Hindawi
Complexity
Volume 2022, Article ID 3108327, 13 pages
https://doi.org/10.1155/2022/3108327

WILEY | Hindawi

Research Article

Allocating Defense and Recovery Resources for Spatial Networks against Cascading Failures

Zhengcheng Dong [1] **and Meng Tian** [2]

[1]*School of Electrical Engineering and Automation, Wuhan University, Wuhan, China*
[2]*Electronic Information School, Wuhan University, Wuhan, China*

Correspondence should be addressed to Meng Tian; mengtian@whu.edu.cn

Received 30 October 2021; Revised 17 November 2021; Accepted 10 January 2022; Published 31 January 2022

Academic Editor: Xuzhen Zhu

This paper proposes the models of allocating defense and recovery resources for spatially embedded networks, respectively, both of which consider the length of links as the allocation cost. In the defense model, the amount of defense resources required for each zone depends on the total length of the links they contain. It is found that dispersed allocation performs better and that parameters that allow for a uniform distribution of link lengths produce better results. In the recovery model, a *shortest link hierarchical recovery* (*HSR*) strategy is proposed and proved to be more effective. In this strategy, the number of repaired links plays a decisive role in the recovery results, while the total length of the links does not seem to matter when the number is constant. In addition, a number of different parameters are adopted to validate the qualitative conclusions. These models might yield insights into studying and protecting spatial infrastructure systems.

1. Introduction

Networks are ubiquitous in the real world. Since the introduction of small-world [1] and scale-free [2] networks, complex network theory has evolved tremendously in the last two decades. Cascading failure, addressing how failures propagate over the network, is a common phenomenon in complex systems [3, 4]. In some networks, the failure of a few components (nodes or links) can trigger cascading failures of other components, even with catastrophic consequences [5–8]. For some networks of networks [4, 9, 10] (NON) with dependencies (e.g., interdependent networks [4, 9]), this phenomenon is exacerbated by dependency links; i.e., failures can propagate across networks. As a typical example, some faulty devices or lines in power grids can lead to the redistribution of power flow, which may aggravate overloads on other lines and eventually lead to widespread blackouts. In smart grids, even information devices can cause large-scale blackouts (e.g., cyberattacks [11, 12]). Meanwhile, some countermeasures have been proposed to improve network invulnerability, such as critical node protection [13], topology modification [3, 14], link addition [15, 16], link removal [17], and source-sink node adjustment [18]. In addition, some methods, such as setting up autonomous nodes [19] and increasing the similarity of dependent node pairs [20, 21], have been shown to be effective for interdependent networks [9].

It is shown that a few nodes (or edges) in a network play a dominant role in cascade failures [22], which can be assessed by some proposed importance metrics, such as degree centrality [3, 23], betweenness centrality [8], and k-shell [22, 24]. Further, some metrics have been proposed and applied to real-world infrastructures [25–27]. Once these vital components are protected from failures, the network becomes more robust. In reality, it is possible to reinforce some nodes to enable them to function properly after being attacked, such as contingency mechanisms and backup facilities [28]. With limited resources, this strategy can protect a small fraction of nodes to make the system more resilient [28]. In other words, adding defense (or protection) resources for components will reduce their probability of being

successfully attacked, resulting in a probabilistic failure model. In this model, overloaded components do not fail immediately, but with a probability [29]. However, infrastructure networks are always spatially embedded, and external threats are often localized, which always cause aggregated damage to adjacent components limited to a specific region. In this case, critical zones, rather than individual components, should be identified and protected [30, 31]. Here is the question for spatial networks: what is the reasonable strategy for allocating defense resources to zones.

On the other hand, some damaged components will recover spontaneously after an inactive period of time, which is common in many real-world phenomena [32, 33], such as brain seizures, sudden market crashes, and traffic congestion. For example, traffic congestion in transportation networks is usually temporary resulting from a high traffic load, and the network may recover over time; a river in water networks dries up during the dry season and recovers in the wet season. Majdandzic et al. [32] proposed a state transition model to study systems in which nodes fail and recover spontaneously. Since then, dynamic failure-recovery models similar to epidemic models have been extensively studied in single isolated and even interacting networks [34–36]. Similarly, after cascading failures, a network will be fragmented into some subnetworks, and some failed components may recover spontaneously with a certain probability [37]. However, some artificial infrastructures are subject to physical attacks, such as wars and natural disasters, in which the damaged components do not recover spontaneously and require deliberate repairs. For instance, some infrastructures damaged by earthquakes, such as transportation and power networks, require manual repairs to regain functions. Such strategies can be classified into in-process [38, 39] and post-process repairs [40–44], which can be applied to both isolated [39, 40, 42, 43] and interdependent networks [38, 41]. It is worth noting that some of the repaired nodes are at risk of secondary failures due to severe load redistribution in some dynamic failure models [39, 40, 43, 44] or disconnection from the functional subnetwork in percolation models [41]. In summary, it is an optimal strategy to repair the damaged nodes that are directly connected to the functional subnetwork or that will not fail again. In particular, for interdependent networks, the state of dependent node pairs should be considered simultaneously. In addition, there is another type of strategy for repairing nonoriginal components; for example, Stippinger and Kertészb [45] proposed a healing model for interdependent networks by establishing new connectivity links between the neighbors of a failed node. It can be found that most of the studies focus on node recovery, where all links of a node work well when the node is repaired. However, for some spatially embedded infrastructures, the length of a link is equivalent to its construction cost; that is, high construction costs are required to establish long-range connections. Quattrociocchi et al. [46] proposed a link self-healing strategy that exploits redundant links to recover the connectivity of the system and compared the effects with different topologies. Although some recovery research has been conducted in spatial networks [38, 42] (e.g., lattice networks) and link recovery has been studied in [42, 46], few studies have considered link length constraints.

This paper proposes two frameworks for studying defense and repair strategies considering link length constraints in geography-based spatial networks. The main contributions are as follows. *i*) Based on key zone identification, a regional defense resource allocation strategy considering the total length of the contained links is proposed, and the effects of different parameters are analyzed. Finally, the most critical factor affecting the effect of defense resource allocation is obtained. *ii*) After localized failures, some link repair strategies considering the length cost of the repaired links are proposed and compared, and the best strategy is obtained. Also, some parameters are discussed. This paper provides insights into the allocation of defense and recovery resources considering link length in spatial networks, which can be generalized to other spatial network studies.

The rest of paper is organized as follows. In Section 2, the geography-based spatial network evolution model is introduced. In Sections 3 and 4, the allocation strategies for defense and recovery resources in spatial networks are investigated, respectively. Conclusions are made in Section 5.

2. Geography-Based Spatial Network Model

A network can be modeled as a mathematical graph $R = R(N, \mathscr{E})$ in which $N = \{N_1, N_2, \ldots, N_n\}$ is the set of nodes and $\mathscr{E} = \{E_1, E_2, \ldots, E_m\}$ is the set of links. In the evolution of the traditional Barabási-Albert (BA) scale-free network [2], no spatial information of components is involved. In general, infrastructures not only are spatially embedded but also have a large number of short-range connections under the constraint of construction cost. Thus, some models have been proposed, such as the Waxman model [47], lattice model [48, 49], geographical network model [50–53], and power grid model [54]. To synthesize the preferential attachment of BA networks and short-range connections of spatial infrastructures, a geography-based spatial network model proposed in [51] is adopted.

In this model, the network starts with n_0 nodes that are assigned random coordinates. At each time step, a new node i is added with a random location and connected to m_0 existing nodes according to their degree and Euclidean distance from i [50].

$$\sigma_{ij} = \frac{k_j^{\alpha}(t)}{d_{ij}^{\beta}}, \tag{1}$$

where j represents an existing node, $k_j(t)$ is the degree of j at time t, d_{ij} is the Euclidean distance between nodes i and j, and α and β are adjustable parameters. During the evolution, m_0 links for each new node are added one by one, and the evolution ends until the network reaches size n. Note that the functions of k and d can be of any desired form [52], even if the numerator [53] or denominator [2] is a constant.

As shown in Figure 1, the network is connected sparsely and locally with only a few nodes having more than two links ($k > 2$). Based on this spatial model, some studies [55, 56] on

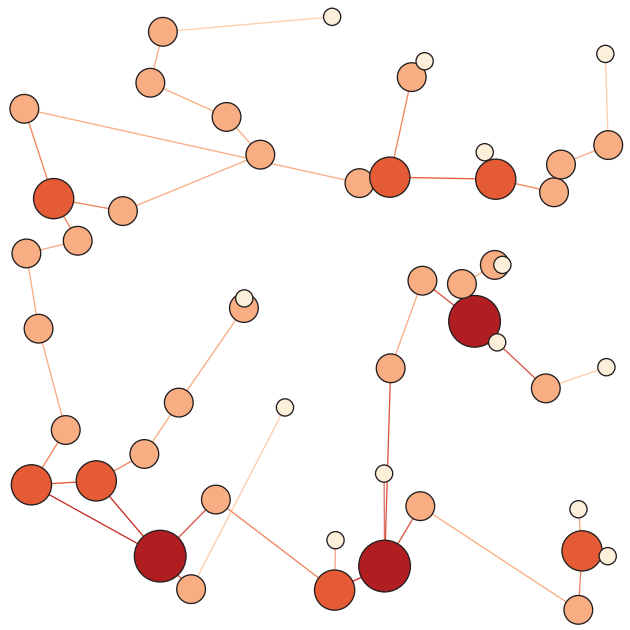

Figure 1: A spatial network generated by the geography-based model is embedded into a unit plane where $n = 50, \alpha = 1, \beta = 5$, and $m_0 = 1$. Each node has unique two-dimensional coordinates $(x, y) \in [0, 1]$. High-degree nodes are marked in dark red, while dark red links characterize the high-degree nodes they connect.

modeling infrastructures have been carried out. For a constant α, in the case of small β, more long-range links will be established while neighboring nodes are most likely to be connected with the increase in β; i.e., extreme spatial networks will be generated with large β.

Moreover, a load-based cascading failure model is adopted to simulate the dynamic failure process of infrastructures, which is called the Motter–Lai capacity model [8]. In the model, the load L_i of a node i is defined as its betweenness centrality [8].

$$L_i = \sum_{(w,v)} \frac{\sigma_{wv}(i)}{\sigma_{wv}}, \tag{2}$$

where $\sigma_{wv}(i)$ is the number of geodesics between nodes w and v that pass node i, and σ_{wv} is the total number of geodesics between nodes w and v.

Typically, a node can only handle a limited amount of loads. Once its load exceeds the capacity, the node fails. Thus, according to the Motter–Lai capacity model [8], the capacity C_i of node i is defined to be proportional to its initial load,

$$C_i = (1 + e)L_{i0}, \tag{3}$$

where L_{i0} is the initial load of node i when the network is intact, and $e \geq 0$ is a tolerance parameter that adjusts the capacity. Initially, a few components are attacked, and the loads of the remaining nodes vary as the topology changes. To be functional, a node i shall *a)* handle the load on it $(L_i \leq C_i)$ and *b)* belong to the largest connected subgraph. The nodes that do not meet the criteria are defined as failed nodes, and all their links will be disconnected. The process will continue recursively until no further failed nodes occur, and the network invulnerability is evaluated by the number of remaining nodes G.

3. Defense Resource Allocation

For spatial infrastructures, external attacks usually result in localized failures, and thus critical parts should be zones rather than components. Based on the key zone identification, the allocation model of defense resources for spatial networks is proposed, and some parameters are studied. It is assumed that the total resources to be allocated are D, and they are divided into K parts. The embedded space is uniformly divided into $t_z \times t_z$ zones, denoted as $Z = \{z_1, z_2, \ldots, z_{t_z \times t_z}\}$. To completely cover the whole space, all zones are regular, and each zone has the same area. When a zone z_i is attacked, all links within z_i will be disconnected. In this case, the invulnerability can be calculated as

$$G_{z_i} = \int_0^1 G_{z_i}(e)\mathrm{d}e, \tag{4}$$

where e is the network capacity parameter in (3), and G_{z_i} is the invulnerability of z_i when it is attacked from $e = 0$ to 1. We assume that the added defense resources reduce the probability of successful attacks. Note that, in the simulations in this section, each zone is attacked in turn, and we use the sum of the invulnerability G_{z_i} obtained by attacking each zone i as the indicator to evaluate the invulnerability of the whole network. Before allocating defense resources, the initial network invulnerability is defined as

$$G_{\mathrm{do}} = \sum_{i=1}^{t_z \times t_z} G_{z_i}. \tag{5}$$

It is assumed that the probability of a successful attack on z_i is $\kappa_i = 1/1 + \tau_i$, where τ_i is the resource added for z_i. When no defense resources are added to z_i $(\tau_i = 0)$, this zone is guaranteed to be attacked successfully $\kappa_i = 1$; for example, an 'enemy' can easily attack a zone without any security defenses. After allocating some resources for z_i $(\tau_i > 0)$, the probability of z_i being attacked successfully is reduced $\kappa_i < 1$. On this occasion, the enemy cannot easily destroy z_i.

In general, the more the resources are applied, the less likely this zone is to be attacked successfully. After adding τ_i resources for zone z_i, the expected invulnerability G'_{z_i} of attacking z_i can be calculated as

$$1 - G'_{z_i} = \frac{1}{1 + \tau_i}\left(1 - G_{z_i}\right). \tag{6}$$

Note that defense resources can be any measure that reduces the failure probability of zones. For example, in power systems, the strategies of defenders (e.g., power grid companies and other security agencies) could be regional security enhancements, power facility inspection enhancements, and power facility upgrades. However, this paper does not focus on the implementation of specific measures but only examines the allocation of defense resources at the system level.

Previous work on component protection only considered number as the cost, and no spatial information is involved. In fact, the cost of defense is different for links with different lengths (e.g., roads or power lines); that is, the longer the length, the higher the cost. Similarly, for localized failures, the defense resources added for z_i should be related to the total length of the links contained in z_i, denoted as r_{z_i}.

$$r_{z_i} = \frac{D}{K} \times \left(\min\left(K, \left(\underbrace{\frac{d_{z_i}}{\min\left(d_{z_i}\right)}}_{p_{z_i}} \right)^q \right) \right), \tag{7}$$

where d_{z_i} is the total length of the links contained in z_i, p_{z_i} is the share of resources required to defend z_i, and $q \in \mathbf{N}^+$ is a tunable parameter that controls the amount of resources allocated for z_i. p_{z_i} is related not only to d_{z_i}, but also to the smallest $d_z^* = \min\left(d_{z_i}\right)$ of all zones. In the case of $q = 0$, the same amount of resources is added for each zone, while for $q > 0$, zones containing longer links require more resources.

We assume that defense resources are always added to the most vulnerable zone dynamically (*minimum G allocation* strategy, denoted as *MGA*), and the allocation process is as follows. *(a)* Initialize the total amount of resources $D_a = D$ for the current step. *(b)* Calculate G_{z_i} for each zone z_i and obtain the most vulnerable zone z_ξ $(\forall i \neq \xi, G_{z_\xi} \leq G_{z_i})$. *(c)* Add r_{z_ξ} resources for z_ξ, and the remaining resources are updated to $D_a = D_a - r_{z_\xi}$. *(d)* Go to step *(b)* if $D_a > 0$; otherwise, go to step *(e)*. *(e)* All resources are allocated, and the process ends. Finally, the growth rate ΔG_d of invulnerability after allocating defense resources is adopted to evaluate the allocation effect.

$$\Delta G_d = \frac{\left(G_{\mathrm{dr}} - G_{\mathrm{do}}\right)}{G_{\mathrm{do}}}, \tag{8}$$

where G_{dr} is the network invulnerability after adding defense resources according to (5). In the following simulations, the basic parameters are set to $m = 2$, $n = 200$, $\alpha = 1$, $\beta = 3$, $t_z = 5$ and $q = 1$ to investigate the effect of different parameters on ΔG_d. Each curve is averaged by 10 random spatial networks. In addition to the *minimum allocation*, a *random allocation* (*RA*) strategy and a *minimum length allocation* (*MLA*) strategy are also analyzed (Figure 2). Among them, *MLA* refers to allocating resources sequentially for zones with small p_z, while *RA* refers to random allocation.

As shown in Figure 2, MGA has the best effect, followed by RA, and MLA is the worst mode. In general, zones with small d_z have fewer components, which will lead to small-scale failures with a higher probability. Therefore, in MLA, adding resources to zones with small d_z implies adding resources to zones with large G_z, which cannot achieve a significant improvement in network invulnerability. In RA, defense resources are added for one random zone z_i $(i \in \{1, 2, \ldots, t_z \times t_z\})$ at each time step. Due to the inverse proportional function (6), adding more resources for zones with moderate or high invulnerability does not significantly improve the performance. In contrast, it is effective to add resources to vulnerable zones. As a general conclusion,

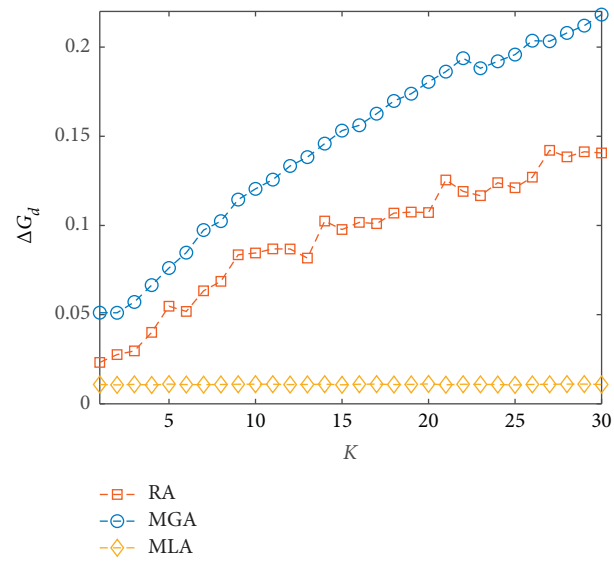

Figure 2: Invulnerability improvement rate ΔG_d as a function of the allocation method K for three allocation strategies MGA, RA, and MLA, where the total resources are $D = 13$.

increasing the total amount of resources can significantly improve the network performance, which also implies higher defense costs. Therefore, it is necessary to find a better allocation method for a given D; for example, how many parts to divide the resources into? (Figure 3).

With a small D (e.g., $D = 1$), ΔG_d hardly changes with the increase in K, indicating that it is useless to change the allocation method for fewer resources. However, for a large D, ΔG_d increases as K increases. In the case of $D = 5$, the growth rate of ΔG_d is seen to slow down gradually, and ΔG_d reaches a stable value when K is large enough. This indicates that, for a constant D, there exists an appropriate K (denoted as K_a) that can bring ΔG_d to a satisfactory level, while the effect of continuing to increase K is not significant. However, with the increase in D, the slope of these fitting curves gradually increases, which means that a large D corresponds to a large K_a. It can be concluded that the dispersed allocation method performs better and that the more the resources that are available, the greater the dispersion required.

In (7), q controls the amount of resources required for each zone with different link lengths. If $q = 0$, all zones require the same amount of resources, regardless of the length of the links they contain. In the case of $q > 0$, the resources required for each zone are positively correlated with the total length of the links involved. The larger q is, the more the resources are required for zones with longer links. As can be seen from Figure 4, in the case of $q = 0$, ΔG_d rapidly reaches a stationary value as K increases, while the curve of ΔG_d gradually moves down with the increase in q, and no stable trend can be observed. For a certain zone, the larger q is, the more the resources it requires, which leads to a poor effect of concentrated resource allocation to a few zones. In other words, a large q produces similar effects as a small K. In addition to the allocation parameter, the effect of

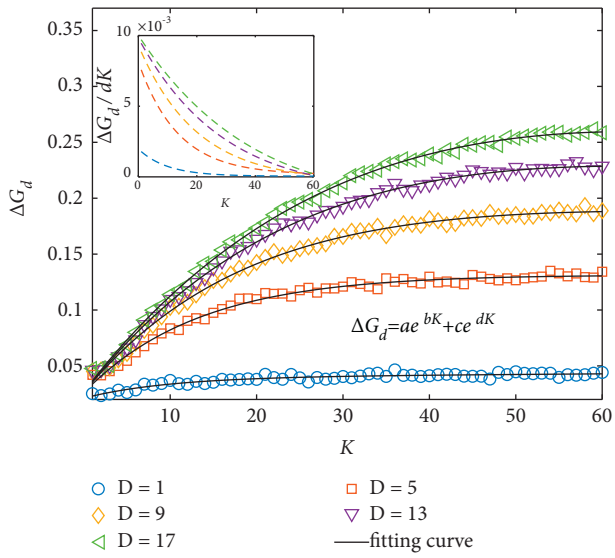

FIGURE 3: Invulnerability improvement rate ΔG_d as a function of the allocation method K with different amounts of defense resources D. The fitting curve for each D is plotted, which can be written as $\Delta G_d = ae^{bK} + ce^{dK}$. The inset shows the growth slope $d\Delta\ G_d/dK$ of the different fitting curves.

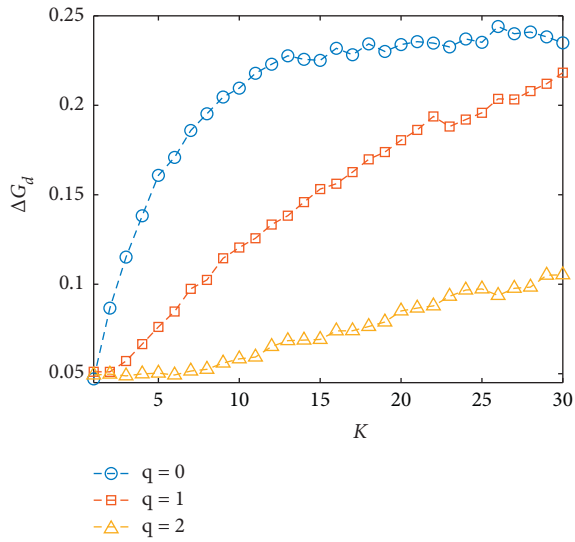

FIGURE 4: Invulnerability improvement rate ΔG_d as a function of the allocation method K with different control parameters q in the defense resource allocation, where the total resources are $D = 13$.

the network evolution parameter β on the results is also analyzed (Figure 5).

In the spatial network model, α and β together govern the total length of links. When α is fixed, a large β generates more short-range links and shortens the total length of the links contained in each zone. As a result, the p_z of each zone is reduced. In this case, fewer defense resources are required, and the same amount of resources can be allocated to more zones, producing the same effect as with large K. In particular, it can be seen that the growth rate of the curve at $\beta = 10$ slows down as K increases, and ΔG_d eventually reaches a stable value when K is large enough ($K \approx 27$). This indicates that the network with large $\beta = 10$ is already an extreme spatial network, which contains enough short-range links. Therefore, when K is large, resources can be evenly allocated to enough zones to produce better results. It seems to be possible to conclude that better results can be obtained when the zones contain shorter links. In addition, another parameter, the number (or size) of zones t_z, can also change the length of the links contained in each zone, and thus the effect of t_z is investigated (Figure 6).

It can be seen that the curve of ΔG_d as a function of K shifts downward as t_z increases, indicating that fewer partitions can improve the allocation effect at each K. In the case of $t_z = 4$, the number of zones $t_z \times t_z$ to be defended decreases. Although each zone contains longer links than those contained in large t_z, they have similar d_z, so each p_z becomes smaller. On this occasion, similar to the effect of β, resources can be evenly allocated to more zones.

For a network of size n, the node density ψ can be calculated as $\psi = n/t_z \times t_z$. In addition to t_z, another parameter n can also adjust the node density (or the total length of the links) in each zone. In the above simulations, only small-scale networks with $n = 200$ are adopted. To verify our results for different node densities for a given $t_z = 5$, the effect of network size is investigated (Figure 7).

For the same K, the value of ΔG_d increases as n increases, and the curves of large n (e.g., $n = 500$ and 1000) gradually converge. Similar to the effect of β, n can also change the length of the links contained in each zone; i.e., large n increases the node density, making the links contained in zones longer. However, the distribution of links becomes uniform; i.e., each zone has a similar d_z, making p_z smaller. Although different network sizes produce different ΔG_d, they all have similar trends, which do not affect the qualitative analysis.

According to the analysis of Figures 4–7, we infer that the uniformity of link distribution controls the effect of defense resource allocation in this model, not just the length of links within a zone. To represent the uniformity of the links contained in each zone, the standard deviation σ of p_z is adopted.

$$\sigma = \sqrt{\frac{1}{t_z \times t_z - 1} \sum_{j=1}^{t_z \times t_z} \left(p_{z_j} - \overline{p}_z\right)^2}, \tag{9}$$

where $\overline{p}_z$ is the average of p_z of all zones.

A small σ refers to a uniform link distribution, indicating that the total length of the links in each zone approximates the minimum value of d_z. Combined with the results in Figures 4–7, it can be seen from Figure 8 that the effect of resource allocation ΔG_d gradually becomes better as σ decreases, which proves our inference.

In summary, this section presents a framework for allocating defense resources in spatial networks, where the length of the links contained in each zone is considered as the cost. Through the simulations with different parameters, it can be concluded that the dispersed allocation method and the parameters that make the link lengths uniformly distributed yield better results.

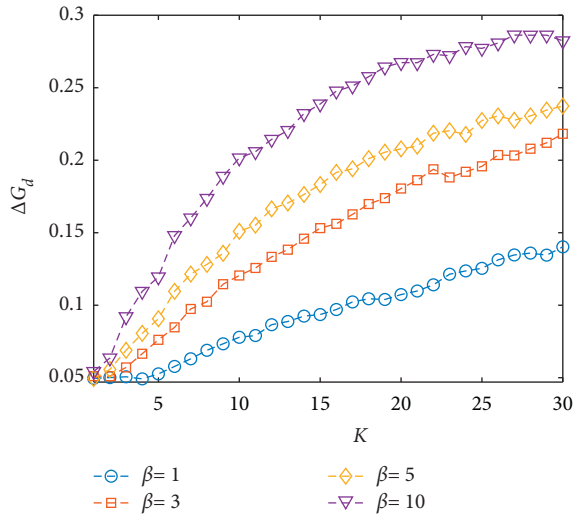

FIGURE 5: Invulnerability improvement rate ΔG_d as a function of the allocation method K with different evolution parameters β in the defense resource allocation, where the total resources are $D = 13$.

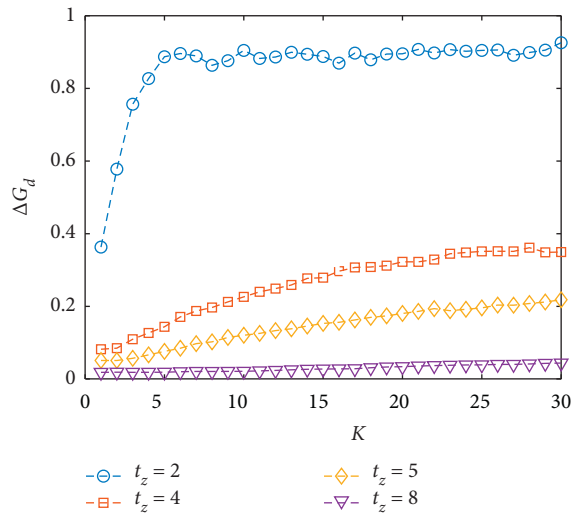

FIGURE 6: Invulnerability improvement rate ΔG_d as a function of the allocation method K with different division parameters t_z in the defense resource allocation, where the total resources are $D = 13$.

4. Recovery Resource Allocation

Generally, damaged components of a network after cascading failures require urgent repairs, such as infrastructure rebuilding or restoration after floods, earthquakes, and other natural disasters. In previous work on network recovery, studies have always focused on finding a better node repair strategy without considering the cost. They assumed that once a node was repaired, all its links would work. However, each node has a different number of links, and these links may have different lengths. For some artificial infrastructures, the repair of connectivity links requires a certain cost depending on their length, such as roads in transportation networks and tracks in railway networks. Therefore, it is necessary to develop a link repair model for spatial networks, which takes into account the link length constraint.

In this section, a circular failure zone of radius ζ is adopted to simulate external attacks. The failure process and invulnerability indicator are the same as those in Section 3. After cascading failures, a network is fragmented, and the recovery process should start from the remaining part (called the active subnetwork). After applying a repair strategy, the new network will be reexamined according to the failure rules described in Section 2 to find the secondary cascading failures. When the network reaches a stable state, the new invulnerability G_{rr} is calculated, and the improvement rate ΔG_r similar to (8) is used to evaluate the effect of the recovery strategy. To maximize ΔG_r, the links closest to the active part should be restored first; then, the newly obtained network is served as the new active subnetwork and the closest links are found, and so on, until the repair length is satisfied. Therefore, inspired by the definition of *k-core* in the network, a *hierarchical recovery* strategy (HR) is proposed. For comparison, a *random recovery* strategy (RR) is also analyzed.

In the HR strategy, the initial subnetwork is called the first layer (*1-layer*), and the nodes directly connected to the *k-layer* nodes belong to $(k+1)$*-layer* until all nodes are layered. Similarly, the links $\mathbf{l}_{\mathbf{k+1}}$ connecting *k-layer* and $(k+1)$*-layer* nodes are defined as candidate repaired links in $(k+1)$*-layer* (Figure 9 shows the hierarchical structure of a simple network). In this typical hierarchical strategy, links should be repaired layer by layer.

$$\mathbf{l}_{\mathbf{k+1}} = \left\{ l_{n_i n_j} \mid n_i \in \mathscr{R}_k \wedge n_j \in \mathscr{R}_{k+1} \setminus \mathscr{R}_k \right\}, \tag{10}$$

where $l_{n_i n_j}$ is the link connecting nodes n_i and n_j, and $\mathscr{R}_k$ represents the active subnetwork in *k-layer*.

As shown in Figure 9(a), some nodes have multiple candidate recovery links; for example, node 5 has two links l_{15} and l_{45}. If only one of the two links is repaired, the node remains connected to $\mathscr{R}_1$, which also reduces the repair cost. However, the reduction of the recovery links may lead to a change in the load of some nodes, resulting in new cascading failures. In this case, two special modes of the HR strategy are proposed, which repair only one link of the node connected to the active subnetwork, including the *shortest link recovery* mode (HSR) (Figure 9(b)) and the *random link recovery* mode (HRR).

$$\mathbf{l}^{\mathbf{s}}_{\mathbf{k+1}} = \left\{ \begin{array}{l} l_{n_i n_j} | l_{n_i n_j} \in \mathbf{l}_{\mathbf{k+1}} \wedge n_i \\ = \operatorname{argmin}_{n_i} \left(d_{n_i n_j} \right) \end{array} \right\}, \tag{11}$$

where $\mathbf{l}^{\mathbf{s}}_{\mathbf{k+1}}$ is the candidate repaired link in $(k+1)$*-layer* for the *HSR* mode, and $d_{n_i n_j}$ is the distance between nodes n_i and n_j.

In spatial networks, the total length of the repaired links δ is considered as the cost of the repair strategy. During the recovery process, δ needs to be preset, and the links should be repaired layer by layer from *2-layer*. However, the total length cannot be controlled exactly as δ, so a

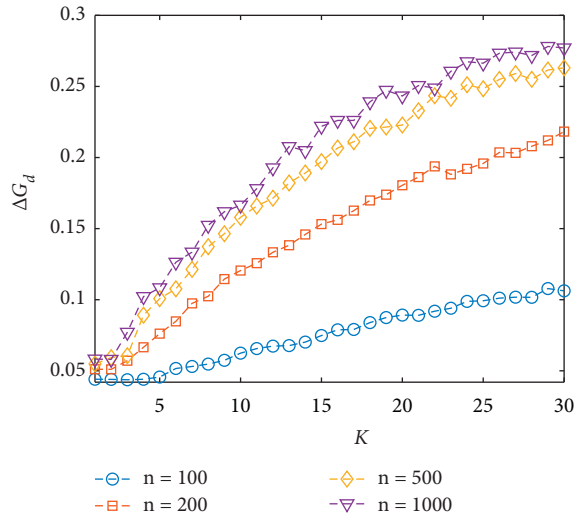

Figure 7: Invulnerability improvement rate ΔG_d as a function of the allocation method K with different network sizes n in the defense resource allocation, where the total resources are $D = 13$. All networks are embedded in the unit plane, i.e., node coordinates $(x, y) \in [0, 1]$.

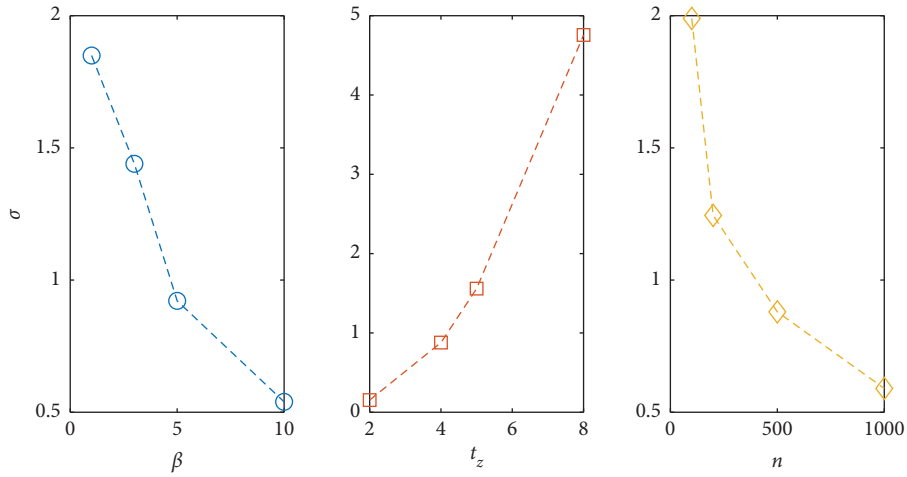

Figure 8: The standard deviation σ of p_z in all zones under different network parameters β (evolution parameter), t_z (division parameter), and n (network size), where the total resources are $D = 13$ and are divided into $K = 15$ parts.

tolerable error μ is introduced; i.e., the actual total length $\delta_a \in [\delta - \delta \times \mu, \delta + \delta \times \mu]$. Taking layer k as an example, the search process of its repaired links U is as follows. (*i*) Define the step flag i, the set U of length $\mathscr{H} = \{h_1, h_2, \ldots, h_l\}$, the total length $\delta_a = \sum_{i=1}^{l} \mathscr{H}$ at the current step, and initialize $i = 1$, $\delta_a = 0$, and $U = \varnothing$. (*ii*) At step i, randomly select a disconnected link $U_i \in \mathbf{l_k}$ of length h_i ($h_i \leq \delta$), and record U_i into U. (*iii*) Discard U_i and go to step (*ii*) if $\delta_a > \delta$, or go to step (*iv*) if $\delta_a < \delta$; otherwise, go to step (*v*). (*iv*) U_i is valid and update $i = i + 1$; then go to step (*ii*). (*v*) All repaired links are found and the search process ends. Note that if all the links within *k-layer* are selected, or if no link of suitable length can be found, the next layer $(k + 1)$*-layer* will be searched. This process continues until either δ is satisfied or all damaged links are selected. The flowchart corresponding to the recovery strategy is shown in Figure 10.

All simulations are averaged over 15 networks with 30 random attacks per network and 40 recoveries per attack. Some basic parameters are set to $\zeta = 0.3$, $m = 2$, $n = 200$, $e = 0.1$, $\alpha = 1$, $\beta = 3$, and $\mu = 0.05$. First of all, the four recovery strategies and modes RR, HR, HSR, and HRR mentioned above are analyzed (Figure 11).

Compared with the RR strategy, HR can significantly improve ΔG_r. In the RR strategy, links are repaired randomly, so some of the repaired links may be disconnected again due to disconnection from the active subnetwork, which leads to some useless recovery. However, this phenomenon can be avoided in the HR strategy because the repaired links always belong to the functional part. In the improved two HR modes, HRR repairs only one connectivity link for each node, and more components will recover at a constant cost. As can be seen from the results, no new large-scale failures occur in the repaired network. In addition, another more efficient mode HSR repairs the shortest link, further improving the utilization of limited recovery resources.

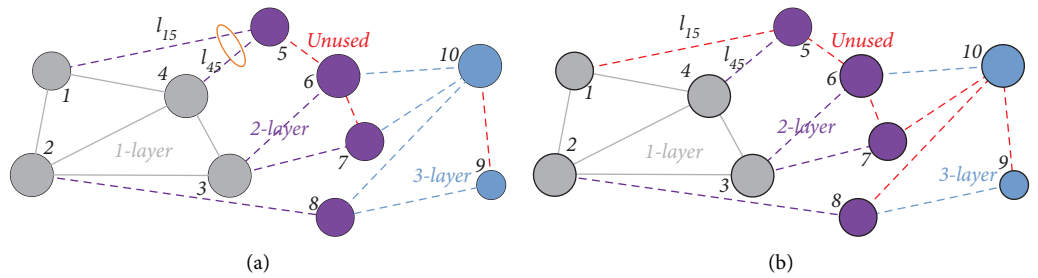

Figure 9: Illustrations of hierarchical recovery strategies with a simple network. The gray nodes refer to the functional nodes before recovery, belonging to *1-layer*; the purple nodes connected to the *1-layer* nodes belong to *2-layer*; and the blue nodes connected to the *2-layer* nodes belong to *3-layer*. The gray, purple, and blue links belong to different layers, while the red ones are unrepaired links. (a) HR mode. (b) HSR mode.

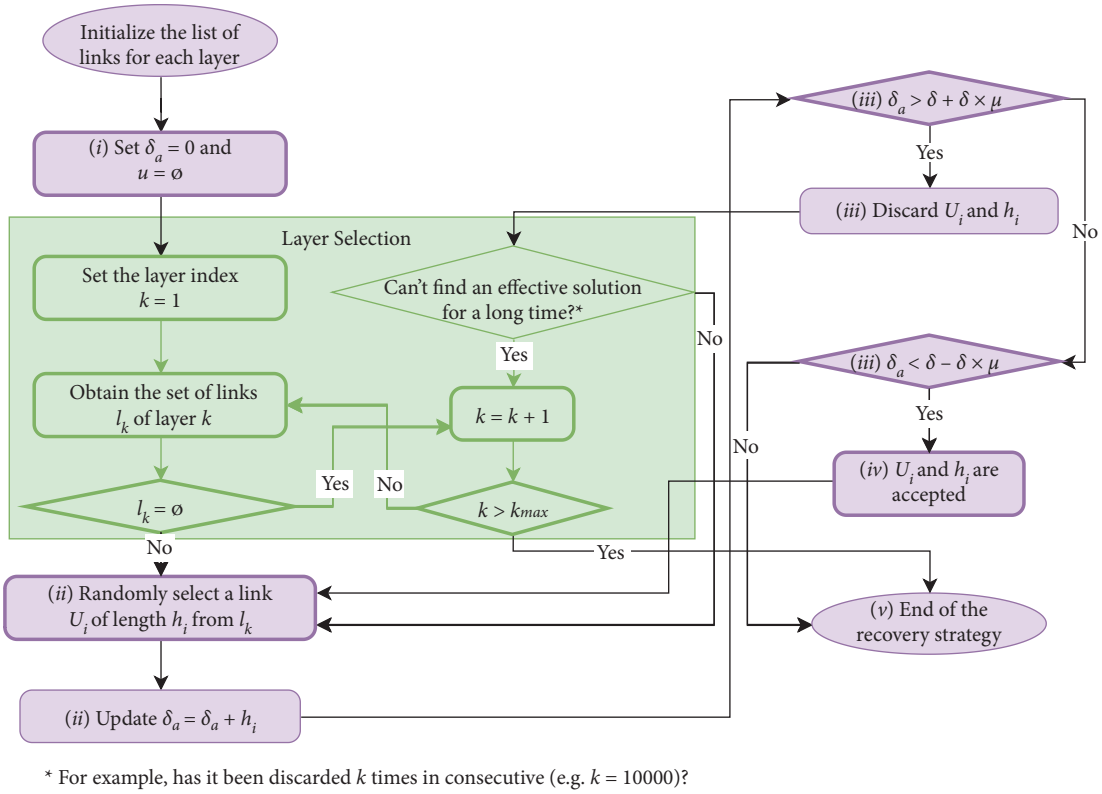

Figure 10: Flowchart of the HR recovery strategy.

For a specific δ, different types of solutions are obtained, which contain different numbers of links n_δ. On this occasion, a large n_δ implies more and shorter links, and the impact of n_δ is studied with two modes HSR and HR (Figure 12).

In both modes, for a constant δ, ΔG_r increases as n_δ increases. In HSR, the same n_δ produces the same results even for different δ. In particular, the piecewise and overall curves show a regular linear relationship between ΔG_r and n_δ, as shown in Figure 12(a), and the fitting function can be written as

$$\Delta G_r = a \times n_\delta, \tag{12}$$

where a is the slope of the fitting curve, which is a constant associated with the network. Some simulations show that different networks have different slopes, but the curves are linear for all networks. Similarly, the same conclusion

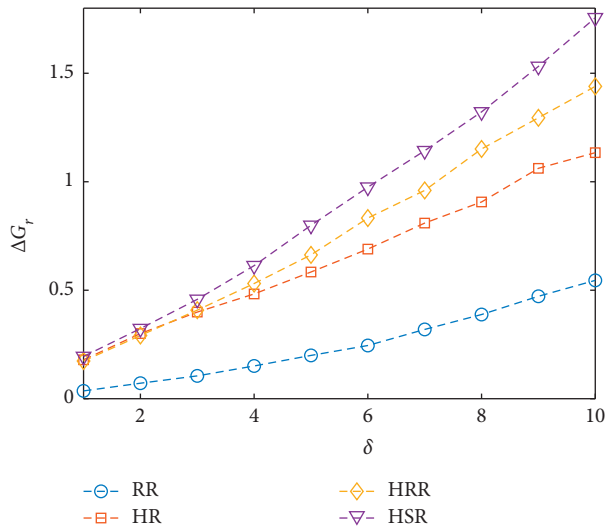

FIGURE 11: Invulnerability improvement rate ΔG_r as a function of the recovery length δ for four recovery strategies and modes RR, HR, HSR, and HRR.

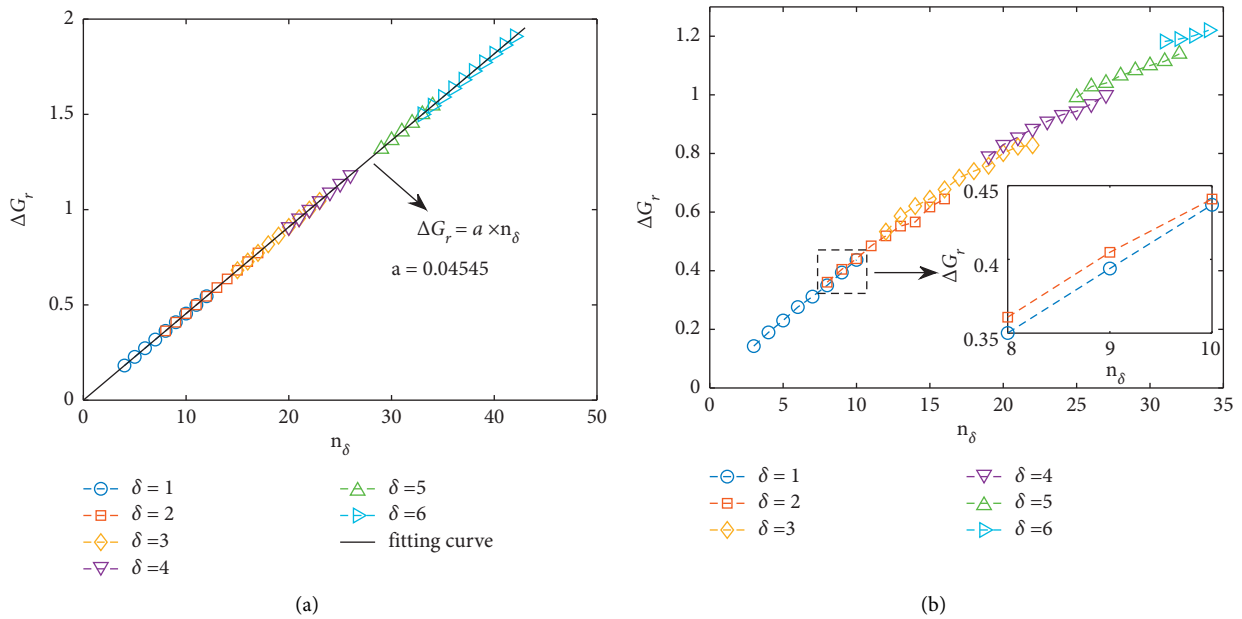

FIGURE 12: Invulnerability improvement rate ΔG_r as a function of the solution type n_δ with different recovery lengths δ for two recovery modes HR and HSR. A total of 500 solutions are searched for each δ. (a) shows the HSR mode, where all data points are fitted by the linear function $\Delta G_r = a \times n_\delta$; (b) shows the HR mode, where the inset zooms in on some overlapped details of $\delta = 1$ and 2. (a) HSR mode. (b) HR mode.

is obtained based on simulations of the HRR mode. However, the difference is that, in HR, a larger δ produces better results for a constant n_δ, and the gap gradually increases with the increase in δ. In both HRR and HSR, each repaired node has only one connectivity link, so the repaired topology is always the same for the same n_δ, which results in the same secondary failure process. However, in HR, multiple links may be repaired for the same node, resulting in different topologies and failure processes. In summary, on the one hand, repairing more links produces better results when the total amount of resources δ is constant; on the other hand, when the number of links n_δ is constant, δ does not affect the effect of HSR but slightly affects HR, where large δ performs better.

Similar to the analysis in Section 4, the recovery results for different spatial network parameters, including the evolution parameter β (Figure 13) and network size n (Figure 13), are also investigated. All cases are carried out based on the HSR mode.

In Figure 13, similar to the results in Figure 5, the curve of ΔG_r gradually shifts upward as β increases, indicating that

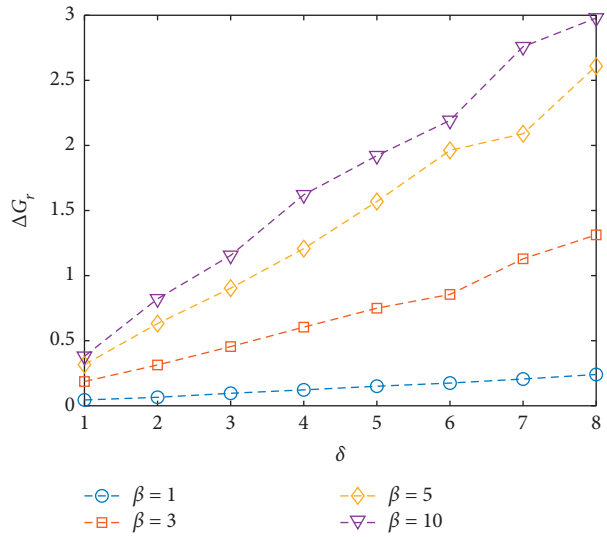

FIGURE 13: Invulnerability improvement rate ΔG_r as a function of the recovery length δ with different evolution parameters β for the HSR recovery mode.

the extreme spatial networks have a better recovery effect. In the spatial networks with large β, short links account for a large proportion and the total length of the connectivity links becomes shorter. In this case, more links will be repaired and more nodes will work properly again with the same total recovery resources, producing better results.

Contrary to the results of the defense resource allocation in Figure 7, in the recovery resource allocation (Figure 14), the curve of ΔG_r shifts downward with the increase in network size n, indicating that small-scale networks have better recovery results. With other network parameters fixed, although each link becomes shorter in large-scale networks, they have more links and the proportion of failed components becomes larger after a localized attack. Therefore, more connectivity links need to be repaired, and large-scale networks will recover less effectively than small-scale ones with the same amount of recovery resources. Similarly, it can be concluded that although ΔG_r varies with different parameters, they have similar trends, indicating that the qualitative results are not affected by the network parameters. Note that as the network capacity parameter e increases, the failure size of the system decreases. In this case, the three hierarchical recovery strategies will have similar improvement effects for large e.

In summary, this section presents a framework for allocating recovery resources in spatial networks, where the total length of the repaired links is constrained. Comparing the four recovery strategies, the HSR mode is the most effective, and the more the links are repaired, the better the results are. In addition, the effects of some parameters on the results are analyzed.

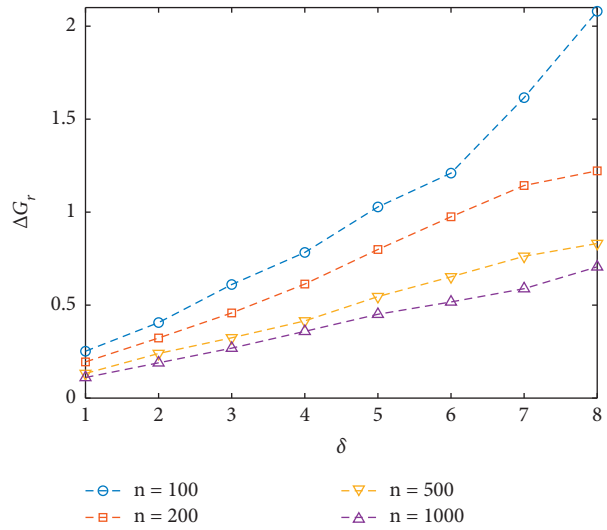

FIGURE 14: Invulnerability improvement rate ΔG_r as a function of the solution type δ with different network sizes n for the HSR recovery mode.

5. Conclusion

In spatial networks, spatial information needs to be considered in the study of various issues. In this paper, two models of allocating defense and recovery resources for spatial networks are proposed, both of which consider the link length. On the one hand, in the defense resource allocation model, the embedded space is divided into different zones, and resources are applied according to the total length of the links contained in each zone to reduce the failure

probability. The simulations reveal that the dispersed allocation performs better. In addition, some network and allocation parameters are analyzed, and the qualitative results are not affected. On the other hand, in the model of recovery resource allocation, the *shortest link hierarchical recovery* strategy is shown to be the most effective than the other strategies when the total amount of resources is constant. It is also found that the number of repaired links is a critical factor in the results; i.e., the more the links repaired, the better. In addition, the results for different network parameters are discussed.

In fact, most infrastructures are spatially embedded and partitioned. In China, for example, the entire power grid is divided into multiple geographic regions, including East China, Central China, North China, Northwest China, Northeast China, South China, and Tibet, most of which cover multiple provinces. Similarly, a provincial grid, for example, is geographically divided into multiple cities. In these networks or subnetworks, links are usually short-range, as long-range connections imply greater construction costs. In general, natural disasters usually result in damage to one or more regional (or municipal) grids. Similarly, similar regional structures and external threats exist for power communication systems or other fiber optic communication systems. In particular, the shortest path-based load model (the Motter–Lai model) used in this paper is a common model to characterize flow-based systems, most typically communication systems and transportation systems. On the one hand, the zone-based resource allocation strategy can improve the invulnerability of the whole system before disasters. On the other hand, after regional disasters, the *shortest link recovery* strategy can quickly achieve the connectivity of the whole system under certain time and cost constraints, especially the connectivity of the control center to other nodes, such as the repair of power transmission lines and communication lines. Therefore, based on the conclusions obtained in this paper, guidance can be provided for the protection and recovery of spatial infrastructure systems.

In summary, this paper provides a framework for allocating resources for spatial networks. However, the two models presented are simple frameworks that illustrate how the cost of link length constrains the effect of the allocation methods, and some constraints are still not considered. For example, in the study of defense resource allocation, the zones are divided regularly, and the invulnerability indicator after defense does not consider the randomness of attacks. In future work, the game between attackers and defenders in resource allocation will also be studied.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (nos. 51807143, 51707135), the China Postdoctoral Science Special Foundation (no. 2018T110797), the China Postdoctoral Science Foundation (no. 2017M612499), and the Fundamental Research Funds for the Central Universities (no. 2042021kf0011).

References

[1] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[2] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[3] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[4] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failure in interdependent networks," *Nature*, vol. 464, no. 15, pp. 1025–1028, 2010.

[5] Y. Xia and D. J. Hill, "Attack vulnerability of complex communication networks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 55, no. 1, pp. 65–69, 2008.

[6] Y. Guo, Z. Wang, S. Luo, and Y. Wang, "A cascading failure model for interdomain routing system," *International Journal of Communication Systems*, vol. 25, no. 8, pp. 1068–1076, 2012.

[7] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the us power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[8] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical review. E, Statistical, nonlinear, and soft matter physics*, vol. 66, no. 6, Article ID 065102, 2002.

[9] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, 2012.

[10] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of Complex Networks*, vol. 2, no. 3, pp. 203–271, 2014.

[11] S. Siddharth, H. Adam, and G. Manimaran, "Cyber physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[12] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2017.

[13] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

[14] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A*, vol. 357, no. 3-4, pp. 593–612, 2005.

[15] X.-B. Cao, C. Hong, W.-B. Du, and J. Zhang, "Improving the network robustness against cascading failures by adding links," *Chaos, Solitons & Fractals*, vol. 57, pp. 35–40, 2013.

[16] X. Ji, B. Wang, D. Liu et al., "Improving interdependent networks robustness by adding connectivity links," *Physica A: Statistical Mechanics and Its Applications*, vol. 444, pp. 9–19, 2016.

[17] D. Witthaut and M. Timme, "Nonlocal effects and countermeasures in cascading failures," *Physical review. E, Statistical,*

nonlinear, and soft matter physics, vol. 92, no. 3, Article ID 032809, 2015.

[18] O. Smith, J. Crowe, E. Farcot, R. D. O'Dea, and K. I. Hopcraft, "Cascading failures in networks of heterogeneous node behavior," *Physical Review*, vol. 101, no. 2, Article ID 020301, 2020.

[19] R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition," *Physical Review Letters*, vol. 105, no. 4, Article ID 048701, 2010.

[20] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, "Inter-similarity between coupled networks," *Europhysics Letters*, vol. 92, no. 6, Article ID 68002, 2011.

[21] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, "Interdependent networks with identical degrees of mutually dependent nodes," *Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics*, vol. 83, Article ID 016112, 2011.

[22] Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science*, vol. 358, no. 6365, Article ID eaan3184, 2017.

[23] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Physical Review Letters*, vol. 86, pp. 3682–3685, 2001.

[24] M. Kitsak, L. K. Gallos, S. Havlin et al., "Identification of influential spreaders in complex networks," *Nature Physics*, vol. 6, pp. 888–893, 2010.

[25] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Breakdown of the internet under intentional attack," *IEEE Trans. Circuits Sys. II*, vol. 65, no. 3, pp. 346–350, 2018.

[26] J. Wang and R. Lili, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Safety Science*, vol. 49, no. 6, pp. 807–812, 2011.

[27] L. Sun, Y. Huang, Y. Chen, and L. Yao, "Vulnerability assessment of urban rail transit based on multi-static weighted method in beijing, China, Transport," *Res. A-POL*, vol. 108, pp. 12–24, 2018.

[28] X. Yuan, Y. Hu, H. E. Stanley, and S. Havli, "Eradicating catastrophic collapse in interdependent networks via reinforced nodes," *P. Natl. Acad. Sci. USA*, vol. 114, no. 13, pp. 3311–3315, 2017.

[29] J. Liu, Q. Xiong, X. Shi, K. Wang, and W. Shi, "Robustness of complex networks with an improved breakdown probability against cascading failures," *Physica A*, vol. 456, pp. 302–309, 2016.

[30] M. Ouyang, "Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks," *Reliability Engineering & System Safety*, vol. 154, pp. 106–116, 2016.

[31] Z. Dong, M. Tian, and J. Liang, "Cascading failures of spatially embedded cyber physical power system under localized attacks," in *Proceedings of the 37th Chinese Control Conference, IEEE*, pp. 6154–6159, Wuhan, China, July 2018.

[32] A. Majdandzic, B. Podobnik, S. V. Buldyrev, D. Y. Kenett, S. Havlin, and H. E. Stanley, "Spontaneous recovery in dynamical networks," *Nature Physics*, vol. 10, pp. 34–38, 2014.

[33] X. Zhan and S. V. Ukkusuri, "Dynamics of functional failures and recovery in complex road networks," *Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics*, vol. 96, no. 5, Article ID 052301, 2017.

[34] L. D. Valdez, M. A. D. Muro, and L. A. Braunstein, "Failure-recovery model with competition between failures in complex networks: a dynamical approach," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 9, Article ID 093402, 2016.

[35] L. Böttcher, M. Luković, J. Nagler, S. Havlin, and H. J. Herrmann, "Failure and recovery in dynamical networks," *Scientific Reports*, vol. 7, Article ID 41729, 2017.

[36] A. Majdandzic, L. A. Braunstein, C. Curme et al., "Multiple tipping points and optimal repairing in interacting networks," *Nature Communications*, vol. 7, Article ID 10850, 2016.

[37] C. Liu, D. Li, E. Zio, and R. Kang, "Modeling framework for system restoration from cascading failures," *PLoS One*, vol. 9, no. 12, Article ID e112363, 2014.

[38] S. Hong, J. Zhu, L. A. Braunstein, T. Zhao, and Q. You, "Cascading failure and recovery of spatially interdependent networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 10, Article ID 103208, 2017.

[39] C. Liu, D. Li, B. Fu, S. Yang, Y. Wang, and G. Lu, "Modeling of self-healing against cascading overload failures in complex networks," *Europhysics Letters*, vol. 107, Article ID 68003, 2014.

[40] C. Fu, Y. Wang, Y. Gao, and X. Wang, "Complex networks repair strategies: dynamic models," *Physica A*, vol. 482, pp. 401–406, 2017.

[41] J. Gao, Y. Yin, L. Fiondella, and L. Liu, "Recovery of coupled networks after cascading failures," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 650–657, 2018.

[42] F. Hu, C. H. Yeun, S. Yang, W. Wang, and A. Zeng, "Recovery of infrastructure networks after localised attacks," *Scientific Reports*, vol. 6, Article ID 24522, 2016.

[43] C. Fu, Y. Wang, and X. Wang, "Research on complex networks' repairing characteristics due to cascading failure," *Physica A*, vol. 482, pp. 317–324, 2017.

[44] J. Wu, B. Fang, J. Fang, X. Chen, and C. K. Tse, "Sequential topology recovery of complex power systems based on reinforcement learning," *Physica A*, vol. 535, Article ID 122487, 2019.

[45] M. Stippingera and J. Kertészb, "Enhancing resilience of interdependent networks by healing," *Physica A*, vol. 416, pp. 481–487, 2014.

[46] W. Quattrociocchi, G. Caldarelli, and A. Scala, "Self-healing networks: redundancy and structure," *PLoS One*, vol. 9, no. 2, Article ID e87986, 2013.

[47] B. M. Waman, "Routing of multipoint connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.

[48] A. F. Rozenfeld, R. Cohen, D. ben Avraham, and S. Havlin, "Scale-free networks on lattices," *Physical Review Letters*, vol. 89, no. 21, Article ID 218701, 2002.

[49] M. M. Danziger, L. M. Shekhtman, Y. Berezin, and S. Havlin, "The effect of spatiality on multiplex networks," *Europhysics Letters*, vol. 115, no. 3, Article ID 36002, 2016.

[50] X.-J. Xu, X. Zhang, and J. F. F. Mendes, "Impacts of preference and geography on epidemic spreading," *Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics*, vol. 76, no. 5, Article ID 056109, 2007.

[51] S.-H. Yook, J. Hawoong, and A.-L. Barabási, "Modeling the internet's large-scale topology," *Proceedings of the National Academy of Sciences*, vol. 99, no. 21, pp. 13382–13386, 2002.

[52] M. Barthélemy, "Crossover from scale-free to spatial networks," *Europhysics Letters*, vol. 63, no. 6, pp. 915–921, 2003.

[53] J. Jost and M. P. Joy, "Evolving networks with distance preferences," *Physical Review E - Statistical Physics, Plasmas,*

Fluids, and Related Interdisciplinary Topics, vol. 66, no. 3, Article ID 036126, 2002.

[54] P. Hines, S. Blumsack, E. C. Sanchez, and C. Barrows, "The topological and electrical structure of power grids," in *Proceedings of the 43rd Hawaii International Conference on System Sciences, IEEE*, Article ID 11205846, Honolulu, HI, USA, January 2010.

[55] M. Ouyang, L. Hong, Z.-J. Mao, M.-H. Yu, and F. Qi, "A methodological approach to analyze vulnerability of interdependent infrastructures," *Simulation Modelling Practice and Theory*, vol. 17, no. 5, pp. 817–828, 2009.

[56] K.-S. Yan, L.-L. Rong, and Q. Li, "Vulnerability analysis of interdependent spatially embedded infrastructure networks under localized attack," *Modern Physics Letters B*, vol. 31, no. 9, Article ID 1750089, 2017.