Physica A 510 (2018) 164–177

Contents lists available at ScienceDirect

Physica A

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

An approach for cascading effects within critical infrastructure systems

Weiping Wang [a,b,c,d], Saini Yang [a,b,c,*], Fuyu Hu [e], H. Eugene Stanley [d], Shuai He [f], Mimi Shi [a,b,c]

[a] *Key Laboratory of Environmental Change and Natural Disaster, Ministry of Education, Beijing Normal University, Beijing 100875, China*
[b] *State Key Laboratory of Earth Surface Processes and Resource Ecology, Beijing Normal University, Beijing 100875, China*
[c] *Faculty of Geographical Science, Academy of Disaster Reduction and Emergency Management, Beijing Normal University, Beijing 100875, China*
[d] *Center for Polymer Studies and Department of Physics, Boston University, Boston, MA, 02215, USA*
[e] *School of Civil Engineering and Environmental Science, University of Oklahoma, Norman, OK, 73071, USA*
[f] *Institute for Disaster Management and Reconstruction, Sichuan University, Chengdu, 610207, China*

HIGHLIGHTS

- A cascading effects model considering various attack, system and cascading types.
- The damage caused by orientated local attack is similar to that of malicious attack.
- The damage to critical infrastructure system varies with cascading types.

ARTICLE INFO

Article history:
Received 31 October 2017
Received in revised form 30 April 2018
Available online xxxx

Keywords:
Cascading effect
Critical infrastructure
Interdependency
Orientated local attack

ABSTRACT

As socioeconomic systems continue to develop, their critical infrastructure systems become more intricate and the interdependencies among systems more intensive. This cascading effect on critical infrastructure systems significantly impacts system performance. We develop an approach to quantitatively assess the complex cascading effect on critical infrastructure systems under four different types of attack: (i) random, (ii) malicious, (iii) shell-based and local, and (iv) orientated and local. In the context of these four we study three types of cascading effect – non-cascading, inner-system cascading, and inter-system cascading – in both independent systems and interdependent systems. We model both logical and geographical interdependency. We apply this approach to the Chinese road and railway system and find that (i) the damage done by different types of attack on critical infrastructures systems varies significantly, (ii) under the same type of attack the damage caused by cascading effects on different critical infrastructure systems varies significantly, and (iii) different cascading effects contribute to damage in critical infrastructure systems. These findings indicate that more theoretical and practical research on cascading effects in infrastructure systems under different attacks is needed, especially when the attacks are local and oriented.

[*] Correspondence to: 19 Xinjiekou St. Haidian, Beijing, 100875, China.
E-mail addresses: wpwang90@bu.edu (W. Wang), yangsaini@bnu.edu.cn (S. Yang), hufuyu2010@gmail.com (F. Hu), hes@bu.edu (H.E. Stanley), shuaihe@scu.edu.cn (S. He), smm123@mail.bnu.edu.cn (M. Shi).

https://doi.org/10.1016/j.physa.2018.06.129
0378-4371/© 2018 Elsevier B.V. All rights reserved.

1. Introduction

Critical infrastructure (CI) is the essential physical and virtual systems(or assets) that significantly impact national security, economic security, public health, and public safety, such as electric power distribution system, transportation system and water supply system [1,2]. CIs provide the foundation for human livelihood, social and economic development, and national security. A failure or shortfall of CIs within the next ten years would have a significant international impact which would negatively affect industries, corporations, and nations [3].

Investigation of network robustness is crucial in reducing the vulnerability of CI, among which interdependency and cascading failure are two important aspects. A CI is a complex network system that is strongly interdependent. A failure in one CI system affects other interdependent CI systems, resulting in their partial or complete damage. Because interdependencies within CI systems and the frequency of their facing compromising disasters appear to be increasing [4,5], the cost of annual losses from natural disasters in the built environment alone has been estimated to be US$314 billion [6]. It is thus essential that we study the negative impact of natural hazards on interdependent CI systems.

In recent years interdependencies in CI systems have received much study. Rinaldi et al. identified four categories of CI interdependencies: physical, cyber, geographic, and logical [7]. Using these four categories, new models and methods have analyzed the cascading effects in interdependent CI under different types of attack. Johansson et al. used logical interdependency to model interdependent CI systems and to study the vulnerability of a virtual electrified railway network consisting of five subsystems [8]. Eusgeld et al. used physical interdependency to analyze the vulnerability of interdependent industrial control systems [9]. Using logical and physical interdependencies, Brummitt et al. studied the cascading of loads in random interdependent networks and an actual interdependent power grid network [10]. Dong et al. introduced logical interdependency to construct a network of networks and defined a targeted attack probability function that is dependent on the vertex degree in order to study the robustness of a network of networks under targeted attack [11]. Tan et al. used logical interdependency to extend the cascading failure model of isolated networks to study failure cascades in a data-packet transport network under intentional attack [12]. Su et al. used physical and logical interdependencies to study the robustness of interrelated Barabasi–Albert networks, Erdos–Renyi graphs, and traffic networks and focused on the subway and bus network in Beijing [13]. Using logical interdependencies among entities in multiple systems, Hong et al. modeled interdependencies, cascading failures, and restoration strategies in interdependent networks [14]. Although functional properties of infrastructures and logical and physical interdependencies among infrastructures are the focus of these studies, geographical interdependency always exists in critical infrastructures [15], such as power-oil transmission systems and road–railway transportation systems. Coupling geographical and logical interdependencies is the logical next step in the modeling of interdependent CI systems.

Different types of attack cause different patterns of damage in CI systems. Many studies have focused on random attacks [16,17] and malicious attacks [18,19]. More realistic attacks, such as natural disasters, require a different model. Researchers have recently focused on local attacks and have used a shell-based local model [20] to describe such natural disasters as earthquakes in which network nodes fail from the center to the periphery. Because this approach is not suitable for other natural disasters such as typhoons and floods in which nodes fail along some directions, we propose an orientated local attack model to depict this type of disaster.

A CI system can be represented by a network in which nodes and links respectively represent system entities and dependencies of entities. The two predominant methods used to study cascading failures in networked CI systems are (i) topology-based and (ii) flow-based. In topology-based methods of modeling CI systems each node and each link is either failed or unfailed [21]. The most frequently used topology-based method is an analytical model based on percolation theory to study cascading failures in undirected [22–25] and directed [26] interdependent networks. Flow-based methods use node and link heterogeneity to determine system flow. A betweenness-based approach [27] is widely used to model cascading failures [28–38]. Because the dynamic measure of traffic density (the ratio of occupation) is non-trivially dependent on the betweenness [39], we here use a betweenness-based model to study cascading failures in CI systems.

Although numerous models for studying the robustness and vulnerability of CI networks have been proposed [15,20,40,41], we still have no integrated approach that considers multiple factors including types of attack, network dependencies, and types of cascading effects. There has also been little research on inner-cascading effects in a single network system and inter-cascading effects in a two-network system [42].

Thus we propose using a betweenness-based model [27] to study cascading effects under various kinds of disturbance in CI systems. We classify disturbances according to the type of attack, (i) random, (ii) malicious, (iii) local and shell-based, and (iv) local and orientated. Our model considers both geographical and logical interdependencies and three types of cascading effect, (i) non-cascading, (ii) inner-system cascading, and (iii) inter-system cascading in both independent and interdependent systems. The proposed approach illustrated potentials as a quantitative analysis tool to study the cascading effects in interdependent critical infrastructure systems. Although previous work has argued that "... when networks are interdependent, this makes them even more vulnerable to abrupt failures..." [4], we find that interdependency among systems can either amplify or attenuate the damage caused by external disturbances. Our results also indicate that the possibility of orientated local attacks should be taken more seriously during the design, construction, and management of a CI system.

Table 1
Possible scenarios for failure modeling.

Types of cascading effect	System types	
	Independent	Interdependent
Non-cascading effect	*(1)*	(2)
Inner-system cascading effect	*(3)*	(4)
Inter-system cascading effect	(5)	*(6)*

2. Methodology

The four attack types defined. Different types of attack cause differing damage patterns in CI systems. Here we summarized the attack patterns of natural and man-made disasters and provide definitions and describe their implementation.
Random attack. A random attack process can be implemented using the following steps:

1. Randomly choose an entity, attack it, and remove it;
2. Repeat Step 1 until a fraction of failed entities $q(0 < q < 1)$ in the CI system has been removed.

Malicious attack. A malicious attack can be implemented using the following steps:

1. Choose the entity that has the highest betweenness value, attack it, and remove it;
2. Repeat Step 1 until a fraction of failed entities $q(0 < q < 1)$ in the CI system has been removed.

Shell-based local attack. A shell-based local attack can be implemented using the following steps:

1. Randomly choose an entity r as a root, attack it, then queue it as $L = r$;
2. When L is not empty:
   (a) Choose an entity v from the front of queue L and attack it;
   (b) Mark each unmarked neighbor w of v in the CI system and add it to end of queue L.
3. Stop this process when a fraction of failed entities $q(0 < q < 1)$ in the CI system has been removed.

Orientated local attack. An orientated local attack can be implemented using the following steps:

1. Randomly choose an entity as a root node;
2. Attack p entities that are adjacent to the root node;
3. Randomly choose $p1$ from the attacked entities in Step 2 as a root node;
4. Repeat Steps 2 and 3 until a fraction of failed entities $q(0 < q < 1)$ in the CI system has been removed.

Interdependency types. The state of geographically interdependent entities changes when there is a local environmental event [7]. We use a dual approach to constructing the road and railway network based on geographical interdependencies [43], i.e., when we construct the Chinese road and railway network system we designate road and railway segments to be network nodes and road and railway intersections to be network links.

There is a mechanism in logical interdependency entities [7]. We use logical interdependencies between road and railway networks to bridge the two infrastructure systems. In real-world scenarios, travelers often use a road to reach a railway station and then the railway to reach another railway station. The railway station is the vital connection point between the rail and road systems. We abstract this logical interdependency by using the railway station as a bridge in which road segments and railway segments that connect to the same railway station interact with each other. Fig. 3 shows, for example that road segments 1157 and 1657 directly connect to the railway station, and that railway segments 10, 220, 229, and 230 directly connect to the same railway station. Here we show the logical interdependency: road segments 1157 and 1657 interact with railway segments 10, 220, 229, and 230. Fig. 1 shows all the abstracted interdependencies in the Chinese road and railway coupled system.

Modeling failures in different CI systems. We have focused on the damage of cascading effects in infrastructure systems. Infrastructure systems can be independent, but they also can be interdependent, such as in power and petroleum transmission systems [15], power and Internet systems [41], and road and railway transportation systems. We classify critical infrastructure systems as either independent or interdependent. Attacks can cause cascading effects bring about partial or total system failure [27]. In addition, an entity failure in one system can cause a cascading effect and a failure of dependent entities in other systems [42]. We classify cascading effects as either inner-system or inter-system. Table 1 shows the six possible scenarios, among which we select three for further failure modeling (bold italics). Without inter-system cascading, the failure patterns of interdependent and interdependent systems are the same. Thus we focus on the damage of cascading effect in scenarios (1) and (3). Because there are no inter-system cascading effects in independent CI systems, we model the failure pattern of scenario (6) to uncover the damage effect in coupled CI systems.

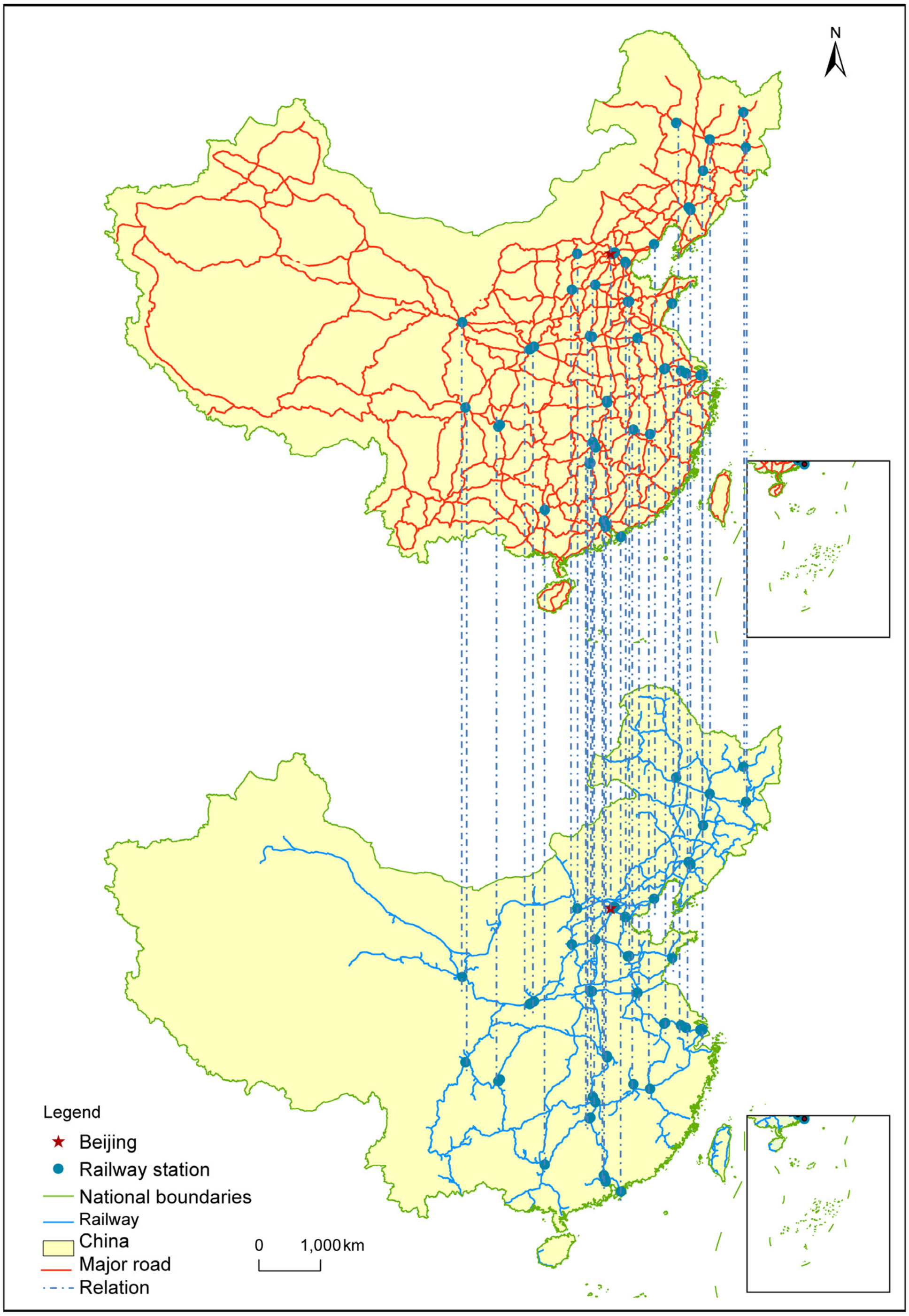

Fig. 1. The schematic depiction of the layered Chinese road–railway system. The map is drawn using ArcGIS 10.1 (http://www.esri.com/software/arcgis/arcgis-for-desktop).

Modeling failures in independent critical infrastructure systems without cascading effects.

In scenario (1) in Table 1, the entities of the system are independent, so the failure of one entity does not cause others to fail, and the failure process in this system under an attack can be implemented as follows:

At the initial stage $i = 0$, all n entities are functioning. When an attack D is imposed on any entity, it fails.

Modeling failures in independent critical infrastructure systems with cascading effects.

In scenario (3) in Table 1, we consider only the inner-system cascading effect. Entities of a critical infrastructure are interdependent and their failure causes the failure of other entities. Abstracting entities to nodes and links among entities to edges, we have a network N that represents a CI system. An attack D is imposed on some system entities. Using the procedure for modeling failures in independent critical infrastructure systems without cascading effects, obtain the set of failed entities N_f. The failure process in this system under an attack can be implemented as follows:

1. First set all n entities initially with capacity $C_j(j = 1, 2, \dots, n)$. The capacity of an entity is the maximum load that the entity can manage. Thus the capacity of C_j of entity j is proportional to its initial load and capacity C_j can be calculated [27,44] as

$$C_j = (1 + \alpha)B_j, \tag{1}$$

   where α is a tolerance parameter and B_j is the betweenness of network entity j. When all the entities are functional, the system operates normally in so far as $\alpha \geq 0$.
2. Remove N_f from the system, and recalculate the betweenness B_k of entity k in the remaining set of system entities $N_r = N - N_f$. For each entity k in N_r, when $B_k > C_k$ entity k fails and is added to N_f.
3. Repeat step 2 until N_r no longer changes. Denote the unchanging removed entities N_f to be $\hat{N}_f$, where $\hat{N}_f$ is the set of final failed entities in the system under attack D.

Modeling failures in an interdependent CI system with cascading effects.

A CI system is a complex network system in which there is both strong entity dependency and interdependency among CI systems. When a CI entity, such as a transport system, is attacked, the negative impact spreads to other entities within the system and to other infrastructure systems, such as energy or economic systems. Thus in this model we consider both inner-system cascading effects and inter-system cascading effects.

Without losing generality, we consider an interdependent infrastructure system composed of systems A and B. By treating the basis entities of a critical infrastructure (e.g. intersections, stations) as nodes and links among entities as edges, we build a complex network N to represent the interdependent infrastructure system. The failure process in N under an attack can be implemented as follows:

1. We first model the interdependency between infrastructure systems. This interdependency causes some nodes n_B in system B to depend on nodes n_A in system A. We add n_B and those links connecting n_B and n_A into A to expand system A to A_p. Similarly we expand system B to B_p.
2. We impose an attack D on some entities in systems A_p and B_p. Using the procedure for modeling failures in independent CI systems without cascading effects, we determine which entities have failed and assign them to set N_{f,A_p} and N_{f,B_p}. Let $N_{f,A} = N_A \cap N_{f,A_p}$ and $N_{f,B} = N_B \cap N_{f,B_p}$.
3. We remove $N_{f,A}$ and $N_{f,B}$ from system A_p and B_p, respectively. Using the procedure for modeling failures in independent CI systems with cascading effects, we calculate $\hat{N}_{f,A_p}$, $\hat{N}_{f,B_p}$ and $\hat{N}_{r,A_p}$, $\hat{N}_{r,B_p}$. Here $\hat{N}_{f,A_p}$ is the set of failed entities in system A_p, and $\hat{N}_{r,A_p}$ is the set of functional entities in system A_p.
4. Let $N_{f,A} = N_A \cap \hat{N}_{f,B_p} \cap \hat{N}_{r,A_p}$, $N_{f,B} = N_B \cap \hat{N}_{f,A_p} \cap \hat{N}_{r,B_p}$, $N_{A_p} = \hat{N}_{r,A_p}$, $N_{B_p} = \hat{N}_{r,B_p}$, $N_{f,A_p} = N_{f,A_p} \cup \hat{N}_{f,A_p}$ and $N_{f,B_p} = N_{f,B_p} \cup \hat{N}_{f,B_p}$.
5. Repeat Steps 3 and 4 until N_{f,A_p} and N_{f,B_p} no longer change. Denote the unchanging removed entities N_{f,A_p} and N_{f,B_p} to be $\tilde{N}_{f,A_p}$ and $\tilde{N}_{f,B_p}$, respectively. In the final stage $\tilde{N}_{f,A_p} \cap N_A$ and $\tilde{N}_{f,B_p} \cap N_B$ are the set of failed entities in system A and B, respectively, under attack D.

Functional measurements of CI systems. *The fraction of the functional entities*

When a CI system is attacked, some system entities malfunction or fail. The fraction of the functional entities (FF) at time t[14] is

$$FF = \frac{|N_t|}{|N|}, \tag{2}$$

where N is the total set of entities in a CI system and N_t is the set of functional entities in a CI system under an attack at time t.

The fraction of the entities in the giant component

Based on percolation theory, only entities in the giant component of the attacked system remain functional [41]. The fraction of the entities in the giant component (FG) at time t is

$$FF = \frac{|G_t|}{|N|}, \tag{3}$$

where G_i is the set of entities that belong to the giant component under an attack at time t.

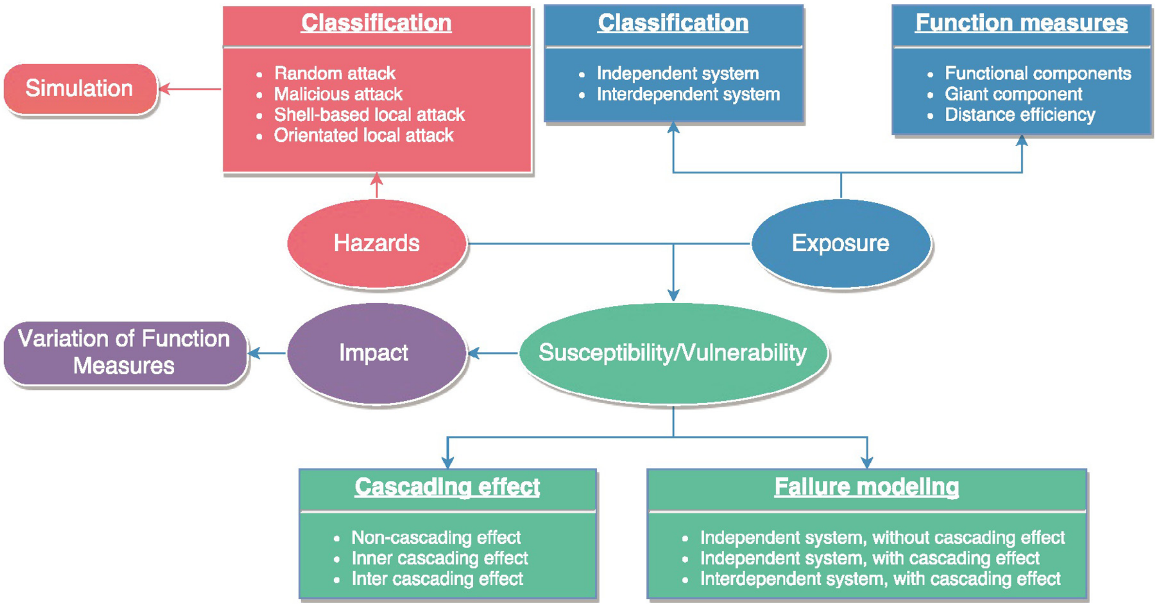

Fig. 2. The framework of the proposed approach.

Distance efficiency

Here we use distance efficiency (DE) to assess the functional efficiency of a CI system [45]. The DE is the average inverse distance between any two system entities. The weight of a system link is the distance. If entities i and j are connected, d_{ij} is the shortest distance between i and j. If they are not connected, d_{ij} is infinite, i.e,

$$d_{i,j} = \begin{cases} \sum\limits_{i,j \in e_{i,j}}, \ if\ C_{ij} = 1 \\ \infty, \ if\ C_{ij} = 0 \end{cases}, \tag{4}$$

where P_{ij} is the shortest path that connects i and j, and e_{ij} is the physical length of the path directly connecting i and j. We use the Dijkstra algorithm [46] to obtain the shortest distance between any two entities.

The DE_t of the critical infrastructure system under an attack at time t is

$$DE_t = \frac{\sum_{i \notin N_t, i \neq j} \sum_{j \in N_t} \frac{1}{d_{ij,t}}}{\mathrm{NDE}}, \tag{5}$$

where NDE is the normalized distance efficiency of a CI system not under attack.

3. Results

In our integrated approach to analyzing complex cascading effects in CI systems, we firstly classify the damage patterns of attacks (external disturbances) into four groups and simulate the process of each type of attack. We then classify CI systems as either independent or interdependent and cascading effects as either inner-system or inter-system. Three different scenarios of CI system and cascading effect are modeled to measure the damage to each CI system under attack. Finally we use three systematic characteristic measurements to assess the damage to CI systems caused by each attack and each subsequent cascading effect. Fig. 2 shows the framework of our proposed approach.

Disaster occurs when a CI system is exposed to a hazard and its vulnerability is such that it cannot reduce the potential negative consequences [47]. Thus we analyze the damage of cascading effects on CI systems, taking into account hazards, exposure, and vulnerability.

We classify attacks as either (i) random [16,17], malicious, local and shell-based [20] (e.g., earthquakes), or local and orientated (e.g., tropical storms) [19]. Random attacks are hazards that affect several random entities in a CI system (e.g., collapsing and falling stones) and correspond to the random attacks modeled in complex network science [16,17]. Malicious attacks damage important entities in a CI system [18,19] (e.g., terrorist attacks). Shell-based attacks destroy all CI entities in a certain area. They start from a root node, advance through nearest neighbors, and spread outward (e.g., earthquakes) [19,20]. Previous studies have produced models of random, malicious, and local shell-based attack patterns, but have ignored the more dynamic orientated local attack.

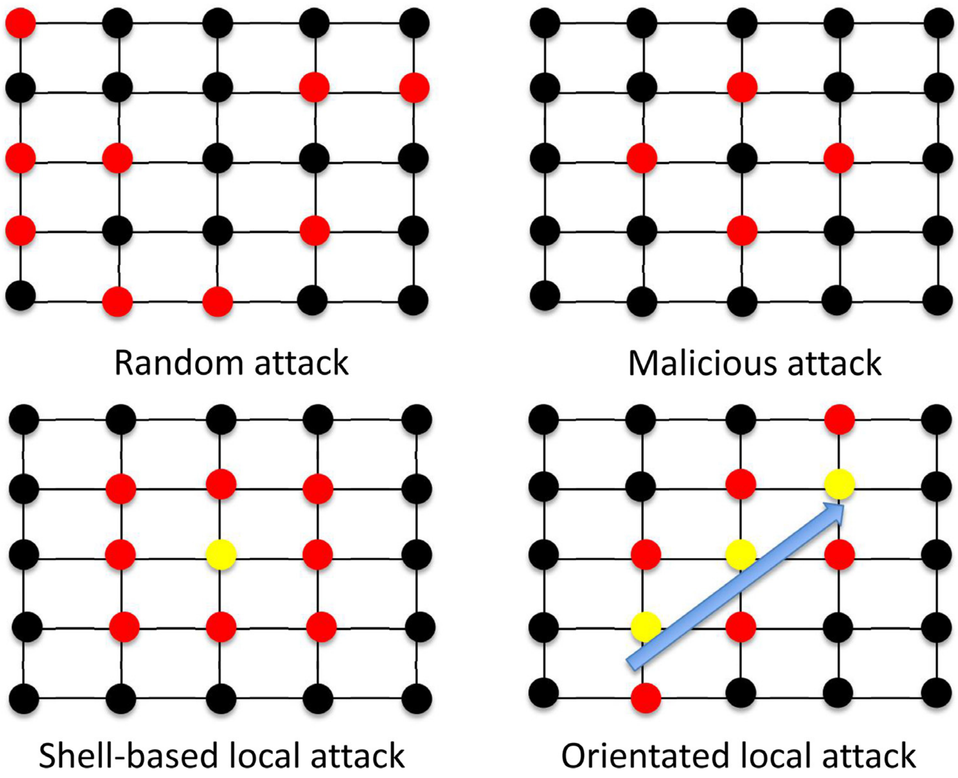

Fig. 3. The schematic depiction of the lattice network under four types of attacks. The black points denote the functional nodes, red points are the failed nodes, yellow points denote the root nodes and the blue arrow denotes orientation. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

An orientated local attack destroys all CI in a certain area and its damage is oriented, i.e., the attacked entities fall into a path and become a trajectory (e.g., floods and typhoons) [45]. Using the literature [16,17,20] and the implementation steps described in Methods, we produce the schematic patterns of random, malicious, local and shell-based, and local and orientated attacks. The schematic depiction of the lattice network under four types of attacks is shown in Fig. 3.

Turning to exposure, we classify CI systems as either independent and not interacting with other systems, or interdependent and interacting with other systems. We use three measurements of exposure function, (i) the fraction of functional entities (FF), the fraction of entities in the giant component (FG), and the distance efficiency (DE). An attack can lead to a cascading effect that causes either partial or complete system failure [27]. The failure of entities in one system can initiate a cascading effect that causes the failure of dependent entities in other systems [41]. Thus we classify cascading effects as either inner-system or inter-system, which in different types of system results in different patterns of failure when attacked. Using the three types of coupled cascading effects and systems, we measure vulnerability by constructing the three failure models described in Methods. Using a variety of measurements of system functionality reveals the cascading effects in CI systems.

Study area. We couple the geographical and logical interdependencies to study the damage of cascading effects on the Chinese road and railway system. Our GIS data of roads and railways is from the National Geomatics Center of China [http://www.ngcc.cn/]. There are 1742 major road segments and 504 major railway segments in this dataset. A schematic depiction of the interdependency in a layered Chinese road–railway system is shown in Fig. 4.

The critical infrastructure damage under different types of attack. To quantify the critical infrastructure damage under four different types of attack, we use the failure model of independent CI systems that disregards cascading effects and parameter settings in Table 2 to study damage to the Chinese road and railway network. Fig. 5 shows the damage to the Chinese road and railway system under the four attack types using the failure model of Scenario (1) in Table 1. We find that the damage pattern varies according to type of attack. The shell-based local attack caused the least damage to the road and railway infrastructure network, and the orientated local attack caused greater damage than that of a shell-based local attack. This is because an orientated local attack tends to divide the network into sub-networks, which is not the case in shell-based local attacks and random attacks.

The damage in different types of CI. Because there has been little research on the orientated local attack on CI systems, the type of attack that causes the most damage, we here make it the focus of our analysis. With the parameter settings in Table 2, the

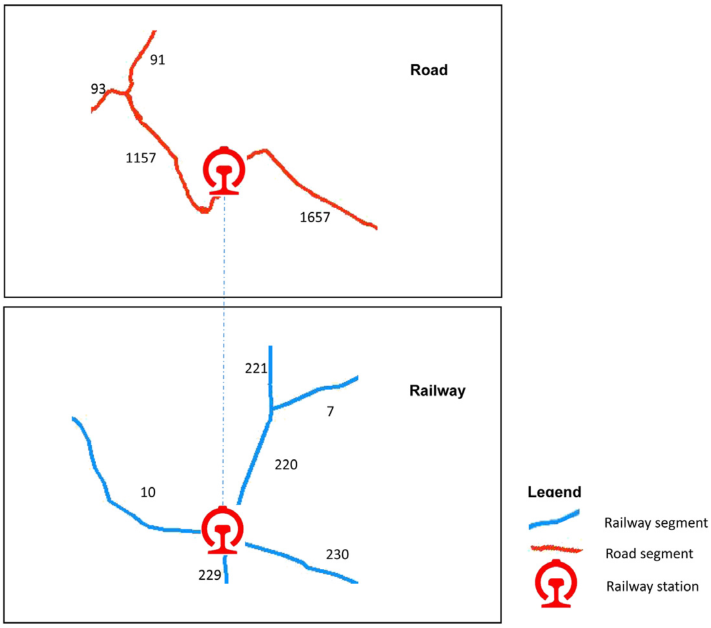

Fig. 4. A schematic depiction of the interdependency in a layered Chinese road–railway system. The 1157th and 1657th road segments connect with the railway station in the road system and the 10th, 220th, 229th and 230th railway segments connect with the same railway station in the railway system. According the interdependencies, the 1157th and 1657th road segments are interdependent with the 10th, 220th, 229th and 230th railway segments.

Table 2
Parameters in simulation.

Variable	Description	Road	Railway
α	Tolerance parameter	0.1	0.1
q	A fraction of attacked entities	(0.05,1)	(0.05,1)
T	The number of runs	100	100
$V(N)$	The number of nodes in network	1742	504
$E(N)$	The number of edges in network	3308	911

damage of Chinese road–railway network under orientated local attack is illustrated in Fig. 6. The red line shows the damage with failure models in scenario (3) (independent system with inner-system cascading effect) and the blue line shows the damage in scenario (6) (interdependent system with inter-system cascading effect).

The Chinese road network has 1704 nodes, and its degree distribution obeys a negative exponential distribution. Fig. 7(b) shows the frequency of the Chinese road network degree, $R^2 = 0.97$. We apply an orientated local attack to study the damage in different types of CI. The Chinese railway network has 504 nodes, and its degree distribution does not obey the negative exponential distribution. Fig. 7(d) shows the frequency of the Chinese railway network degree, $R^2 = 0.01$.

We examined the interdependency in the Chinese road–railway coupled network by focusing on railway nodes that interact with road nodes and road nodes that interact with railway nodes. Fig. 7(a, c) show the degree frequencies of the Chinese road and Chinese railway networks. Fig. 6 shows the functional measurements of Chinese road network and railway network after an orientated local attack. We see a phase-transition occur between damage amplification (where the blue line is below the red line, e.g., the 0.1 attack rate) and damage reduction (where the red line is below the blue line, e.g., the 0.5 attack rate). In the Chinese road system, however, we find only the damage reduction phase (the red line remains below the blue line). Fig. 7(a, b) and Fig. 8(a, b) show that the Chinese road network degree distribution obeys the negative exponential distribution $R^2 > 0.9$. From Fig. 7(d) and Fig. 8(d) to Fig. 7(c) and Fig. 8(c) we see the Chinese railway network degree distribution change from a non-negative exponential distribution ($R^2 < 0.3$) to an exponential distribution ($R^2 > 0.9$). Thus the degree distribution and network size of the Chinese road network differs from those of the Chinese railway network. Combining these finding with Fig. 6 we conjecture that the differences in CI systems strongly affect damage levels, and that damage amplification and reduction are strongly affected by levels of interdependency and degree distribution.

The damage in CI systems is shaped by the type of cascading effect. The level of interdependency within the Chinese railway system significantly impacts the level of damage. To avoid the impact of interdependency when studying the level of damage

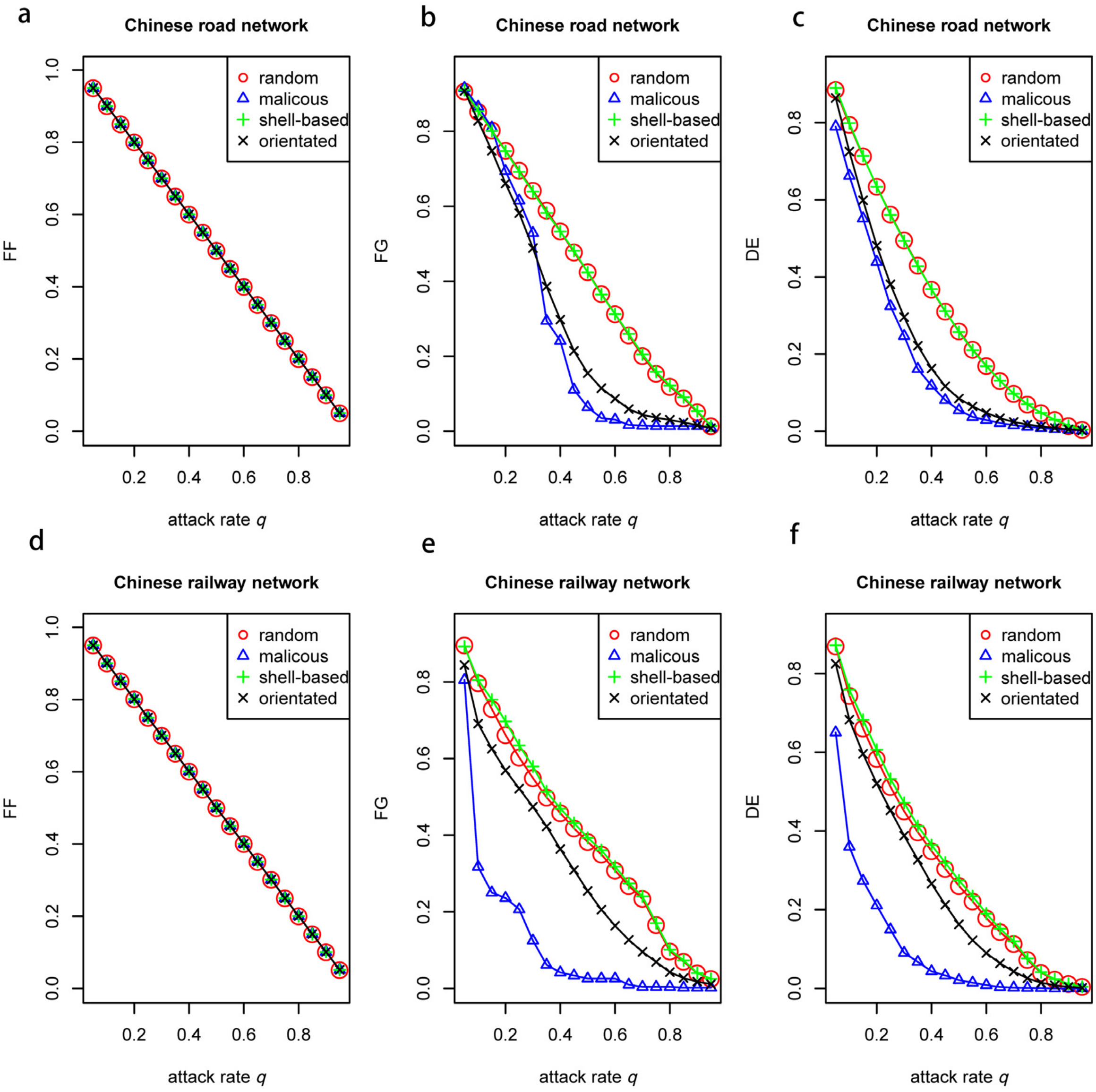

Fig. 5. The Chinese road–railway network damage under different types of attacks using the failure model in section that modeling failures in independent critical infrastructure systems without cascading effects as described in Methods. The symbols ○, △, + and ×, respectively, indicate the random attacks, malicious attacks, shell-based local attacks and orientated local attacks; (a) variations in the values of the fraction of the functional entities (FF) in the Chinese road network by attack rates; (b) variations in the values of the fraction of the entities (FG) in the giant component in the Chinese road network by attack rates; (c) variations in the values of the Chinese road network distance efficiency (DE) by attack rates; (d) variations in the values of the fraction of the functional entities (FF) in the Chinese railway network by attack rates; (e) variations in the values of the fraction of the entities (FG) in the giant component in the Chinese railway network by attack rates; and (f) variations in the values of the Chinese railway network distance efficiency (DE) by attack rates. Simulation results are the outcome averages of 100 independent runs.

to a CI under different types of attack, we simulate three failure models under different coupled attacks and cascading effects with parameter settings in Table 2. Fig. 9 shows the results.

When the attack rate is low, the ratio of removed entities in the system induces their flow and distribution to other systems. It is the betweenness of the removed entities increase that leads to a cascading overload failure. In contrast, a high attack rate removes many entities from the system, which decreases network traffic flow and entity betweenness with fewer cascading failures and higher FF, FG and DE values than those when the attack rate is low. Thus Fig. 9(d)–9(i) show non-monotonic decreasing curves.

Fig. 9 shows that damage in critical infrastructure reaches different levels under different coupled attacks and cascading effects. Fig. 9(a, b, c) show coupled non-cascading effects with four types of attack in which the damage effects differ according to type of attack. Fig. 9(d, e, f) show coupled inner-system cascading effects with four types of attack in which

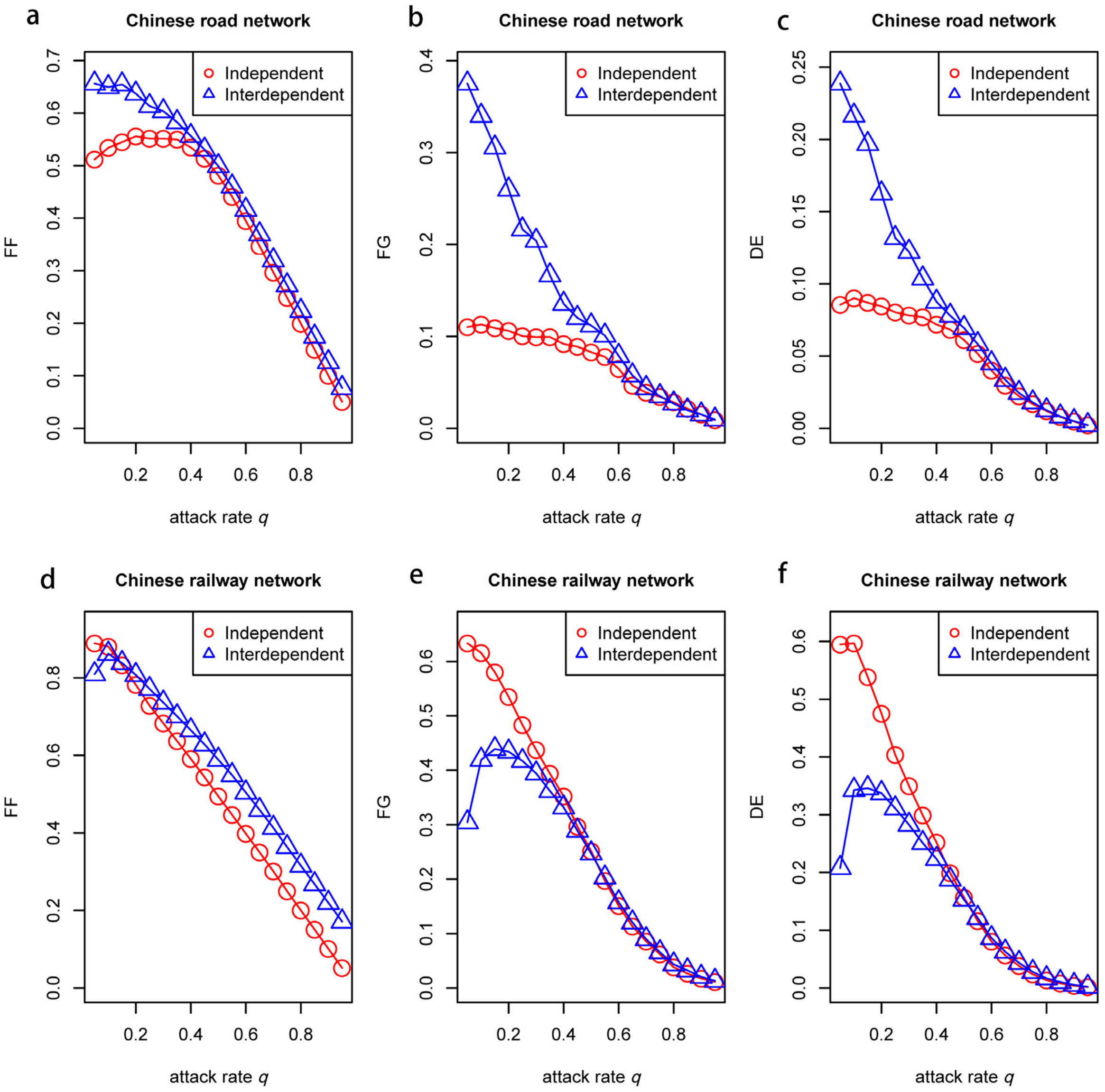

Fig. 6. The Chinese road–railway network damage under orientated local attack using the failure models in section that modeling failures in independent critical infrastructure systems with cascading effects (red line) and section that modeling failures in interdependent critical infrastructures system with cascading effects (blue line) as described in Methodology. (a) Value variations of the fraction of the functional entities (FF) in the Chinese road network by attack rates; (b) value variations of the fraction of the entities (FG) in the giant component in the Chinese road network by attack rates; (c) value variations of the Chinese road network distance efficiency (DE) by attack rates; (d) value variations of the fraction of the functional entities (FF) in the Chinese railway network by attack rates; (e) value variations of the fraction of the entities (FG) in the giant component in the Chinese railway network by attack rates; and (f) value variations of the Chinese railway network distance efficiency (DE) by attack rates. Simulation results are the outcome averages of 100 independent runs. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the damage effects again differ according to type of attack. Fig. 9(g, h, i) show both coupled inner-system and inter-system cascading effects with four types of attacks in which the damage effects once again differ according to type of attack.

Comparing Fig. 9(d, e, f) with Fig. 9(g, h, i) we find that inner cascading effects in the system cause the maximum damage. Comparing Fig. 9(a, b, c)(disregarding the cascading effect) with Fig. 9(d, e, f) (taking the cascading effect into account) we find that in Fig. 9(d, e, f, g, h, i) the FG and DE are much smaller than the FF. Because cascading can cause entity overload anywhere in the system and divide the network into subnetworks, which causes low FG and DE values.

We find that although the damage effect of a random attack approximates that of a shell-based local attack, in Fig. 9(b) the damage is greater than the damage of the shell-based local attack shown in Fig. 9(e, h). Under the four types of attack,

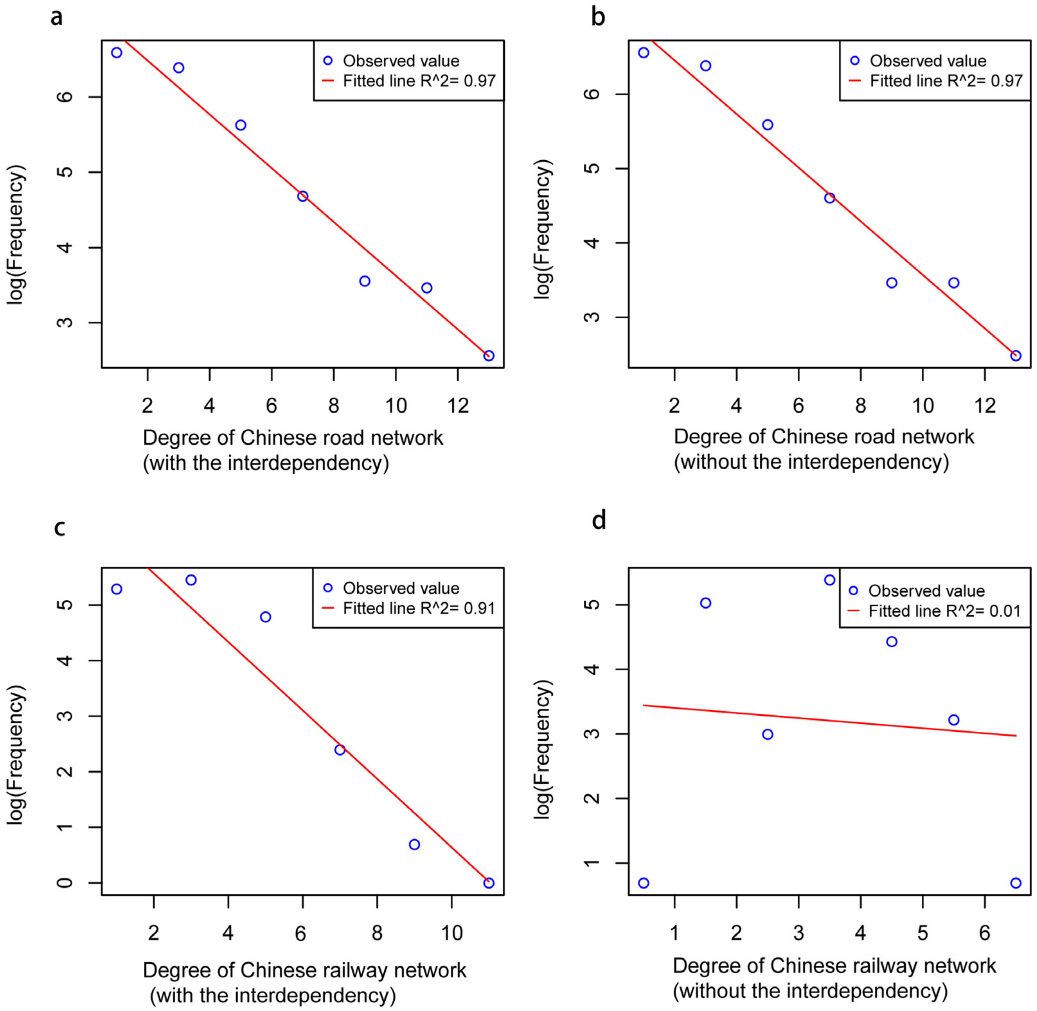

Fig. 7. The frequency of Chinese road and railway network degree. (a) Degree frequency of Chinese road network with the interdependency; (b) Degree frequency of Chinese road network without the interdependency; (c) Degree frequency of Chinese railway network with the interdependency; and (d) Degree frequency of Chinese railway network without the interdependency. The red line represents the fitted linear regression line. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the damage effect in Fig. 9(b, e, h) is different in each case. Thus we conclude that in CI systems differing cascading effects cause differing damage effects.

4. Conclusion

We have proposed a new approach to investigating the cascading effects of hazards in CI systems. By simulating four types of attack – random, malicious, local and shell-based, and local and orientated – with two types of exposure – independent and interdependent – and two types of cascading—inner-system and inter-system, we modeled the failures under three scenarios, (i) independent infrastructures system without cascading effects, (ii) independent infrastructure systems with inner-system cascading effects, and (iii) interdependent infrastructures system with both inner-system and inter-system cascading. We applied this approach in Chinese road and rail networks. Our simulation results indicated that: (1) The damage caused by different types of attack varies significantly. A shell-based local attack causes the least damage in the road and railway infrastructure network, and the damage caused by an orientated local attack is similar to that caused by a malicious attack. (2) Differences in CI system can cause differing degrees of damage when the attacks are of the same type. (3) Different cascading effects also cause differing damage degrees in CI systems. Coupling inner-system and inter-system cascading effects in all four types of attack, the damage pattern of random attacks is approach to that of a shell-based local attack.

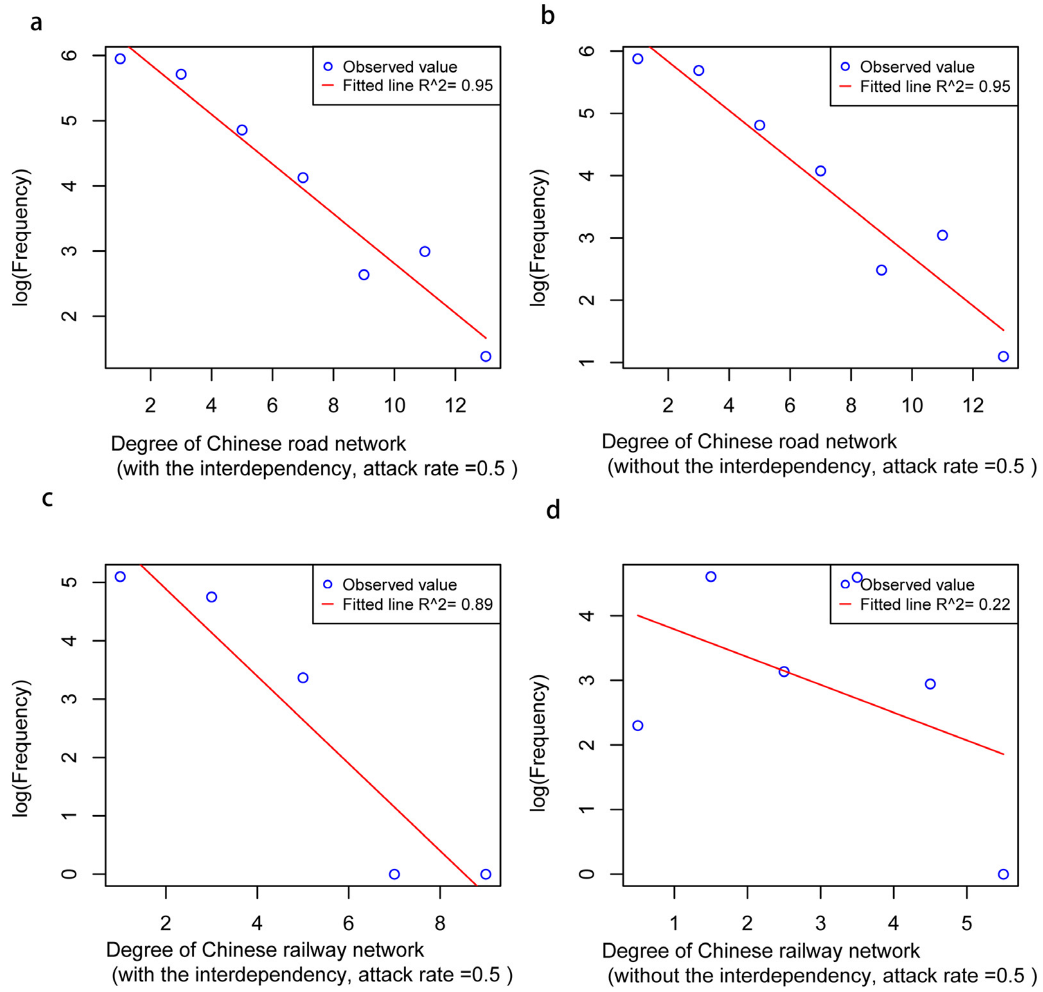

Fig. 8. The frequency of Chinese road and railway network degree when the attack rate is 0.5. (a) Degree frequency of Chinese road network with the interdependency; (b) Degree frequency of Chinese road network without the interdependency; (c) Degree frequency of Chinese railway network with the interdependency; and (d) Degree frequency of Chinese railway network without the interdependency. The red line represents the fitted linear regression line. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

(4) More attention should be paid to orientated local attacks when designing, constructing, and managing CI systems, and further theoretical research on infrastructure risk assessment under orientated local attacks is needed.

Proposed approach also can be extended into criticality identification and risk analysis or management, which are essential in decision-making when designing operation schemes and disaster risk reduction strategies for CI systems. Limitation of this study is we considered only the betweenness-based model when constructed failure model. In real-world CI systems such as transportation networks, however, the dynamic traffic flow in an entity is the key factor of their functioning. Future studies modeling system failure could take dynamic flow calculated in real time rather than betweenness into consideration. Our definitions and the implementation of attacks are related to topological network properties. Future improvement will focus on better definition and implementation of dynamic attacks by studying the geographic properties of networks. Well-defined and better implemented attacks will enable us to better explore and discover the driven factors associated with damage in CI systems.

Acknowledgments

This study was supported by the National Key Program of China (No. 2016YFA0602403), the fund for Creative Research Groups of the National Natural Science Foundation of China (No.41321001), scholarship from China Scholarship Council (CSC.201606040133), Chengdu Science and Technology Bureau, China (2015-HM01-00564-SF), and the ICCR-DRR at BNU. We also thank the reviewers for their valuable suggestions to improve the paper.

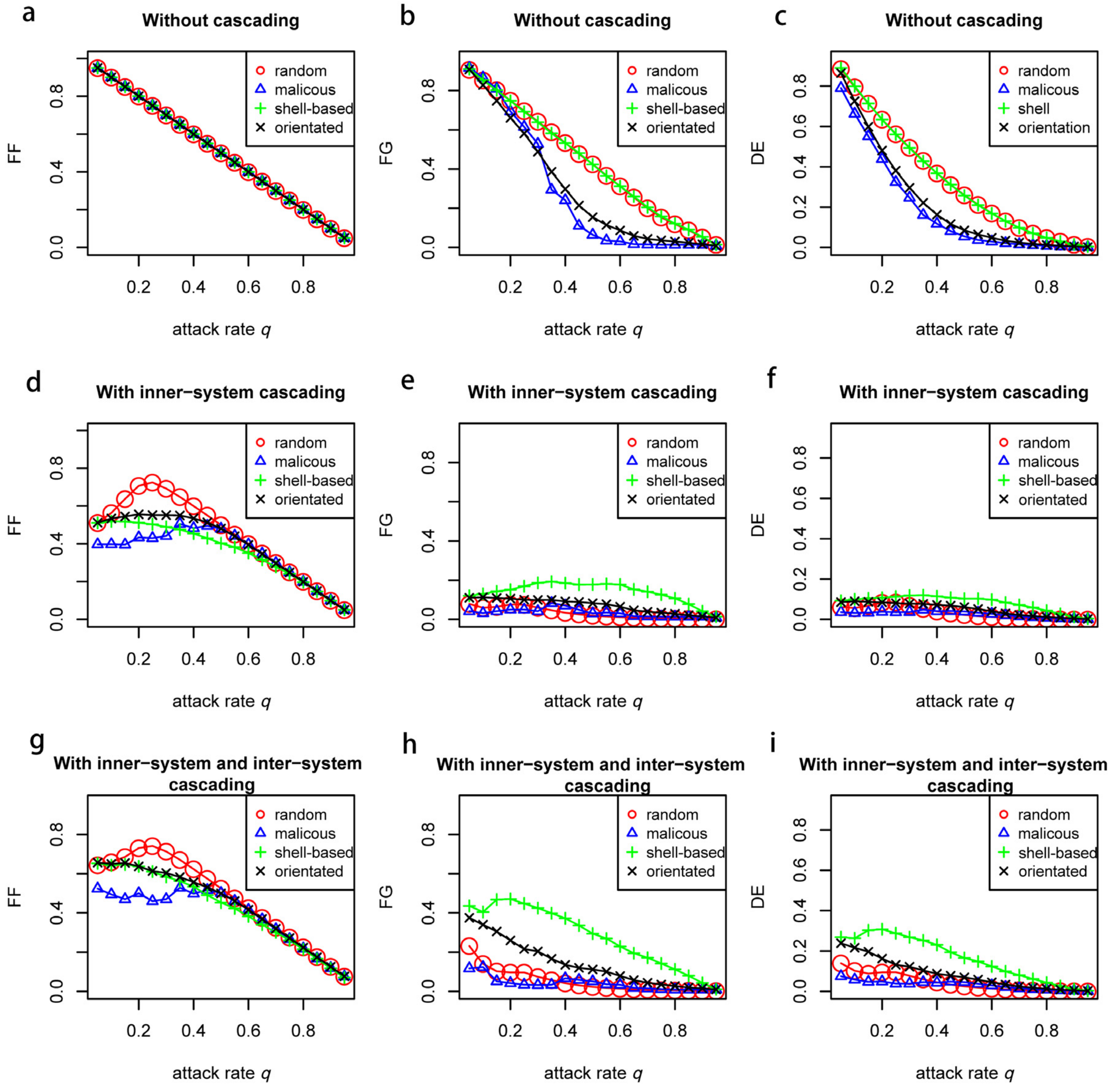

Fig. 9. The Chinese road network damage under different types of attack using the three different failure models as described in Methodology. The symbols ∘, △, + and ×, respectively, indicate the random attacks, malicious attacks, shell-based local attacks and orientated local attacks; (a), (b) and (c) respectively indicate the variations of FF, FG and DE in the Chinese road network by attack rates, starting from $q = 0.05$ with an increment of 0.05, and using the failure model in section that modeling failures in independent critical infrastructure systems without cascading effects;(d), (e) and (f) respectively indicate the variations of FF, FG and DE in the Chinese road network by attack rates q, starting from $q = 0.05$ with an increment of 0.05, and using the failure model in section that modeling failures in independent critical infrastructure systems with cascading effects; (g), (h) and (i) respectively indicate the variations of FF, FG and DE in the Chinese road network by attack rates and using the failure model in section that modeling failures in interdependent critical infrastructures system with cascading effects. Simulation results are the outcome averages of 100 independent runs.

References

[1] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security, 2013.

[2] G. Brown, M. Carlyle, J. Salmerón, K. Wood, Defending critical infrastructure, Interfaces 36 (6) (2006) 530–544.

[3] The Global Risks Report 2016, 11th ed., World Economic Forum, 2016.

[4] D. Helbing, Globally networked risks and how to respond, Nature 497 (7447) (2013) 51–59.

[5] Sendai framework for disaster risk reduction 2015-2030, United Nations International Strategy for Disaster Reduction, 2015.

[6] Global assessment report on disaster risk reduction 2015, United Nations International Strategy for Disaster Reduction, 2015.

[7] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Syst. 21 (6) (2001) 11–25.

[8] J. Johansson, H. Hassel, An approach for modelling interdependent infrastructures in the context of vulnerability analysis, Reliab. Eng. Syst. Saf. 95 (12) (2010) 1335–1344.

[9] I. Eusgeld, C. Nan, S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, Reliab. Eng. Syst. Saf. 96 (6) (2011) 679–686.

[10] C.D. Brummitt, R.M. DSouza, E. Leicht, Suppressing cascades of load in interdependent networks, Proc. Natl. Acad. Sci. 109 (12) (2012) E680–E689.
[11] G. Dong, J. Gao, R. Du, L. Tian, H.E. Stanley, S. Havlin, Robustness of network of networks under targeted attack, Phys. Rev. E 87 (5) (2013) 052804.
[12] F. Tan, Y. Xia, W. Zhang, X. Jin, Cascading failures of loads in interconnected networks under intentional attack, Europhys. Lett. 102 (2) (2013) 28009.
[13] Z. Su, L. Li, H. Peng, J. Kurths, J. Xiao, Y. Yang, Robustness of interrelated traffic networks to cascading failures, Sci. Rep. 4 (2014).
[14] S. Hong, C. Lv, T. Zhao, B. Wang, J. Wang, J. Zhu, Cascading failure analysis and restoration strategy in an interdependent network, J. Phys. A 49 (19) (2016) 195101.
[15] B. Wu, A. Tang, J. Wu, Modeling cascading failures in interdependent infrastructures under terrorist attacks, Reliab. Eng. Syst. Saf. 147 (2016) 1–8.
[16] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.
[17] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Resilience of the internet to random breakdowns, Phys. Rev. Lett. 85 (21) (2000) 4626.
[18] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Mitigation of malicious attacks on networks, Proc. Natl. Acad. Sci. 108 (10) (2011) 3838–3841.
[19] F. Hu, C.H. Yeung, S. Yang, W. Wang, A. Zeng, Recovery of infrastructure networks after localised attacks, Sci. Rep. 6 (2016).
[20] S. Shao, X. Huang, H.E. Stanley, S. Havlin, Percolation of localized attack on complex networks, New J. Phys. 17 (2) (2015) 023049.
[21] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2014) 43–60.
[22] J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of a network of networks, Phys. Rev. Lett. 107 (19) (2011) 195701.
[23] X. Huang, J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of interdependent networks under targeted attack, Phys. Rev. E 83 (6) (2011) 065101.
[24] J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (1) (2012) 40.
[25] J. Gao, S.V. Buldyrev, H.E. Stanley, X. Xu, S. Havlin, Percolation of a general network of networks, Phys. Rev. E 88 (6) (2013) 062816.
[26] X. Liu, H.E. Stanley, J. Gao, Breakdown of interdependent directed networks, Proc. Natl. Acad. Sci. 113 (5) (2016) 1138–1143.
[27] A.E. Motter, Y.-C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (6) (2002) 065102.
[28] R. Kinney, P. Crucitti, R. Albert, V. Latora, Modeling cascading failures in the north american power grid, Eur. Phys. J. B 46 (1) (2005) 101–107.
[29] Y. Xia, J. Fan, D. Hill, Cascading failure in Watts-Strogatz small-world networks, Physica A 389 (6) (2010) 1281–1285.
[30] L. Dueas-Osorio, S.M. Vemuru, Cascading failures in complex infrastructure systems, Struct. Saf. 31 (2) (2009) 157–167.
[31] Z. Lu, Z. Meng, S. Zhou, Cascading failure analysis of bulk power system using small-world network model, in: International Conference on Probabilistic Methods Applied To Power Systems, 2004, pp. 635–640.
[32] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, D. Helbing, Transient dynamics increasing network vulnerability to cascading failures., Phys. Rev. Lett. 100 (21) (2008) 2539–2541.
[33] L. Zhao, K. Park, Y.-C. Lai, Attack vulnerability of scale-free networks due to cascading breakdown., Phys. Rev. E 70 (3 Pt 2) (2004).
[34] M. Babaei, H. Ghassemieh, M. Jalili, Cascading failure tolerance of modular small-world networks, Circuits Syst. II. Express Briefs IEEE Trans. 58 (8) (2011) 527–531.
[35] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 542–542.
[36] J. y.H. Bakke, A. Hansen, J. Kertsz, Failure and avalanches in complex networks, Physics 76 (4) (2007) 717–723.
[37] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the North American power grid, Phys. Rev. E 69 (2 Pt 2) (2004) 292–313.
[38] J. Zhao, D. Li, H. Sanhedrai, R. Cohen, S. Havlin, Spatio-temporal propagation of cascading overload failures in spatially embedded networks., Nature Commun. 7 (2016).
[39] P. Holme, Congestion and centrality in traffic flow on complex networks, Adv. Complex Syst. 6 (02) (2003) 163–176.
[40] J.-W. Wang, L.-L. Rong, Cascade-based attack vulnerability on the US power grid, Saf. Sci. 47 (10) (2009) 1332–1336.
[41] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (7291) (2010) 1025–1028.
[42] R.-R. Liu, M. Li, C.-X. Jia, B.-H. Wang, Cascading failures in coupled networks with both inner-dependency and inter-dependency links, Sci. Rep. 6 (2016).
[43] P. Ye, Complex network characteristics of urban road network topology, J. Transp. Eng. Inf. (2012).
[44] E. Zio, G. Sansavini, Component criticality in failure cascade processes of network systems, Risk Anal. 31 (8) (2011) 1196–1210.
[45] S. Yang, F. Hu, C. Jaeger, Impact factors and risk analysis of tropical cyclones on a highway network, Risk Anal. 36 (2) (2016) 262–277.
[46] E.W. Dijkstra, A note on two problems in connexion with graphs, Numer. Math. 1 (1) (1959) 269–271.
[47] Terminology on disaster risk reduction, United Nations International Strategy for Disaster Reduction, 2009.