually underground, we first examine the vulnerability to attack of the electrical power network. When a critical area is attacked, the load on failed nodes is reallocated according to the artificial flow model. When the load on a power component exceeds its maximum capacity, it is removed. We continue this process until the power network reaches its steady state. The cascading process is then extended to the coupled gas network and gas nodes dependent on power components fail. The damage spreads between the power and gas networks, back and forth, until they arrive at their steady state, and no more nodes and links are removed.

For simplicity, we select the vertex with the maximum degree to be the attack center, define the attack strength to be 1, and the tolerance parameter to be 0.2. Table 2 shows the attack times under different scenarios, and Table 3 shows the generated vulnerability values. We assume that there are only three gas-fired gen-

Table 2
Attack times that cause critical area collapse under different scenarios.

Cases	Area 1	Area 2	Area 3	Area 4	Area 5	Area 6	Area 7	Area 8	Area 9
Independent case	3	7	3	7	3	4	6	2	4
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.2	3	7	3	7	3	4	6	2	4
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.4	3	7	3	7	3	4	6	2	4
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.6	3	6	3	6	3	4	6	2	4

Table 3
Vulnerability values generated by the collapse of critical area under different scenarios.

Cases	Area 1	Area 2	Area 3	Area 4	Area 5	Area 6	Area 7	Area 8	Area 9
Independent case	0.248	0.801	0.581	0.594	0.687	0.637	0.707	0.395	0.285
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.2	0.257	0.821	0.584	0.616	0.687	0.639	0.718	0.395	0.295
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.4	0.259	0.833	0.589	0.629	0.692	0.646	0.733	0.395	0.309
Interdependent case with $P(P_t^{\text{failure}}\|G_s^{\text{failure}})$=0.6	0.276	0.833	0.594	0.629	0.707	0.667	0.751	0.415	0.332

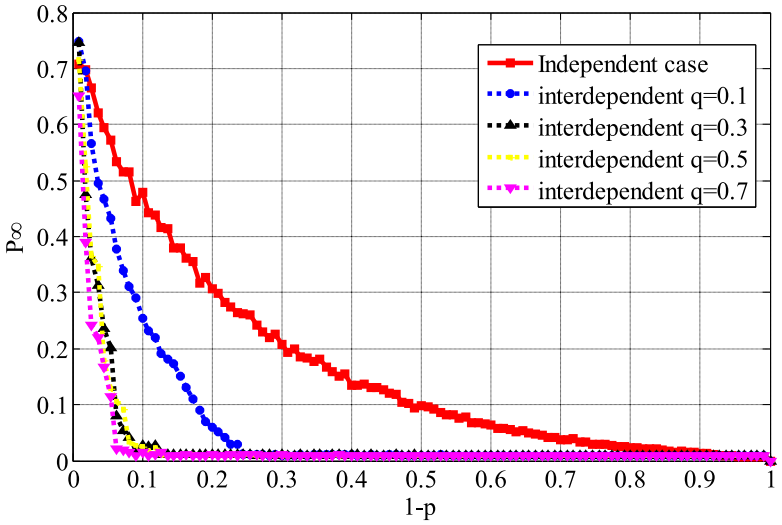

Fig. 10. Giant component as a function of 1-p under both independent and interdependent scenarios.

erators in our interdependent systems, and therefore the effect of interdependency on the attack times is not obvious. However, there are still some differences, attack times on areas 2, 4, and 9 changed under interdependent scenarios.

Table 3 also shows that the vulnerability values of areas 1, 3, 5, 7, 8, and 9 in interdependent scenarios are higher than in independent scenarios. This becomes more obvious when the conditional probability increases. Interdependency causes power network failures to spread to the gas pipeline network and, when the gas nodes affecting power production begin to fail, the failure process rebounds back to the power network, making it increasingly fragile and increasing its vulnerability. Note that in the simulation results the most vulnerable area changes when cases are interdependent. It is the area 7 under interdependent scenario while area 2 is the most vulnerable regions under independent cases. Thus, when there is a "network of networks" the system becomes more complicated.

5. Discussion

We studied the vulnerabilities under deliberate attacks from independent to interdependent scenarios in the above section. When systems are interdependent their vulnerability increases. However, it seems that the impact of interdependency on vulnerabilities is not obvious. This is probably because of the low coupling strength. In this section, we discuss how coupling strength affects systems properties. i.e., robustness. The robustness of the networks is based on the ideas of percolation theory. We characterize it by the value of the critical threshold and the integrated size of the largest connected cluster during the entire attack process.

A pair of partially interdependent networks with different coupling strength are studied. Denote the nodes of the power and gas networks as N_A and N_B, respectively. The nodes in the power network have a degree distribution $P_A(k)$, whereas the node in the gas network has the degree distribution $P_B(k)$. In addition, a fraction q_{power} of the power network nodes depend on the nodes in the gas network and a fraction q_{gas} of the gas network nodes depend on the nodes in the power network. Meanwhile, we assume that dependency satisfy a no-feedback condition.

For simplicity, it is assumed $q_{\text{power}} = q_{\text{gas}} = q$. Fig 10 gives the fraction of nodes in the mutual giant component as a function of 1-p under both independent and interdependent scenarios. It has been found from the figure that the network is relatively robust in the independent cases. Meanwhile, it is shown that interdependent networks are extremely vulnerable with a large amount of coupling strength between networks. In interdependent cases, the failure of nodes in the power network leads to the failure of dependent nodes in the gas network, which in turn may cause further damage to the power network, leading to cascading failures and catastrophic consequences. It can be seen from the figure that p_c increases with the increase of the coupling strength. The networks become more vulnerable with a large value of coupling strength. The networks collapse as in a first order when $q = 0.7$. Once the fraction of nodes increases above a cer-

tain threshold, the abrupt collapse happens to the interdependent networks.

6. Conclusion

We analyze the vulnerability of CISs under deliberate attacks, especially in interdependent systems, and we propose a method of identifying critical attack areas that uses intelligence available to terrorists. We use a fast modularity algorithm of community detection that identifies dense areas that are likely to be the target of deliberate attacks. We then use a methodological framework to examine vulnerability, including vulnerability models, vulnerability metrics, interdependency models, and patterns of deliberate attacks.

We use an interdependent infrastructure system of electrical power and gas networks to explore the vulnerability of both independent and interdependent networks to deliberate attacks. We examine and analyze the vulnerabilities of different critical areas in both independent and interdependent scenarios. We believe our model can be applied to vulnerability studies of other interdependent systems, and that it is valuable for those developing means of protecting critical infrastructures.

However, we mainly give a methodological framework to analyze vulnerability of interdependent infrastructure systems, we have used only a simple power artificial-flow model and gas generalized betweenness-centrality model. The more accurate alternative current (AC) power-flow model will better capture power grid behavior, and analyzing the effect of different interface design criteria and coupling strengths on system vulnerability will also be an interesting direction for future research.

Acknowledgments

This work is jointly supported by National Natural Science Foundations of China (No. 61503166, No. 71601030), and the Scientific Research Foundation of Chongqing Education Commission (KJ1400329). The Science and Technology Project of Xuzhou (KC16SG253).

Author contributions

Shuliang Wang designed the research and performed the experiments. H. Eugene Stanley and Yachun Gao analyzed the data and improved the method. Shuliang Wang, H. Eugene Stanley and Yachun Gao wrote the main manuscript text. All authors reviewed the manuscript.

Competing financial interests

The authors declare no competing financial interests.

References

[1] Cen N, Irene E. Adopting HLA standard for interdependency study. Reliab Eng Syst Saf 2011;96:149–59.
[2] Tao J, Barabási A-L. Control capacity and a random sampling method in exploring controllability of complex networks. Sci Rep 2013;3(1-6):02354.
[3] Vincenzo N, et al. Controlling centrality in complex networks. Sci Rep 2012;2:218.
[4] Yuan X, Hu Y, Stanley HE. Eradicating catastrophic collapse in interdependent networks via reinforced nodes. Proc Natl Acad Sci 2017:201621369.
[5] Ouyang M. Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. Reliab Eng Syst Saf 2016;154:106–16.
[6] Yehiel B, et al. Localized attacks on spatially embedded networks with dependencies. Sci Rep 2015;5(1-5):08934.
[7] Li Wei, et al. Cascading failures in interdependent lattice networks: the critical role of the length of dependency links. Phys Rev Lett 2012;108(22):228702.
[8] Wang J, Li Y, Zheng Q. Cascading load model in interdependent networks with coupled strength. Phys A: Stat Mech Appl 2015;430:242–53.
[9] Aven T. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Anal 2011;31(4):515–22.
[10] Hong L, Ouyang M, Peeta S, et al. Vulnerability assessment and mitigation for the Chinese railway system under floods. Reliab Eng Syst Saf 2015;137:58–68.
[11] Ouyang M, Zhao L, Pan Z, et al. Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks. Phys A: Stat Mech Appl 2014;403:45–53.
[12] SRA. Society of Risk Analysis, Glossary of the Specialty Group on Foundations of Risk Analysis http://www.sra.org/news/sra-develops-glossary-risk-related-terms.
[13] Enrico Z. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab Eng Syst Saf 2016;152:137–50.
[14] Rinaldi SM, Peerenboom JP, Kelley TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 2001;21(6):2–11.
[15] Earl E. Restoration of services in interdependent infrastructure systems: a network flows approach. IEEE Trans Syst Man Cybern—Part C Appl Rev 2007;37(6):1303–17.
[16] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 2014;121:43–60.
[17] Berezin Y, Bashan A, Danziger MM, et al. Localized attacks on spatially embedded networks with dependencies. Sci Rep 2015;5:8934.
[18] Brown G, Carlyle M, Salmerón J, et al. Defending critical infrastructure. Interfaces 2006;36(6):530–44.
[19] Li HJ, Wang Y, Wu LY, et al. Potts model based on a Markov process computation solves the community structure problem effectively. Phys Rev E 2012;86(1):016109.
[20] Li HJ, Daniels JJ. Social significance of community structure: statistical view. Phys Rev E 2015;91(1):012801.
[21] Wang S, Hong L, Ouyang M, et al. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. Saf Sci 2013;51(1):328–37.
[22] Ouyang M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos: Interdiscip J Nonlinear Sci 2013;23(2):023114.
[23] KalyanK S, EricJ S. UPFC-unified power flow controller: theory, modeling, and applications. IEEE Trans Power Deliv 1998;13(4):1453–60.
[24] Wang JW, Rong LL. Robustness of the western United States power grid under edge attack strategies due to cascading failures. Saf Sci 2011;49(6):807–12.
[25] Kollikkathara N, Feng H, Yu D. A system dynamic modeling approach for evaluating municipal solid waste generation, landfill capacity and related cost management issues. Waste Manag 2010;30(11):2194–203.
[26] Utne IB, Hokstad P, Vatn J. A method for risk modeling of interdependencies in critical infrastructures. Reliab Eng Syst Saf 2011;96(6):671–8.
[27] Xu W, Hong L, He L, et al. An uncertainty assessment of interdependent infrastructure systems and infrastructure sectors with natural disasters analysis. Int J Syst Syst Eng 2012;3(1):60–75.
[28] North MJ. Toward strength and stability agent-based modeling of infrastructure markets. Soc Sci Comput Rev 2001;19(3):307–23.
[29] Hong L, Yan Y, Ouyang M, et al. Vulnerability effects of passengers' intermodal transfer distance preference and subway expansion on complementary urban public transportation systems. Reliab Eng Syst Saf 2017;158:58–72.