Highlights

Effectiveness of Link-addition Strategies for Improving the Robustness of Both Multiplex and Interdependent Networks[⋆]

Yui Kazawa, Sho Tsugawa

- Link addition improves the robustness of multilayer networks against attacks.
- Link addition is more effective in multiplex network than in interdependent network.
- Link-addition strategies based on degree are generally more effective than others.

Effectiveness of Link-addition Strategies for Improving the Robustness of Both Multiplex and Interdependent Networks

Yui Kazawa[a], Sho Tsugawa[a,*]

[a] *Graduate School of Systems and Information Engineering, University of Tsukuba,*
1–1–1 Tennodai, Tsukuba, Ibaraki 305–8573, Japan

Abstract

Recent research trends in network science have shifted from the analysis of single-layer networks to that of multilayer networks. Two popular multilayer network models exist: interdependent networks and multiplex networks. This paper presents an extensive investigation of the effectiveness of link-addition strategies for improving the robustness of both interdependent and multiplex networks against degree-based targeted node attacks. The results demonstrate that link-addition strategies that are effective for interdependent networks are also effective for multiplex networks, suggesting that findings regarding such strategies for interdependent networks are also applicable to multiplex networks. Furthermore, the results demonstrate that the existing low-degree link-addition strategy for single-layer networks and its extensions proposed herein are relatively effective among the seven link-addition strategies investigated in this study.

Keywords: multiplex network, interdependent network, targeted attack, robustness, link addition

1. Introduction

Recent research trends in network science have shifted from the analysis of single-layer networks to that of multilayer networks [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. A multilayer network has multiple interacting layers of networks [2, 3], and many real-world complex systems have multilayer structures [2, 4]. For instance, in an infrastructure context, water supply systems, transportation systems, and power grids can be viewed as interdependent networks that compose a multilayer network [4]. Furthermore, the various types of multiple relationships among people can be viewed as constituting a multilayer network.

Two popular multilayer network models exist: interdependent and multiplex. An interdependent network comprises multiple layers (i.e., networks) whose nodes are interdependent [3]; if a node fails in a particular layer, then nodes in other layers that depend on the failed node will also fail [3, 4]. Meanwhile, a multiplex network is a collection of several network layers that contain the same nodes but with different intralayer connections [3]; in other words, each node in each layer has exactly one interlayer link with a node in each different layer. Each node in a layer is called a layer node, and each set of nodes that are connected via an interlayer links is called a multiplex node. Contrary to the interdependent network, even if a layer node fails in a particular layer, nodes in other layers that have interlayer links to the failed layer node will not fail in a multiplex network [10].

The robustness of multilayer networks has received significant attention [4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18]. The robustness of a network is its ability to maintain its connectivity against random node failures and intentional attacks on the network. For many systems defined as multilayer networks, it is desirable for them to maintain their overall connectivity even when some nodes fail. Consequently, the robustness of multilayer networks has attracted extensive research interest. Buldyrev *et al.* demonstrated that an interdependent network can be fragmented by a few nodes failing in a single layer as a result of cascading failures [4]. Parshani *et al.* demonstrated that the intersimilarity

[⋆] An earlier version of this paper was presented as a conference short paper [1]

[*] Corresponding author

Email address: s-tugawa@cs.tsukuba.ac.jp (Sho Tsugawa) between layers in an interdependent network affects the network's robustness [11]. Brummit *et al.* demonstrated that multiplex networks are generally more vulnerable than simple single-layer networks [6]. Min *et al.* demonstrated that the intersimilarity between layers in a multiplex network has a considerable effect on the robustness of such networks against failures and attacks [8].

Several methods for improving the robustness of interdependent networks have been examined in terms of their effectiveness [12, 13, 14, 15, 16, 17, 19, 18]. These methods include node protection to improve the robustness against targeted attacks [19] and increasing node capacities to improve the robustness against cascading failures [18].

To improve the robustness of a network, adding only a few connectivity links to the network appears promising based on the feasibility demonstrated in actual networks [17]. Ji *et al.* [17] proposed two link-addition strategies: (i) random inter degree–degree difference (RIDD) and (ii) low inter degree–degree difference (LIDD). Because interdependent networks with high levels of intersimilarity are known to be robust against random failures of nodes [11], the aim of both RIDD and LIDD is to increase the intersimilarity between layers through link addition. Ji *et al.* [17] demonstrated that both RIDD and LIDD are more effective at improving the robustness of an interdependent network against random failures than conventional link-addition strategies such as random addition (RA) and low degree (LD). Wang *et al.* [20] proposed improved versions of LIDD, RA, and LD and demonstrated their effectiveness.

We herein present a comprehensive evaluation of the effectiveness of several link-addition strategies for improving the robustness of both multiplex and interdependent networks against targeted node attacks. We investigate the effectiveness of existing link-addition strategies for interdependent networks (i.e., RIDD and LIDD), existing link-addition strategies for single-layer networks (i.e., LD and RA), and extensions of the aforementioned strategies, which we refer to as low-degree IDD (LD_IDD), low-degree-product IDD (LDP_IDD), and low-degree-sum IDD (LDS_IDD). Through extensive simulations, we investigate the effectiveness of these strategies for both interdependent and multiplex networks.

Our main contributions are as follows.

- We investigate the effectiveness of link-addition strategies for improving the robustness of interdependent networks against *targeted attacks*. Most previous studies investigated the effectiveness of link-addition strategies under random failures [17, 20], implying that the effectiveness of link-addition strategies against targeted attacks remains unclear.
- We investigate the effectiveness of link-addition strategies for improving the robustness of *multiplex* networks. Although a multiplex network is a representative model of multilayer networks, most previous studies focused on only interdependent networks, implying that methods for improving the robustness of multiplex networks remain limited [21].
- We propose extensions of existing link-addition strategies and investigate their effectiveness. For link addition, the proposed extensions use the degrees of nodes in each layer (as used in LD) and the intersimilarity between layers (as used in RIDD and LIDD).

The remainder of this paper is organized as follows. In Section 2, we introduce the definitions and notations used herein. In Section 3, we describe the link-addition procedures used in this study. In Section 4, we explain the experimental methodology of our network attack simulation. In Section 5, we present the results and discuss the simulation. In Section 6, we present our conclusions and describe future work.

2. Definitions and Notation

A multilayer network is denoted as $\mathcal{M} = (\mathcal{G}, C)$, where $\mathcal{G}$ is a set of layers and C is a set of interlayer links [3]. Each layer α is defined as an undirected unweighted network $G_\alpha = (V_\alpha, E_\alpha)$, where V_α and E_α are a set of nodes and a set of links, respectively. Let $E_{\alpha\beta}$ be a set of interlayer links connecting nodes between layer α and layer β; then, C is defined as $C = \{E_{\alpha\beta} \subseteq V_\alpha \times V_\beta; \alpha, \beta \in \{1, \ldots, M\}; \alpha \neq \beta\}$, where M is the number of layers in $\mathcal{M}$. Interdependent networks and multiplex networks are special cases of multilayer networks.

An interdependent network exhibits interdependent relationships between different layers [3]. In an interdependent network, the interlayer link $(v_i^\alpha, v_i^\beta) \in E_{\alpha\beta}$ represents node v_i^α depending on node v_i^β, and vice versa. In other words, if

$(v_i^\alpha, v_i^\beta) \in E_{\alpha\beta}$ and node v_i^α (or v_i^β) is removed from the network, then v_i^β (or v_i^α) is also removed from the network [4, 17]. Herein, we consider a one-to-one interdependent network (i.e., each node has one and only one interlayer link) [4].

A multiplex network comprises a fixed set of nodes connected by different types of links, and different layers in a multiplex network represent different types of links [3]. Each node in a layer is called a layer node, and each set of nodes that are connected via interlayer links is called a multiplex node [10]. Let N be the number of nodes in a multiplex network, then a set of layer nodes is denoted as $V_\alpha = \{v_1^\alpha, v_2^\alpha, \dots, v_N^\alpha\}$ and a set of multiplex nodes is denoted as $V = \{v_1, v_2, \dots, v_N\}$. Note that $v_i = \{v_i^1, v_i^2, \dots, v_i^M\}$. For any combinations of layers α and β, $|V_\alpha| = |V_\beta|$ and $(v_i^\alpha, v_i^\beta) \in E_{\alpha\beta}$. Two multiplex nodes $v_i \in V$ and $v_j \in V$ are considered to be connected if they are connected in at least one layer [10]. In other words, a set of links connecting multiplex nodes is defined as $E = E_1 \oplus E_2 \oplus \cdots \oplus E_M$.

This study refers to previous studies [8, 10, 17] and considers two-layer networks, in which the two layers are denoted as G_A and G_B. Each node in graphs G_A and G_B is denoted as $v_i^A (i = 1, \dots, N)$ and $v_i^B (i = 1, \dots, N)$, respectively, and v_i^A and v_i^B are connected via an interlayer link.

3. Link-addition Strategy

In this section, we introduce the link-addition strategies used in this study. Following [10], we consider the problem of adding links to two-layer networks. Each link-addition strategy has a fixed budget of M' links and repeats the procedure that will be explained later in this section until all M' of those links have been added. For each link-addition strategy, (i) self-loop and parallel edges are not allowed and (ii) the degrees of layer nodes are calculated at each step.

3.1. Link-addition Strategies for Single-layer Networks

LD, in which links are added between low-degree nodes, is a popular link-addition strategy for single-layer networks [22]. Moreover, RA [23, 24], in which links are added at random, is often used as a reference for comparison with other link-addition strategies. The detailed procedures of LD and RA are as follows.

LD. At each step, the degrees of all the nodes in G_A and G_B are calculated. In both G_A and G_B, a link is added between a pair of unconnected nodes with the lowest degrees.

RA. In both G_A and G_B, a link is added between a randomly selected pair of unconnected nodes.

Although a link addition strategy that adds links to high-degree nodes has been studied in [22], we do not use such strategies in this study. Such high-degree-based link-addition strategies are expected to be ineffective under the degree-based targeted node attack studied herein as the additional links added by the high-degree-based link-addition strategies are always removed by the attacker.

3.2. Link-addition Strategies Using IDD

Ji *et al.* [17] proposed the RIDD and LIDD link-addition strategies, in which links are added based on the IDD, which is defined as the degree difference between two interconnecting nodes. Because it has been shown that networks with high intersimilarities (i.e., networks with low average inter degree–degree difference (AIDD)) are robust against random failures, both strategies are aimed at reducing the AIDD, which is calculated as the average absolute IDD per node in an interdependent network [17]. Let u and v be nodes in graphs G_A and G_B, respectively, where u has an interlayer link with v. Then, the IDD of u in G_A is defined as $IDD(u) = k_u - k_v$, where k_u and k_v are the degrees of u and v, respectively. The detailed procedures of RIDD and LIDD are as follows.

RIDD. At each step, the IDD of each node in G_A and G_B is calculated. For both G_A and G_B, a link is added between a pair of nodes selected randomly from the pairs of unconnected nodes with negative IDD. If no pair of nodes has a negative IDD, then a link is added between randomly selected unconnected nodes.

LIDD. At each step, the IDD of each node in G_A and G_B is calculated. For both G_A and G_B, a link is added between the pair of unconnected nodes with the lowest negative IDD. If no pair of nodes has a negative IDD, then a link is added between the pair of unconnected nodes with the lowest degree. While RIDD selects a pair of nodes to add a link randomly from the nodes with negative IDD, LIDD adds a link between the pair of unconnected nodes with the lowest negative IDD.

3.3. Link-addition Strategies Using IDD and Degrees of Layer Nodes

We propose three link-addition strategies that consider both the IDD and the degrees of layer nodes: (i) low-degree IDD (LD_IDD), (ii) low-degree-product IDD (LDP_IDD), and (iii) low-degree-sum IDD (LDS_IDD). Similar to RIDD and LIDD, LD_IDD involves adding links between nodes with negative IDD but with a preference for adding links to low-degree nodes, such nodes being vulnerable to both attacks and failures [25]. Specifically, low-degree nodes tend to be isolated during attacks and failures because their connectivity depends heavily on other nodes of higher degrees. Therefore, LD_IDD involves adding links to low-degree nodes while reducing the AIDD in the network. Note that the LD link-addition strategy for single-layer networks also involves adding links to low-degree nodes [22]. LDP_IDD and LDS_IDD are variants of LD_IDD: LDP_IDD uses the layer degree product (i.e., the product of the degrees of two interconnecting nodes) and LDS_IDD uses the layer degree sum (i.e., the sum of degrees of two interconnecting nodes) instead of using only the degrees of nodes in each layer. The layer degree product is defined as $DP(u) = DP(v) = k_u \times k_v$ and the degree sum is defined as $DS(u) = DS(v) = k_u + k_v$, where k_u and k_v are the degrees of interconnecting nodes u and v, respectively. These measures are used to quantify the importance of nodes in multiplex networks [3, 26].

The detailed procedures of LD_IDD, LDP_IDD, and LDP_IDD are as follows.

LD_IDD. At each step, the IDD and the degree of all nodes in both G_A and G_B are calculated. In both G_A and G_B, a link is added between the pair of unconnected nodes with the lowest degree and negative IDD. If no pair of nodes has a negative IDD, then a link is added between randomly selected unconnected nodes.

LDP_IDD. At each step, the IDD and the degree product of all nodes in both G_A and G_B are calculated. In both G_A and G_B, a link is added between the pair of unconnected nodes with the lowest degree product and negative IDD, except when the degree product is zero. While LD_IDD uses the node degree, LDP_IDD uses the degree product of a node. If no pair of nodes has a negative IDD, then a link is added between randomly selected unconnected nodes.

LDS_IDD. At each step, the IDD and the degree sum of all nodes in both G_A and G_B are calculated. In both G_A and G_B, a link is added between the pair of unconnected nodes with the lowest degree sum and negative IDD. While LD_IDD uses the node degree, LDS_IDD uses the degree sum of a node. If no pair of nodes has a negative IDD, then a link is added between randomly selected unconnected nodes with the lowest degree sum.

4. Methodology

4.1. Overview

Following [21], we conducted experiments by performing the following steps. 1) Generate a two-layer network using various network generation models. 2) Add links to both layers of the generated network using the link-addition strategies described in Section 3. 3) Simulate an attack on the network and investigate the connectivity of the remaining network. The details of these three steps are explained in the remainder of this section.

4.2. Generating Network

We generate a two-layer network $\mathcal{M}$ by connecting two single-layer networks. We generate two graphs G_A and G_B with the same size N. For each node in G_A, an interlayer link is created between that node and a randomly selected node in G_B to construct an uncorrelated structure.

We use the following models to generate the single-layer networks: the Barabási–Albert (BA) model [27], community emergence (CE) model proposed by Kumpula *et al.* [28], and Erdös–Rényi (ER) model [29]. We generate six types of multilayer networks: (i) BA–BA network, (ii) CE–CE network, (iii) ER–ER network, (iv) BA–ER network, (v) CE–BA network, and (vi) CE–ER network. The BA model that generates scale-free networks and the ER model that generates random networks are popular models used to generate artificial networks. The CE model generates networks that have a skewed degree distribution and tunable community structure. Although the CE model generates weighted graphs, we ignore weighting herein and treat the generated graph as an unweighted undirected graph.

We generated 10 two-layer networks. Unless explicitly stated, the number of nodes $N = 1,000$ in the following experiments. We constructed a BA graph with $m = 2.0$, an ER graph with $p = 0.004$, and a CE graph with $\delta = 2.0$,

$p\delta = 0.004$, $p_r = 0.001$, and $p_d = 0.001$. The parameters used to generate the CE and ER graphs were determined based on values that render the density of the graphs approximately equivalent to that of the BA graph. The number of links in the BA graph was 1,997, 2,004.8 in the CE graphs, and 2,006.7 in the ER graphs.

4.3. Network Attack Simulation

We simulated a targeted node attack to investigate the robustness of multilayer networks with additional links. We began by adding $M'/2$ links to graphs G_A and G_B based on the link-addition strategies described in Section 3. We define the fraction of links added to the multilayer network $\mathcal{M}$ as $fa = M'/(M_A + M_B)$, where M_A and M_B are the numbers of links for G_A and G_B, respectively.

Interdependent Networks. For interdependent networks, following [5], we simulated a targeted node attack as follows.

1. Remove $N \times \phi_A$ nodes from G_A in descending order of their degree.
2. Remove nodes that do not belong to the giant component in G_A.
3. In G_B, remove all nodes that have interlayer links with the nodes removed from G_A.
4. Remove nodes that do not belong to the giant component in G_B.
5. In G_A, remove all nodes that have interlayer links with the nodes removed from G_B.
6. Repeat procedures 2–5 while no removed nodes exist in the procedures.

To evaluate the connectivity of interdependent networks after a network attack, we calculated $R = (N'_A + N'_B)/(N_A + N_B)$, where N'_A and N'_B are the numbers of nodes remaining in networks G_A and G_B, respectively, after the network attack. Note that by the definition of interdependent networks, $N'_A = N'_B$.

Multiplex Networks. For multiplex networks, we simulated a layer node-based attack similar to that in [10]. We removed $N \times \phi_A$ nodes from G_A and $N \times \phi_B$ nodes from G_B in the descending order of their degree. Subsequently, we removed nodes that were not part of the largest components of G_A and G_B. Finally, we calculated the size of the mutually connected giant component (MCGC), which is a common measure of the robustness of multiplex networks [3, 4, 10]. Note that the MCGC is a set of connected multiplex nodes [10], which are regarded as connected if they have links on at least one layer [10]. We used the normalized size R of the MCGC, which is defined as the number of nodes belonging to the MCGC normalized by the number of nodes N in the network.

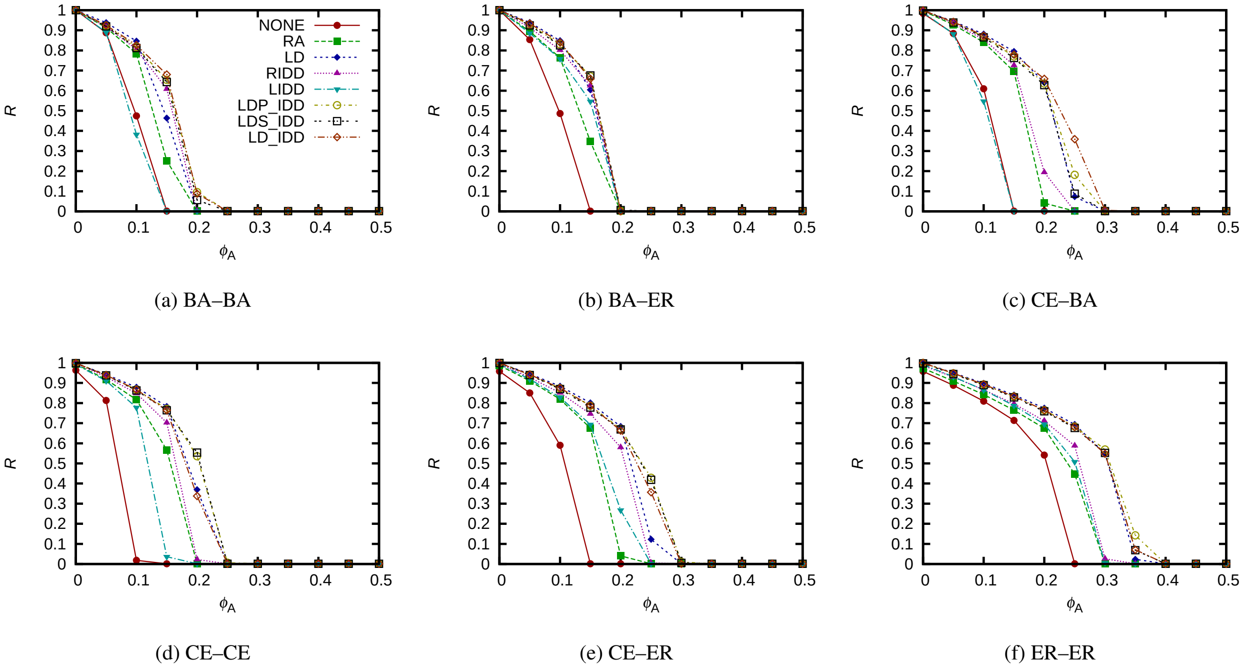
For each network and link-addition strategy, we performed 10 independent simulations of link addition and node removal. Subsequently, we obtained the average value of R from 100 independent simulation runs for each link-addition strategy. Although other possible measures can be used for evaluating the robustness of networks (e.g., [30]), we used the R values for evaluating the robustness of multilayer networks following the existing studies regarding link addition for multilayer networks [20, 17].

5. Results and Discussion

5.1. Robustness of Interdependent Networks

To evaluate the effectiveness of the link-addition strategies for interdependent networks, we investigated the robustness of interdependent networks when using each strategy. Figure 1 shows the relative number R of remaining nodes versus the fraction ϕ_A of removed nodes. We used $fa = 0.10$, which corresponds to a low budget of links to be added. For comparison purposes, the graphs in Fig. 1 include results with no link addition (denoted as *NONE*).

Figure 1 shows that the existing link-addition strategies and our extensions to them (i.e., LD_IDD, LDP_IDD, and LDS_IDD) improve the robustness of interdependent networks against degree-based attacks. Among the seven strategies, LD, LD_IDD, LDP_IDD, and LDS_IDD are the most effective. Although RIDD and LIDD have been reported as being more effective than LD and RA against random node failures [17], the present results suggest that LD is more effective than RIDD and LIDD against targeted attacks. Comparing LD with the three extensions that use node degree and IDD, the extensions achieve higher R values than LD in some cases (e.g., BA–BA and CE–BA networks). However, the differences are slight. The difference among different networks shows that BA–BA, BA–ER, and CE–BA networks are less robust than other networks even if link-addition strategies are applied. BA



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 1: Fraction R of nodes remaining after a degree-based attack versus fraction of nodes removed from G_A for $fa = 0.10$, and $N = 1,000$ (interdependent networks).

networks have a power-law degree distribution, and such networks are shown to less robust against degree-based targeted attacks [4, 5]. Therefore, interdependent networks composed of BA networks tend to be less robust.

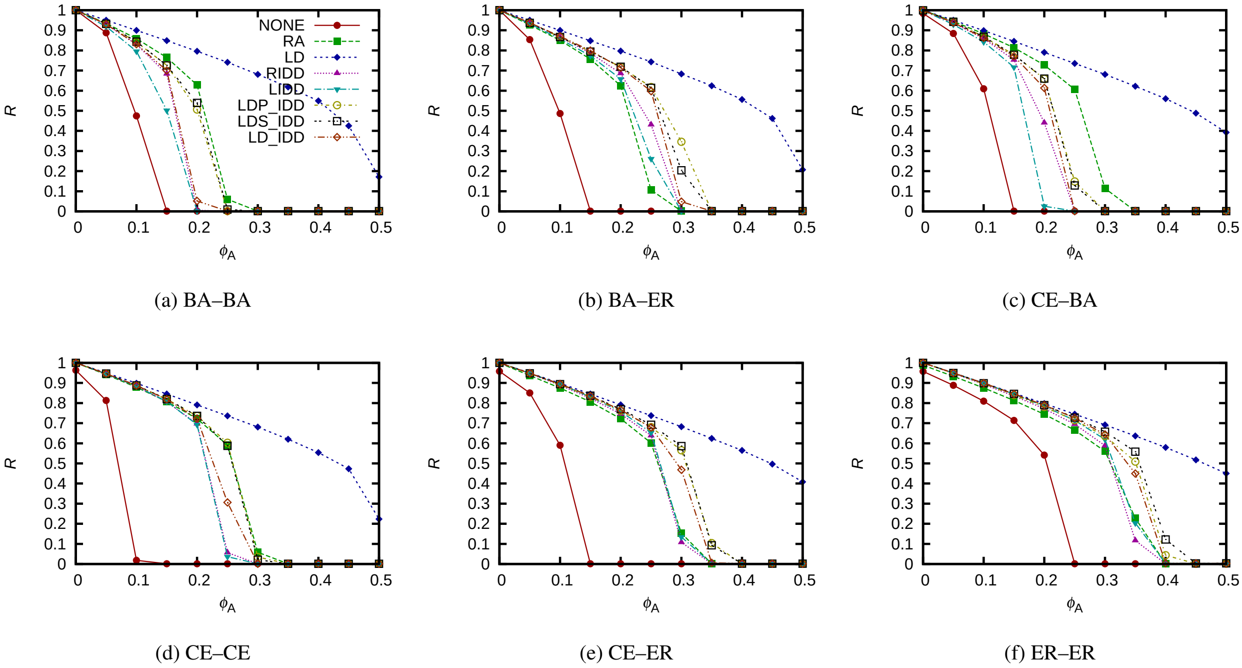
Next, we investigate the effectiveness of the strategies when more links are available to be added compared with the previous results. Figure 2 shows the relative number of remaining nodes versus the fraction ϕ_A of removed nodes for $fa = 0.30$. These results show that LD achieves much higher R values than the other strategies. This suggests that when many links are to the networks, LD is the best strategy. However, this is surprising given that LD was designed for single-layer networks; therefore, we investigate the cause in Section 5.3.

Furthermore, we investigate the effectiveness of the link-addition strategies for larger networks. Figure 3 shows the relative number of remaining nodes versus the fraction ϕ_A for networks with $N = 5,000$ nodes. The parameters used for network generation were the same as those for generating $N = 1,000$ networks. Here, the fraction of added links $fa = 0.10$. These results show that overall, similar to the results for $N = 1,000$, LD, LD_IDD, LDP_IDD, and LDS_IDD are relatively effective. This suggests that the network size does not significantly affect the effectiveness of the link-addition strategies. Degree-based strategies are suggested as a better approach than strategies that consider only IDD (i.e., RIDD and LIDD). Note that owing to the parameter setting when generating the ER networks, ER networks with $N = 5,000$ are extremely dense; therefore, the results for the ER–ER network are almost the same regardless of the link addition strategy.

5.2. Robustness of Multiplex Networks

Next, we investigate the effectiveness of the link-addition strategies for multiplex networks. Figure 4 shows the relative size of MCGC R versus the fraction ϕ_A of removed nodes, for which we used $fa = 0.10$ and $\phi_B = 0.40$.

These results indicate that the link-addition strategies improve the robustness of multiplex networks. The R values when using the link-addition strategies are much higher than those with no link addition. These results indicate that the link-addition strategies for interdependent networks can also be used to improve the robustness of multiplex networks. Among the seven strategies, LD, LD_IDD, LDP_IDD, and LDS_IDD are the most effective. The difference among different networks shows that BA–BA, BA–ER, and CE–BA networks are less robust than other networks. These tendencies are similar to the results for interdependent networks.



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 2: Fraction R of nodes remaining after a degree-based attack versus the fraction of nodes removed from G_A for $fa = 0.30$, and $N = 1,000$ (interdependent networks).

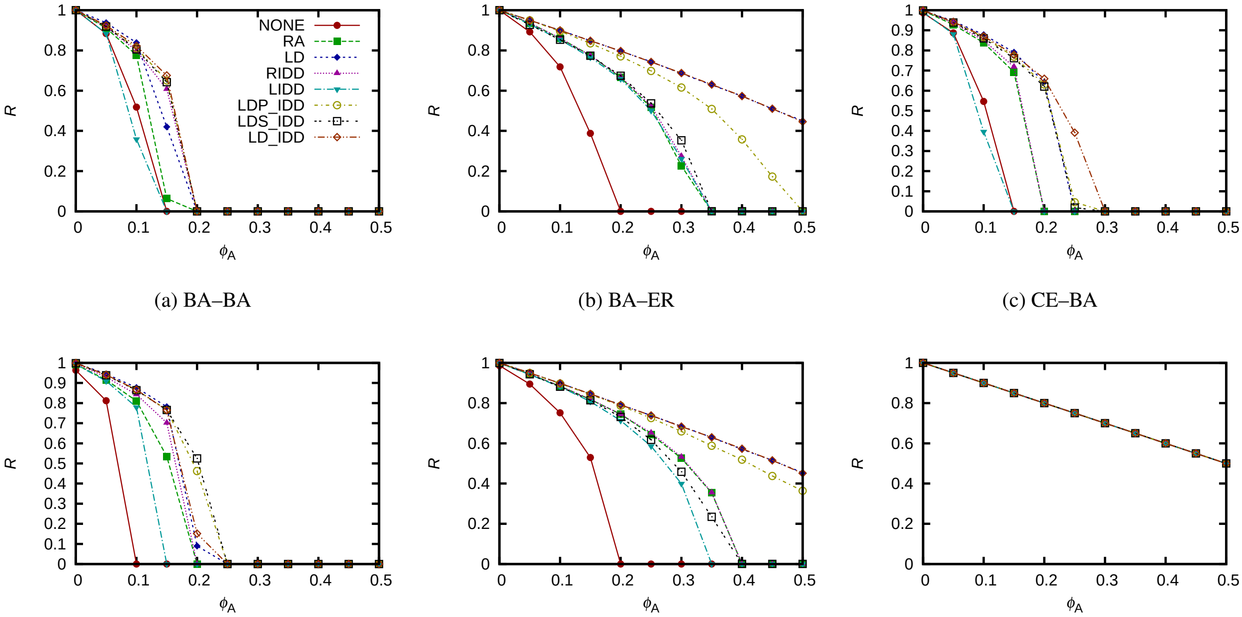
Figure 5 shows the results for $fa = 0.20$ and $\phi_B = 0.40$, which correspond to more links being available for addition compared with the previous results. Again, these results demonstrate the effectiveness of LD. Regarding the results in the previous subsection, LD achieves much higher R values than the other strategies. This suggests that when many links can be added in multiplex networks, LD is the best option.

We finally investigate the effectiveness of the link-addition strategies for larger multiplex networks. Figure 6 shows the relative size of MCGC R versus the fraction ϕ_A of removed nodes, for networks with $N = 5,000$ nodes. Here, $fa = 0.10$ and $\phi_B = 0.40$ are used. Similarly, these results demonstrate that LD, LD_IDD, LDP_IDD, and LDS_IDD are relatively effective, and that the network size does not significantly affect the effectiveness of the link-addition strategies. Note that owing to the parameter setting when generating ER networks, ER networks with $N = 5,000$ are extremely dense; consequently, the R values for the BA–ER, CE–ER, and ER–ER networks are large.

Our main findings can be summarized as follows. 1) Link-addition strategies are effective for improving the robustness of both interdependent and multiplex networks against targeted node attacks. 2) Among the seven strategies used herein, LD, LD_IDD, LDP_IDD, and LDS_IDD are the most effective. 3) When many links can be added to the networks, LD (which was designed for single-layer networks) is unexpectedly effective for both interdependent and multiplex networks.

5.3. Discussion

This subsection discusses our experimental results. First, we consider why some strategies are better than others. A network attack may remove links that are added by one of the link-addition strategies. If such an attack removes many such added links, then the latter are ineffective for improving network robustness. Degree-based attacks remove high-degree nodes. Therefore, links added to high-degree nodes tend to be ineffective. By contrast, links added to low-degree nodes tend not to be removed by the attacks. This may be why low-degree based strategies (i.e., LD, LD_IDD, LDP_IDD, and LDS_IDD) are effective than others. To confirm the hypothesis above, we compare the numbers of such ineffective links added by the link-addition strategies. Figures 7–10 show the number of links added by each link-addition strategy that are then deleted by the network attack divided by the number of added links. Hereinafter, we only show the results for $N = 1,000$.



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

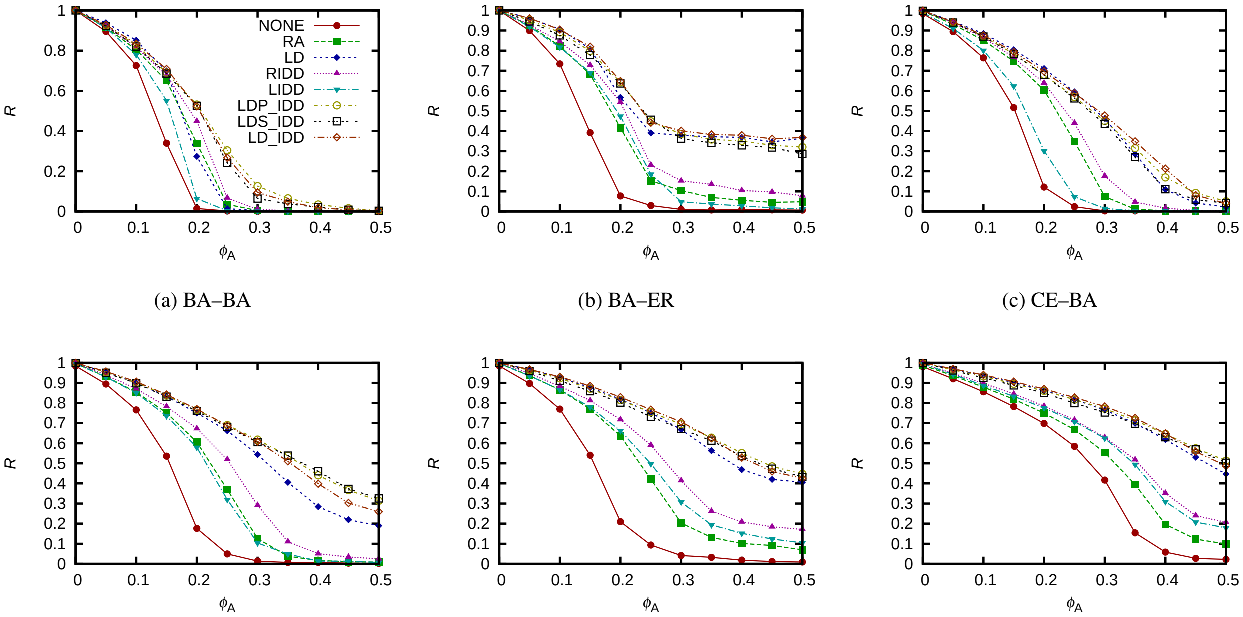
Figure 3: Fraction R of nodes remaining after a degree-based attack versus the fraction of nodes removed from G_A for $fa = 0.10$, and $N = 5,000$ (interdependent networks).

These figures show that the fractions of deleted links with LD, LD_IDD, LDS_IDD, and LDP_IDD are smaller than those with other strategies. These results confirm our hypothesis. In particular, when fa is large, the fractions of deleted links with LD are the smallest. This is why LD is more effective than the other strategies, particularly when fa is large. This result also suggests that the effectiveness of the selected link-addition strategy depends on the attack strategy, and that it is important to investigate the effectiveness of link-addition strategies for different attack strategies in the future.

Next, we examine the difference and similarity between the results of interdependent and multiplex networks. Focusing on the difference between interdependent and multiplex networks, link-addition strategies are more effective in multiplex networks than in interdependent networks under the similar attack strength. For instance, Fig. 1(b) shows that in the BA–ER multiplex network when $\phi_A = 0.3$, LD achieves approximately $R = 0.4$, which is approximately 0.4 higher than that without using link-addition strategies. By contrast, Fig. 4(b) shows that in the BA–ER interdependent network when $\phi_A = 0.3$, LD achieves approximately $R = 0$. This suggests that under similar sizes of network attacks, link-addition strategies are more effective for multiplex networks than for interdependent networks. This is because in multiplex networks, multiplex nodes are regarded as connected if they have links on at least one layer. Therefore, as shown in Figs. 7–10, multiplex networks have considerably fewer ineffective links than interdependent networks. Focusing on the similarity between interdependent and multiplex networks, link-addition strategies effective for interdependent networks are also effective for multiplex networks (and vice versa). As discussed above, low-degree based strategies have fewer ineffective links both in interdependent and multiplex networks, which results in their effectiveness.

6. Conclusions and Future Work

We herein provided an extensive analysis of the effectiveness of link-addition strategies for improving the robustness of both interdependent and multiplex networks against targeted node attacks. We demonstrated that link-addition strategies are effective for both interdependent and multiplex networks. Moreover, the link-addition strategies for



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 4: Relative size of MCGC R under a degree-based attack versus fraction of nodes removed from G_A for $fa = 0.10$, $\phi_B = 0.40$, and $N = 1,000$ (multiplex networks).

multiplex networks were similarly (or even more) effective than those for interdependent networks. Several studies regarding link-addition strategies for interdependent networks have been performed; however, those for multiplex networks are few. Our results suggest that the findings regarding interdependent networks are applicable to multiplex networks. Furthermore, we demonstrated that the LD strategy, which was designed for single-layer networks, was unexpectedly effective. Strategies combining node degree and IDD (i.e., LD_IDD, LDP_IDD, and LDS_IDD) were effective when the budget for link addition was limited (i.e., the number of added links is small). Overall, degree-based strategies were shown to be effective against targeted attacks.

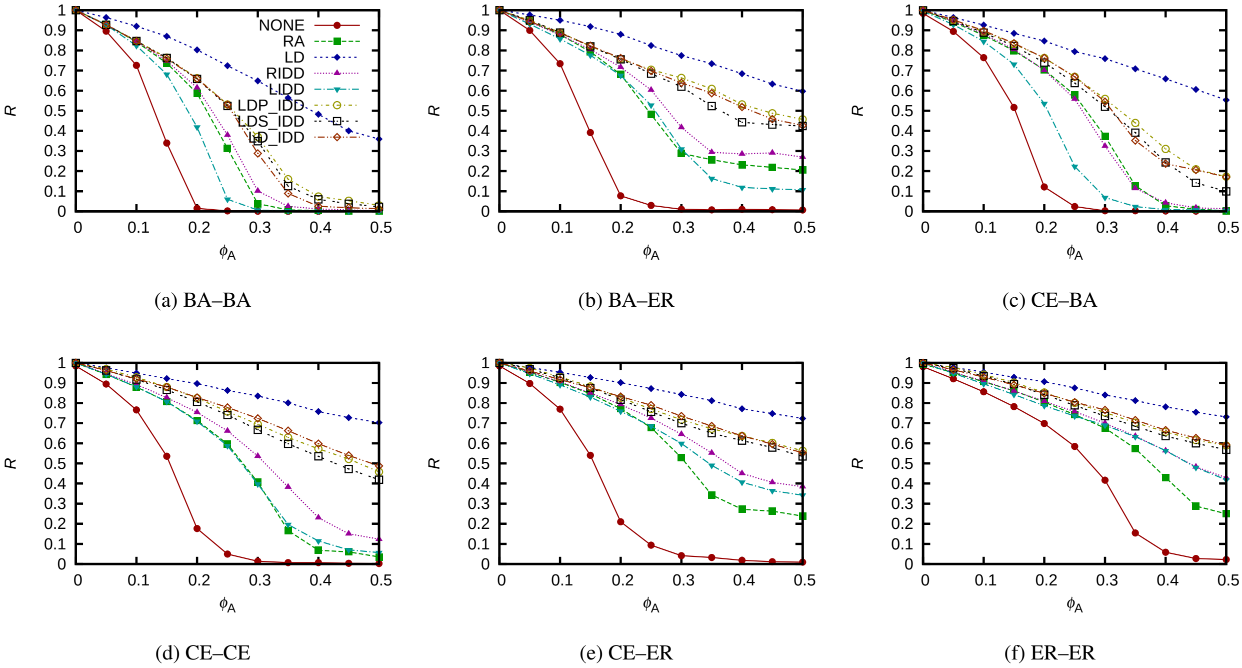
We recognized the limitations in this study, and they suggest directions for future work. First, to fully understand the effectiveness of link-addition strategies for improving the robustness of multilayer networks, theoretical analyses should be provided. This paper provides numerical results; however, in future work, we plan to provide analytical results. Next, we used only strategies involving the addition of links between layer nodes (i.e., we only used intralink addition strategies). By contrast, strategies involving the addition of interlayer links exist [31, 32]. By combining intralink and interlayer link addition strategies, the robustness of multilayer networks can be improved with lower costs than by using only intralink addition strategies. Additionally, it is important to study network recovery after a network failure. Network recovery problems have been studied recently [33, 34, 35, 36, 37]; furthermore, the effectiveness of link-addition strategies to such problems can be investigated in future work. Finally, the effectiveness of link-addition strategies against attack strategies other than degree-based attacks should be investigated.

Acknowledgments

This work was partly supported by JSPS KAKENHI Grant Number 16K20931 and 19K11917.

References

[1] Y. Kazawa, S. Tsugawa, Proposal of strategic link addition for improving the robustness of multiplex networks, in: Proceedings of the 9th International Conference on Complex Networks (CompleNet'18), 2018, pp. 75–84.



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 5: Relative size of MCGC R under a degree-based attack versus fraction of nodes removed from G_A for $fa = 0.20$, $\phi_B = 0.40$, and $N = 1,000$ (multiplex networks).

[2] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, M. A. Porter, Multilayer networks, Journal of Complex Networks 2 (3) (2014) 203–271.

[3] S. Boccaletti, G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, M. Zanin, The structure and dynamics of multilayer networks, Physics Reports 544 (1) (2014) 1–122.

[4] 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.

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

[6] C. D. Brummitt, K.-M. Lee, K.-I. Goh, Multiplexity-facilitated cascades in networks, Physical Review E 85 (4) (2012) 045102.

[7] K.-M. Lee, J. Y. Kim, W.-k. Cho, K.-I. Goh, I. Kim, Correlated multiplexity and connectivity of multiplex random networks, New Journal of Physics 14 (3) (2012) 033027.

[8] B. Min, S. Do Yi, K.-M. Lee, K.-I. Goh, Network robustness of multiplex networks with interlayer degree correlations, Physical Review E 89 (4) (2014) 042811.

[9] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering & System Safety 121 (2014) 43–60.

[10] D.-w. Zhao, L.-h. Wang, Y.-f. Zhi, J. Zhang, Z. Wang, The robustness of multiplex networks under layer node-based attack, Scientific Reports 6 (2016).

[11] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, S. Havlin, Inter-similarity between coupled networks, Europhysics Letters 92 (6) (2011) 68002.

[12] J. Shao, S. V. Buldyrev, S. Havlin, H. E. Stanley, Cascade of failures in coupled network systems with multiple support-dependence relations, Physical Review E 83 (3) (2011) 036116.

[13] D. Zhou, H. E. Stanley, G. D'Agostino, A. Scala, Assortativity decreases the robustness of interdependent networks, Physical Review E 86 (6) (2012) 066103.

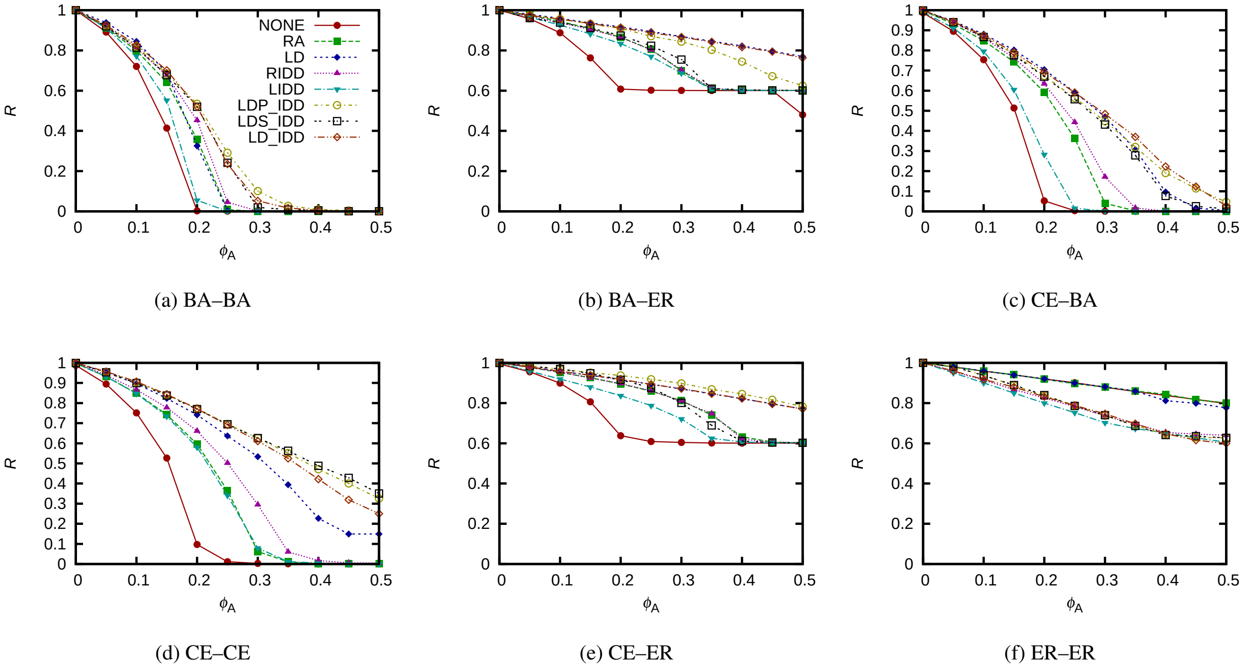
[14] D. T. Nguyen, Y. Shen, M. T. Thai, Detecting critical nodes in interdependent power networks for vulnerability assessment, IEEE Transactions on Smart Grid 4 (1) (2013) 151–159.

[15] S. Ruj, A. Pal, Analyzing cascading failures in smart grids under random and targeted attacks, in: Proceedings of AINA'14, 2014, pp. 226–233.

[16] S. D. Reis, Y. Hu, A. Babino, J. S. Andrade Jr, S. Canals, M. Sigman, H. A. Makse, Avoiding catastrophic failure in correlated networks of networks, Nature Physics 10 (10) (2014) 762–767.

[17] X. Ji, B. Wang, D. Liu, G. Chen, F. Tang, D. Wei, L. Tu, Improving interdependent networks robustness by adding connectivity links, Physica A: Statistical Mechanics and its Applications 444 (2016) 9–19.

[18] Z. Zhao, P. Zhang, H. Yang, Cascading failures in interconnected networks with dynamical redistribution of loads, Physica A: Statistical



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 6: Relative size of MCGC R under a degree-based attack versus fraction of nodes removed from G_A for $fa = 0.10$, $\phi_B = 0.40$, and $N = 5,000$ (multiplex networks).

Mechanics and its Applications 433 (2015) 204–210.

[19] R. Du, G. Dong, L. Tian, R. Liu, Targeted attack on networks coupled by connectivity and dependency links, Physica A: Statistical Mechanics and its Applications 450 (2016) 687–699.

[20] X. Wang, J. Cao, R. Li, T. Zhao, A preferential attachment strategy for connectivity link addition strategy in improving the robustness of interdependent networks, Physica A: Statistical Mechanics and its Applications 483 (2017) 412 – 422.

[21] Y. Kazawa, S. Tsugawa, On the effectiveness of link addition for improving robustness of multiplex networks against layer node-based attack, in: Proceedings of the 41st Annual IEEE International Computers, Software, and Applications Conference (Student Research Symposium), 2017, pp. 697–700.

[22] J. Zhao, K. Xu, Enhancing the robustness of scale-free networks, Journal of Physics A: Mathematical and Theoretical 42 (19) (2009) 195003.

[23] A. Beygelzimer, G. Grinstein, R. Linsker, I. Rish, Improving network robustness by edge modification, Physica A: Statistical Mechanics and its Applications 357 (3) (2005) 593–612.

[24] X.-B. Cao, C. Hong, W.-B. Du, J. Zhang, Improving the network robustness against cascading failures by adding links, Chaos, Solitons & Fractals 57 (2013) 35–40.

[25] A.-L. Barabási, F. Jennifer, Linked: The New Science of Networks Science of Networks, Basic Books, 2002.

[26] C. Pu, S. Li, X. Yang, J. Yang, K. Wang, Information transport in multiplex networks, Physica A: Statistical Mechanics and its Applications 447 (2016) 261–269.

[27] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.

[28] J. M. Kumpula, J.-P. Onnela, J. Saramäki, J. Kertesz, K. Kaski, Model of community emergence in weighted social networks, Computer Physics Communications 180 (4) (2009) 517–522.

[29] P. Erdös, A. Rényi, On random graphs I, Publ. Math. Debrecen 6 (1959) 290–297.

[30] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, H. J. Herrmann, Mitigation of malicious attacks on networks, Proceedings of the National Academy of Sciences 108 (10) (2011) 3838–3841.

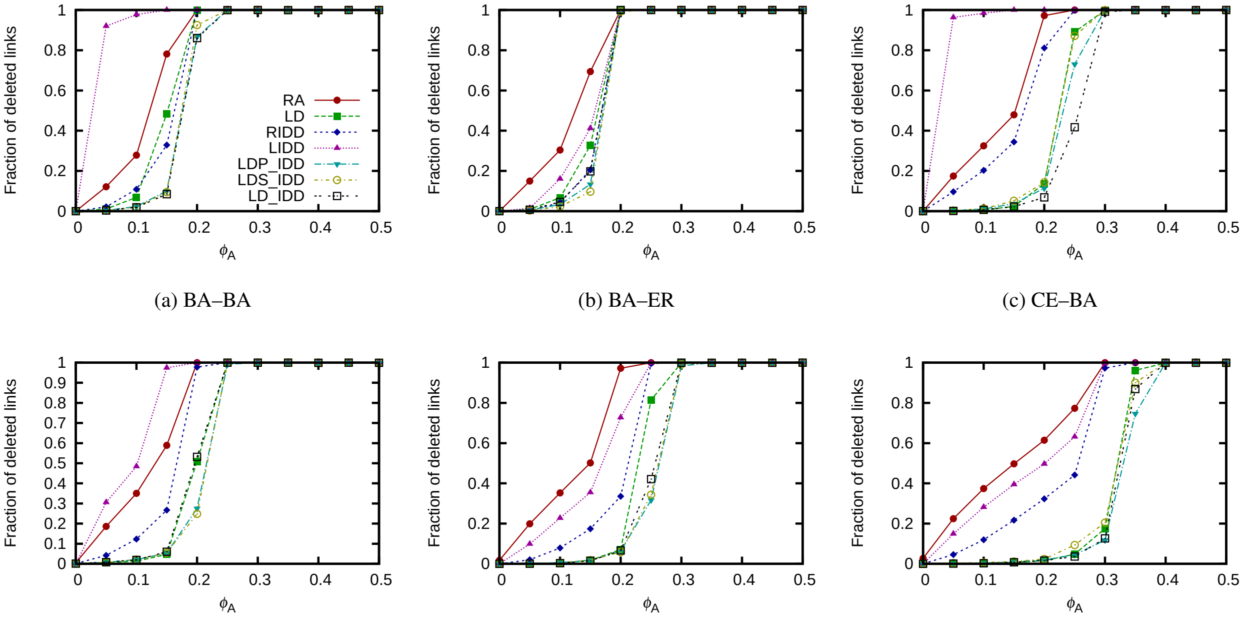
[31] P. Cui, P. Zhu, K. Wang, P. Xun, Z. Xia, Enhancing robustness of interdependent network by adding connectivity and dependence links, Physica A: Statistical Mechanics and its Applications 497 (2018) 185 – 197.

[32] X. Wang, W. Zhou, R. Li, J. Cao, X. Lin, Improving robustness of interdependent networks by a new coupling strategy, Physica A: Statistical Mechanics and its Applications 492 (2018) 1075 – 1080.

[33] G. Dong, J. Fan, L. M. Shekhtman, S. Shai, R. Du, L. Tian, X. Chen, H. E. Stanley, S. Havlin, Resilience of networks with community structure behaves as if under an external field, Proceedings of the National Academy of Sciences 115 (27) (2018) 6911–6915.

[34] L. Böttcher, M. Luković, J. Nagler, S. Havlin, H. J. Herrmann, Failure and recovery in dynamical networks, Scientific Reports 7 (2017) 41729.

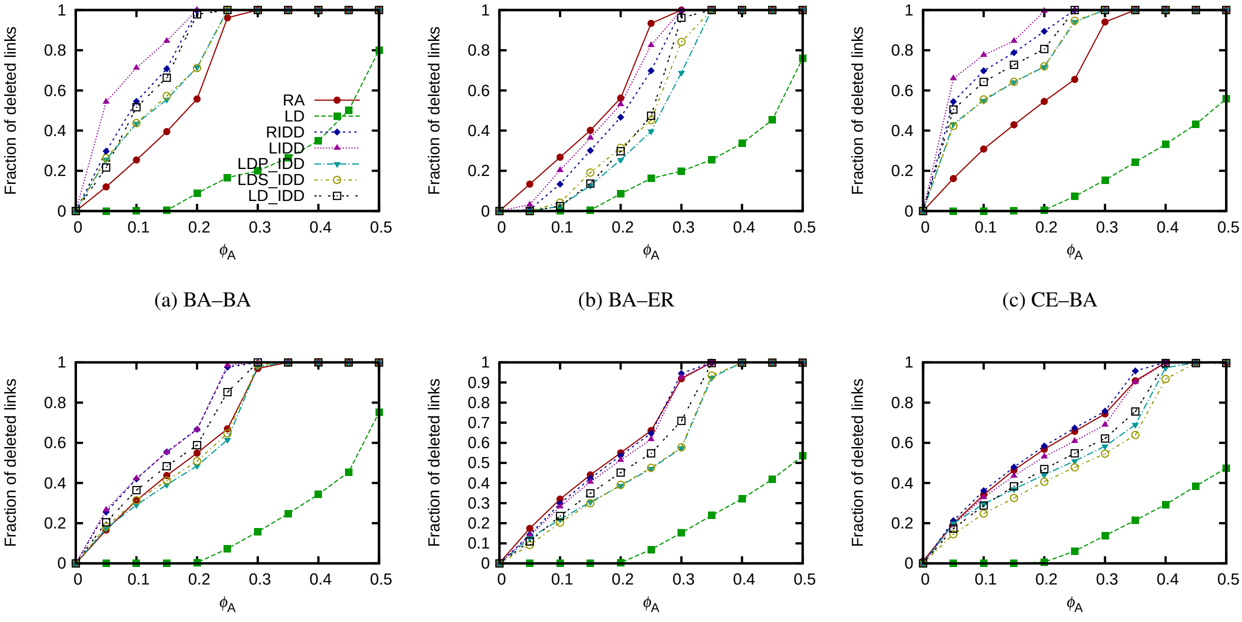
[35] M. Stippinger, J. Kertész, Enhancing resilience of interdependent networks by healing, Physica A: Statistical Mechanics and its Applications 416 (2014) 481–487.



(a) BA–BA (b) BA–ER (c) CE–BA

(d) CE–CE (e) CE–ER (f) ER–ER

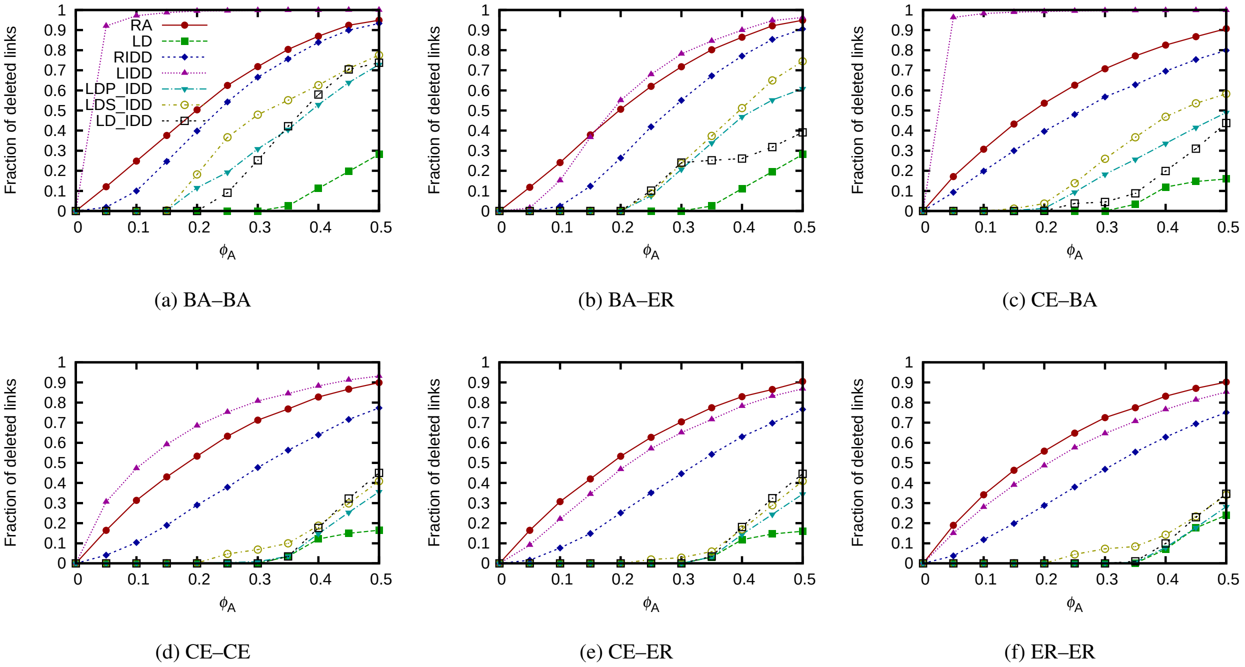
Figure 7: Fraction of added links that are subsequently deleted by a degree-based attack versus fraction of nodes removed from G_A (interdependent network, $fa = 0.10$), $N = 1,000$.



(a) BA–BA (b) BA–ER (c) CE–BA

(d) CE–CE (e) CE–ER (f) ER–ER

Figure 8: Fraction of added links that are subsequently deleted by a degree-based attack versus fraction of nodes removed from G_A (interdependent network, $fa = 0.30$, $N = 1,000$).



(a) BA–BA

(b) BA–ER

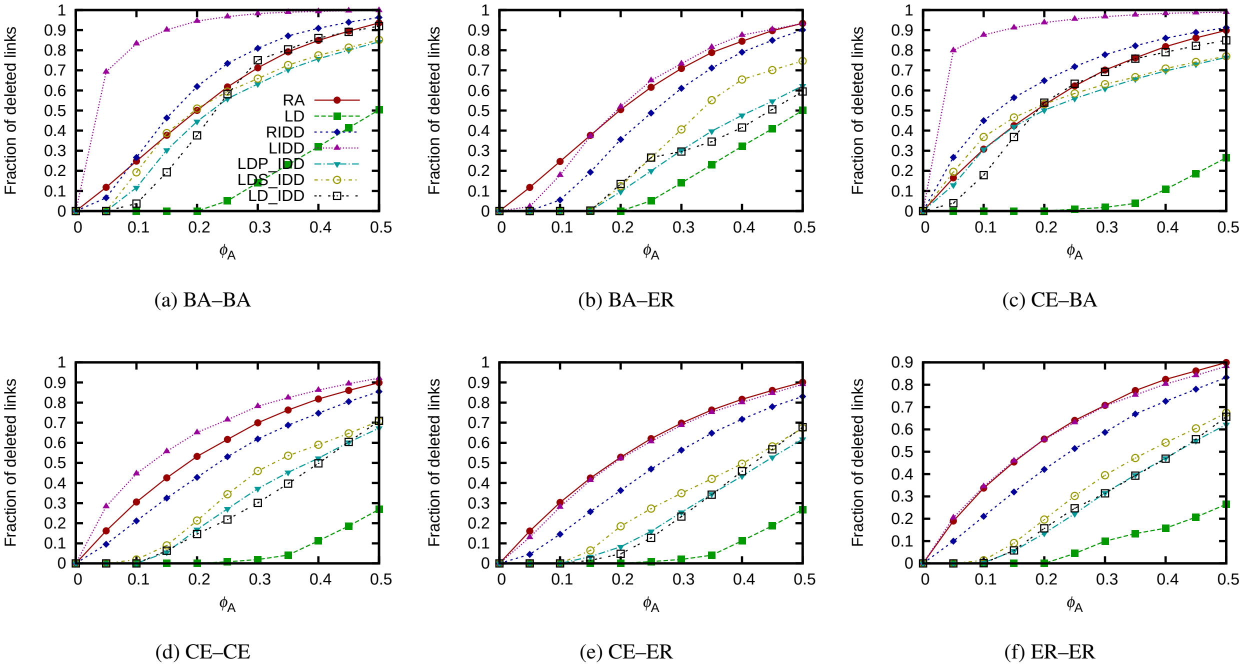
(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 9: Fraction of added links that are subsequently deleted by a degree-based attack versus fraction of nodes removed from G_A (multiplex network, fa = 0.10, ϕ_B = 0.40, N = 1,000).



(a) BA–BA

(b) BA–ER

(c) CE–BA

(d) CE–CE

(e) CE–ER

(f) ER–ER

Figure 10: Fraction of added links that are subsequently deleted by a degree-based attack versus fraction of nodes removed from G_A (multiplex network, fa = 0.20, ϕ_B = 0.40, N = 1,000).

[36] M. A. Di Muro, C. E. La Rocca, H. Stanley, S. Havlin, L. A. Braunstein, Recovery of interdependent networks, Scientific Reports 6 (2016) 22834.

[37] A. Majdandzic, B. Podobnik, S. V. Buldyrev, D. Y. Kenett, S. Havlin, H. E. Stanley, Spontaneous recovery in dynamical networks, Nature Physics 10 (1) (2014) 34–38.