Enhancing Robustness and Resilience of Multiplex Networks against Node-community Cascading Failures

Lijia Ma, Xiao Zhang, Jianqiang Li, *Member, IEEE,* Qiuzhen Lin, *Member, IEEE,* Maoguo Gong, *Senior Member, IEEE,* Carlos A. Coello Coello, *Fellow, IEEE,* and Asoke K. Nandi, *Fellow, IEEE*

***Abstract*—Many real systems are represented in form of multiplex networks composed of a set of nodes, multiple layers of links and coupling node relationships across all layers. These systems are very vulnerable to damages during both attacks and recoveries due to potential node cascading failures (NCFs). Although some progress has recently been made in studying network robustness and resilience, the comprehensive impacts of coupling node relationships and community structures on NCFs remain unclear. Accordingly, in this paper, we study the robustness and resilience of multiplex networks in the presence of NCFs caused by coupling node relationships and community structures. We first model the failure processes of multiplex networks during both attacks and recoveries as node-community cascading failures (called NCCFs), and then theoretically demonstrate the fragility of multiplex networks to random node damages under NCCFs. Subsequently, to improve network robustness and resilience, we adopt a node protection strategy and propose a cost-aware constrained optimization problem. Finally, we devise a degree-based simulated annealing algorithm for solving this optimization problem. Extensive experiments on both simulated and real multiplex networks show that NCCFs make networks more vulnerable to unpredictable damage than classical NCFs. The results also show the superiority of the proposed algorithm over the state-of-the-art algorithms in improving network robustness and resilience.**

***Index Terms*—Multiplex networks, robustness and resilience, cascading failures, community structures, simulated annealing.**

I. Introduction

With the rapid development of information technology, many real systems have become more complex due to the existence of multiple types (or layers) of communications between entities [1]–[5]. These systems can be well represented by multiplex networks with multiple layers, where the nodes and links of each layer represent the entities and communications of a particular system platform, respectively [6], [7]. For example, the air transportation system in Europe can be modeled by a multiplex network with thirty-seven layers, where the nodes and links of each layer represent the airports and flights respectively of a particular commercial airline in the system.

Recent studies have demonstrated that multiplex networks are very vulnerable to node damages during both attacks and recoveries [8]–[11]. This is because damage to a node may induce node cascading failures (NCFs) caused by node coupling relationships [12]. More specifically, a node damage in a layer may first cause intra-layer node failures (i.e., failures of nodes in the same layer), and then the failed nodes further trigger inter-layer node failures (i.e., failures of nodes in the other layers). These failures occur recursively until there are no further node failures [8]–[10]. For example, in transportation systems, damage to ground traffic first leads to severe road congestion, and then triggers underground traffic failures due to increased passenger flows. These failures may lead to severe congestion in both ground and underground traffic. Such cascading failures are ubiquitous in real systems and cause destructive damage to our daily life. Examples include power system blackouts in Italy [13], [14], virus outbreak in spreading systems [15], traffic congestion in transportation systems [16], mission failures in multi-fleet systems performing tasks on the sea [17], synchronization perturbance in nonlinear systems [18]–[20], etc.

Network robustness evaluates the ability of a system to withstand node damages during attacks, while network resilience measures the ability of a system to repair its functionality during recoveries when failures. The robustness and resilience improvement have been attracting much attention due to their applicability in mitigating system failures and resisting targeted attacks [8], [13], [21]–[24]. In recent years, many effective methods have been proposed for improving network robustness and resilience by decreasing NCFs, including link exchange [13], [25]–[27], coupling reduction, [28] and entity protection [11], [29] of influential nodes. Although the influential nodes of complex networks are generally unknown *a priori*, they can be approximately detected using certain classical heuristic algorithms, such as the greedy-based Betweenness [30], Degree [30], PageRank [31], [32] and Collective Influence (CI) [33]. However, these greedy algorithms are easy to get trapped into local optima. These aforementioned methods are

This work was supported by the National Natural Science Foundation of China under Grants 61803269, U1713212, 61672358, 61572330, 61772393 and 61836005. The work of C. A. Coello Coello was supported in part by CONACyT under Project 1920 (Fronteras de la Ciencia) and in part by SEP-Cinvestav 2018 Project (application no. 4).

L. Ma, X. Zhang, J. Li, and Q. Lin are with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China.

M. Gong is with the School of Electronic Engineering, the Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, Xidian University, No. 2 South TaiBai Road, Xi'an 710071, China.

C. A. Coello Coello is with the Department of Computer Science, CINVESTAV-IPN, México, D.F., 07360, México.

A. K. Nandi is with the Department of Electronic and Electrical Engineering, Brunel University London, Uxbridge, UB8 3PH, United Kingdom and also a Distinguished Visiting Professor at Shenzhen University, China.

*Corresponding author: J. Li (e-mail: lijq@szu.edu.cn).

further generalized through the use of various strategies, such as the selective removal of nodes [29], defensive islanding [34], spontaneous and optimal recovery [35], [36], self-healing [37], preferential and optimal repairing [38], system parameter monitoring [39], etc.

Although some progress has recently been made in studying network robustness and resilience, the impacts of coupling node relationships and community structures on the robustness and resilience of multiplex networks remain to be analyzed. Community structures, which are ubiquitous in real systems [40], [41], consist of a set of nodes with similar functionality. Studies on communities are important for analyzing the robustness and resilience of networks, as these community structures may affect NCFs [25], [38], [42]–[44]. Recent studies [25], [38], [42]–[44] have shown that network robustness and resilience can be significantly improved by increasing links across different communities. However, these approaches neglect some potential community failures. In many real-world applications, the functionality of a system is distributed over communities, and each of which will lose its functionality if the number of failed nodes in the community exceeds a certain threshold. For example, transportation in a city will be destroyed by the failure of certain public traffic systems, while the website system in a university will be paralyzed if parts of its websites are subjected to access attacks. A representative contemporary example is the closing of some social community systems (like schools and factories) due to individuals being infected by novel coronavirus (COVID-19). These community failures may subsequently give rise to a new iteration of cascading failures on nodes and communities, which will further destroy the functionality of systems.

In this paper, we study the robustness and resilience of multiplex networks in the presence of cascading failures caused by coupling node relationships and community structures. More specifically, when a multiplex network suffers from node damage, the coupling node relationships can trigger NCFs, while the node failures in community structures can further cause community failures. The cascading of NCFs and community failures makes the network more vulnerable to unpredictable damage. To understand the ability of a multiplex network to resist damage, we evaluate its robustness and resilience during attacks and recoveries, respectively, and further provide some theoretical analyses of the fragility of multiplex networks. Moreover, to improve network robustness and resilience, we first model the situation as a cost-aware robustness (or resilience) optimization problem, and then adopt a node protection strategy to protect a set of influential nodes from damages and failures. However, identifying influential nodes in this context is a challenging task as the number of possible solutions increases exponentially with the node and layer sizes of networks. Simulated annealing algorithm (SA) is an adaptation of the Metropolis-Hastings Monte Carlo algorithm, and it has been widely utilized to solve combinational optimization problems [45] (like node robustness optimization [25], network alignment [46] and 3D structural transition [47]) in complex networks. Hence, we devise a degree-based SA in order to find an optimal set of influential nodes. The main contributions of this paper are as follows:

1) We propose the concept of novel node-community cascading failures (NCCFs) in multiplex networks, which consists of the NCFs and community failures caused by both coupling node relationships and community structures. Compared with classical NCFs [8], NCCFs make a multiplex network more vulnerable to unpredictable node damage.
2) We further propose a system model for evaluating the robustness and resilience of multiplex networks, and theoretically analyze the fragility of multiplex networks to NCCFs.
3) We model the improvement of network robustness and resilience using a node protection strategy as a cost-aware combinational optimization problem, and then devise a degree-based SA algorithm for solving this problem.
4) Extensive experiments on simulated and real multiplex networks validate that NCCFs outperform classical NCFs in triggering node failures. The results also show the superiority of the proposed SA algorithm over the state-of-the-art algorithms in improving network robustness and resilience.

The remainder of this paper is organized as follows. Section II presents the system model for evaluating the robustness and resilience of multiplex networks. Section III introduces the problem formulation and the proposed SA algorithm for improving the robustness of multiplex networks. The experimental results are analyzed in Section IV, and the concluding remarks and some future work are given in Section V.

II. System model

We consider the functional robustness and resilience of a complex system with n entities and q types of communications against cascading failures under all possible entity attacks (or recoveries). There are at most n attacks (or recoveries), and each attack (or recovery) will directly cause the functional damage (or recovery) of an entity. After all attacks (or recoveries) are occurred, the system's functionality will be completely destroyed (or recovered).

This system can be modeled as a multiplex network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}^{[1]}, \mathcal{E}^{[2]}, \ldots, \mathcal{E}^{[q]}, \mathcal{D}\}$ with $|\mathcal{V}| = n$ nodes, q layers of edges and interdependency relationships $\mathcal{D}$, in which every layer $\alpha \in \{1, 2, ..., q\}$ represents a simple network $\mathcal{G}^{[\alpha]} = \{\mathcal{V}, \mathcal{E}^{[\alpha]}\}$ with $|\mathcal{E}^{[\alpha]}| = m^{[\alpha]}$ edges. In the multiplex network, every layer contains all n nodes in $\mathcal{V}$, and every node with the same label appears in every layer (see Fig. 1). Moreover, the nodes in various layers that have the same label are actually the same one (i.e., these nodes are the replicas of an entity across q layers, and they are used to represent the relationships with other entities in various layers), and they are considered to be interdependent on each other.

The edges $\mathcal{E}^{[\alpha]}$ of each layer $\alpha \in \{1, 2, \ldots, q\}$ of $\mathcal{G}$ can be expressed as an adjacent matrix $\mathrm{A}^{[\alpha]}$, in which each element $\mathrm{A}_{ij}^{[\alpha]} \in \{0, 1\}$ represents the link state between the nodes i and j in layer α. More specifically, $\mathrm{A}_{ij}^{[\alpha]}$ is represented as follows:

$$\mathrm{A}_{ij}^{[\alpha]} = \begin{cases} 1 & \text{if nodes } i \text{ and } j \text{ are linked in the layer } \alpha \\ 0 & \text{otherwise.} \end{cases}$$

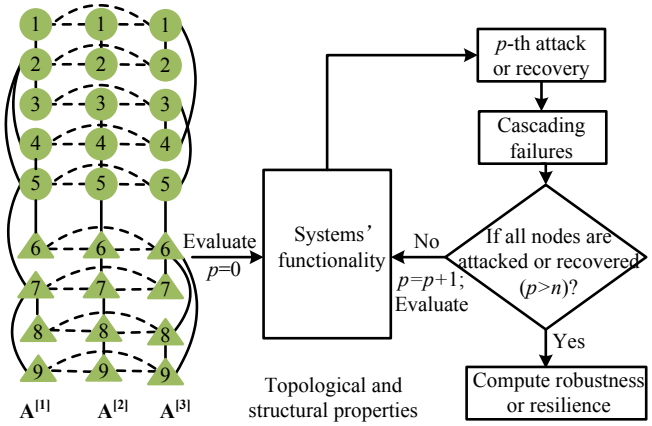


Fig. 1. Framework of the system model for evaluating the robustness and resilience of a multiplex network with $n = 9$ nodes and $q = 3$ layers of links. Full lines represent edges while dotted lines denote interdependency relationships. Nodes in various layers that have the same label denote the same entity.

We use $\mathrm{A} = [\mathrm{A}_{ij}^{[\alpha]}]_{n\cdot n\cdot q}$ to represent the edges $\{\mathcal{E}^{[1]}, \mathcal{E}^{[2]}, \ldots, \mathcal{E}^{[q]}\}$ of $\mathcal{G}$ in all layers. The interdependency relationships $\mathcal{D}$ between replica nodes can also be expressed as an adjacent matrix D, in which each element $\mathrm{D}_{ij}^{[d\alpha]} \in \{0, 1\}$ represents the interdependency relationship of nodes i and j in different layers d and α. More specifically, $\mathrm{D}_{ij}^{[d\alpha]}$ is represented as follows:

$$\mathrm{D}_{ij}^{[d\alpha]} = \begin{cases} 1 & \text{if } i = j \text{ and } d \neq \alpha \\ 0 & \text{otherwise.} \end{cases}$$

We use $\mathrm{D} = [\mathrm{D}_{ij}^{[d\alpha]}]_{n\cdot n\cdot q\cdot q}$ to represent the interdependency relationships $\mathcal{D}$ of $\mathcal{G}$.

Fig. 1 illustrates the framework of the system model used to evaluate the robustness and resilience of a toy multiplex network with 9 nodes and 3 layers of links. The key aspects of this system model, such as the functionality, attack and recovery models, cascading failures, and robustness (or resilience), are given next.

A. Functionality of multiplex networks

When a system suffers from unpredictable attacks, its functionality may fail or may even be damaged. The damage (or failure) of a system means that all entities (or a part of entities) lose their functionality. The functionality of a network is usually reflected by its largest connected component (LCC) [13], namely the maximum set of nodes that have at least one link path among these nodes. Nodes of a network are functional if and only if they are contained in the LCC [13].

Note that, the functionality of many systems is determined not only by the LCC, but also by structural properties such as community structures [38]. A community in a network is composed of a group of nodes that are connected densely with each other, but sparsely linked with the others [40], [48] (see Fig. 1 for an illustration). Moreover, nodes within the same community generally have similar functionality [40], [41]. Accordingly, when a community loses its functionality due to an attack, the nodes in this community will become non-functional. For example, in transportation systems, traffic congestion on the roads of a specific area will cause the congestion of nearby roads in this area.

To comprehensively represent the functionality of multiplex networks, we introduce a community-aware LCC. Here, nodes and links are normally functional for the systems if and only if they are in the LCC and their community is functional. In addition to functional nodes, a failed multiplex network also contains two other types of nodes, namely damaged nodes and failed nodes. Damaged nodes are attacked ones that have lost their functionality. Moreover, failed nodes are unattacked ones that are not in the community-aware LCC. They will also lose their functionality. Unlike the damaged nodes, the failed nodes will automatically become functional after they are put into the recovered community-aware LCC during the recovery process.

To simplify notation, we use parameters with a superscript a and r to denote the variables in attacks and recoveries, respectively. For each node i, $b \in \{a, r\}$, we let $z_{ip}^{b} \in \{0, 1\}$ denote the functional state of node i in our system model after the p-th attack ($b = a$) or recovery ($b = r$). More specifically, z_{ip}^{b} is represented as follows:

$$z_{ip}^{b} = \begin{cases} 1 & \text{if } i \text{ is functional} \\ 0 & \text{if } i \text{ is failed or damaged.} \end{cases} \quad (1)$$

Moreover, we let $\mathcal{V}_p^b = \{i \in \mathcal{V} : z_{ip}^{b} = 1\}$ be the set of functional nodes after the p-th operation.

B. Attacks and recoveries in multiplex networks

1) Attacks: In real-world applications, entities of a system will fail when they are subjected to attacks such as functional decline, volcanic eruptions, hurricanes, earthquakes and tsunamis. Most of these attacks are unpredictable *a priori*. In order to model these attacks, we adopt a random node attack model [8], [11], [13].

The random node attack model executes a set of attacks $\{\mathbf{T}^a(\mathcal{V}_{p-1}^a, p)\}_n$ in order, and each of those attacks $\mathbf{T}^a(\mathcal{V}_{p-1}^a, p)$ will directly damage one node, which is randomly chosen from the set of functional nodes $\mathcal{V}_{p-1}^a$. Recall that n is the number of nodes, while $\mathcal{V}_{p-1}^a$ denotes the set of functional nodes of the test network after the $(p-1)$-th attack. This attack model is described in more detail below.

Initialization: Set $p = 1$ and $\mathcal{V}_0^a = \mathcal{V}$;
Step 1): Find the functional nodes $\mathcal{V}_{p-1}^a$ of the network $\mathcal{G}$;
Step 2): If the set $\mathcal{V}_{p-1}^a$ is not empty, execute $\mathbf{T}^a(\mathcal{V}_{p-1}^a, p)$, $p = p + 1$, and go to **Step 1**). Otherwise, the attack is terminated.

2) Recoveries: In real-world applications, many systems such as transportation and power systems need to be recovered after catastrophic damage. Thus, similar to the attack model, a random recovery strategy [11], [35] is adopted to model the recovery of a damaged real-world system.

The random node recovery model executes a set of recoveries $\{\mathbf{T}^r(\mathcal{V}_{p-1}^d, p)\}_n$ in order, in which each recovery $\mathbf{T}^r(\mathcal{V}_{p-1}^d, p)$ will recover one damaged node, randomly chosen from the set of damaged nodes $\mathcal{V}_{p-1}^d$ remaining after the previous $(p-1)$ recoveries. This recovery model is described

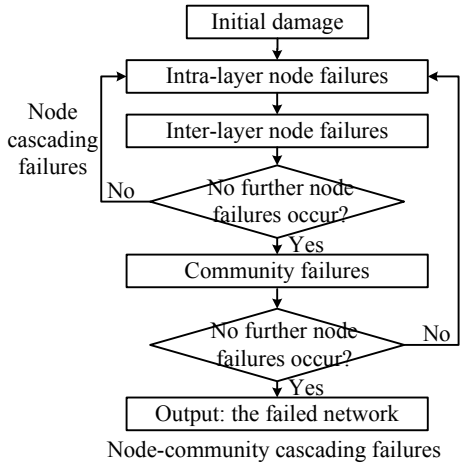


Fig. 2. Flowchart of NCCFs in multiplex networks.

in more detail below.

Initialization: Set $p = 1$ and $\mathcal{V}_0^d = \mathcal{V}$;

Step 1): Find the set of damaged nodes $\mathcal{V}_{p-1}^d$ of the network $\mathcal{G}$ before the p-th recovery;

Step 2): If the set $\mathcal{V}_{p-1}^d$ is not empty, execute $\mathbf{T}^r(\mathcal{V}_{p-1}^d, p)$, $p = p+1$, and go to **Step 1**). Otherwise, the recovery process is terminated.

Note that, in this recovery model, the recovered nodes will become failed nodes when they are not contained within the community-aware LCC. Moreover, failed nodes will automatically become functional when they are located in the community-aware LCC of the recovered network during the recovery processes.

C. Cascading failures of multiplex networks during both attacks and recoveries

Compared with a single-layered network, a multiplex network is more vulnerable to node damage as the failures in its topological and coupling structures will cause both intra-layer and inter-layer node failures. Moreover, these failures in turn affect each other, causing a cascade of node failures. These types of cascading failures have been widely verified in a number of real systems, e.g., the cascading failures between a power system and its centralized control system in Italy that resulted in the catastrophic blackout on 28/9/2003.

Classical models [8]–[11], [29], [34], [35], [49] focus primarily on NCFs in multiplex networks. Under these circumstances, some node damages first cause intra-layer node failures in the same layers, and then trigger inter-layer node failures in the other layers. Next, these failures further trigger a new iteration of intra-layer and inter-layer node failures. The above-mentioned failures occur recursively until the network falls into a stable state (i.e., there are no further node failures). Note that, in reality, an attack can begin from a different layer while the final state of a multiplex network under an attack is irrelevant to the order in which intra-layer and inter-layer node failures occur. For better presentation, we try to illustrate the cascading failures caused by the damage to nodes at the first layer.

Unlike the classical models [8]–[11], [29], [34], [35], [49], our system model considers NCFs together with community failures. The community structure is ubiquitous in networks, and nodes within the same community usually have similar functionality. In many real-world applications, the functionality of a system is distributed throughout its communities, and each community has a minimum threshold λ below which node failures within the community can be tolerated. More specifically, when the proportion of failed nodes and damaged nodes in a community after attacks (recoveries) exceeds the minimum threshold λ, the community's functionality will fail, resulting in the failure of all nodes in the community. The community failure will break the original stable state and trigger a new iteration of node cascading failures. We refer to the cascade of node and community failures as NCCFs.

A flowchart of NCCFs is presented in Fig. 2, which consists of the following steps:

Step 1) Cascading failures of nodes. The failures of nodes trigger a cascade of node failures (intra-layer and inter-layer node failures).

Step 2) Failures of communities. The failures of nodes cause the failures of communities, which results in further failures of the communities' nodes.

Step 3) Cascading failures of nodes and communities. The steps above occur recursively until there are no further node failures and community failures.

Fig. 3 presents schematic illustrations of NCFs (see Figs. 3(a)-3(d)) and NCCFs (see Figs. 3(a)-3(f)) on a toy multiplex network under an attack. For the NCFs, the initial node attack (see Fig. 3(a)) first causes intra-layer node failures (see Fig. 3(b)), and then triggers inter-layer node failures (see Fig. 3(c)). Next, the node failures cause a further cascade of intra-layer and inter-layer node failures until there are no further node failures (see Fig. 3(d)). In this case, the toy multiplex network under the NCFs has five functional nodes after the initial attack. For the NCCFs, the initial node attack (see Fig. 3(a)) first causes the node cascading failures (see Figs. 3(b-d)), and then triggers the failure of the community as indicated by the circles (see Fig. 3(e)). Next, the community failure causes new iterations of node-community cascading failures until there are no further node failures (see Fig. 3(f)). In this case, all nodes of the toy multiplex network are failed after the initial attack. Therefore, compared with NCFs, NCCFs make the toy multiplex network more vulnerable to initial node damage.

Fig. 4 presents schematic illustrations of NCFs (see Figs. 4(a)-4(d)) and NCCFs (see Figs. 4(a)-4(f)) on a toy multiplex network under a recovery state with five recovered nodes. We can make similar observations regarding cascading failures between the recovery of Fig. 4 and the attack of Fig. 3. Moreover, compared with NCFs, NCCFs make it more difficult for the toy multiplex network to recover its functionality. In particular, in this recovery state, the toy multiplex network recovers the functionality of three and zero nodes under NCFs and NCCFs, respectively.

When a fraction p/n of nodes are attacked (or recovered), for $b \in \{a, r\}$, the mathematical expression of NCCFs in a multiplex network is as follows:

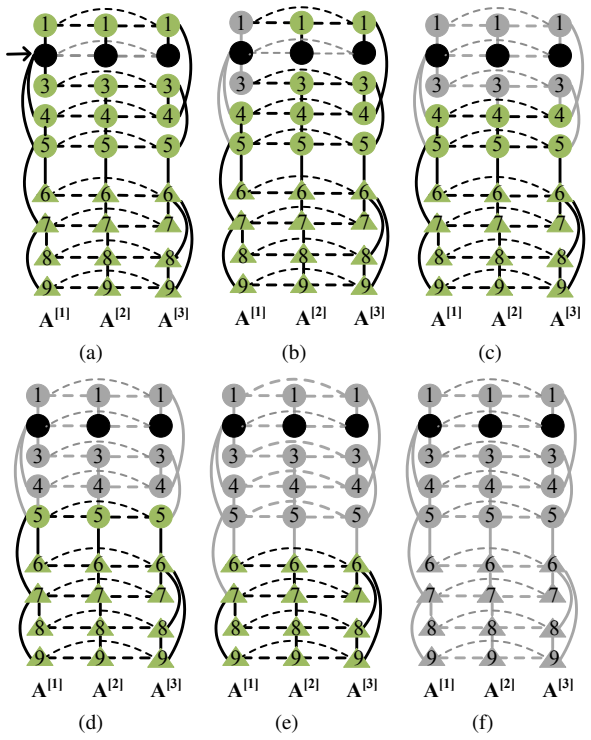


Fig. 3. Schematic illustrations of NCFs ((a)-(d)) and NCCFs ((a)-(f)) on a toy three-layered multiplex network under attacks with community failure threshold $\lambda = 0.7$. (a) an initial attack that directly causes the failures of the replica nodes of attacked entities at all layers, (b) intra-layer node failures, (c) inter-layer node failures, (d) cascading node failures, (e) community failures, and (f) new iterations of node-community cascading failures until there are no further node failures. The functional, damaged and failed nodes are marked in green, black and gray, respectively, while an arrow indicates a node under attack. Nodes with different shapes belong to different communities. There are five and zero functional nodes after NCFs and NCCFs occur, respectively.

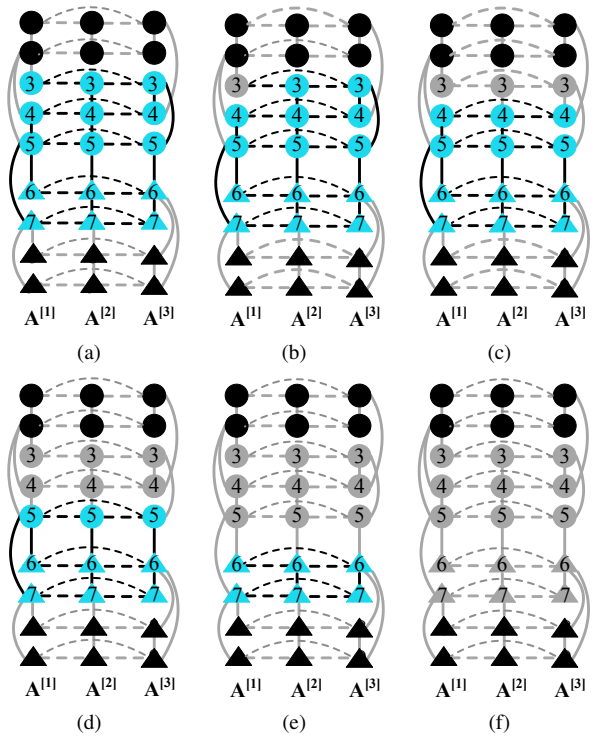


Fig. 4. Schematic illustrations of NCFs ((a)-(d)) and NCCFs ((a)-(f)) on a toy three-layered multiplex network under recoveries with community failure threshold $\lambda = 0.7$. (a) an initial recovery that directly causes the recovery of the replica nodes of recovered entities at all layers, (b) intra-layer node failures, (c) inter-layer node failures, (d) node cascading failures, (e) community failures, and (f) new iterations of node-community cascading failures until there are no further node failures. The recovered, damaged and failed nodes are marked in cyan, black and gray, respectively. Nodes with different shapes belong to different communities. There are three and zero functional nodes after NCFs and NCCFs occur, respectively.

$$\begin{cases} \phi_{\alpha}^{b,l+1}(p) = \mathbf{F}_{n}^{b}(\phi_{\alpha}^{b,l}(p)) \\ \phi_{\alpha}^{b,l+1}(p) = \mathbf{F}_{c}^{b}(\phi_{\alpha}^{b,l+1}(p)), \end{cases} \tag{2}$$

where $\mathbf{F}_{n}^{b}(.)$ and $\mathbf{F}_{c}^{b}(.)$ are functions that describe the processes of the node cascading failures and community failures, respectively. Moreover, $\phi_{\alpha}^{b,l+1}(p)$ denotes the fraction of functional nodes of the multiplex network at the α-th layer after the l-th iteration of node and community cascading failures caused by the p-th attack $(b = a)$ or recovery $(b = r)$. The cascading failures in (2) are iterated until there are no further node failures.

Here, $\mathbf{F}_{n}^{b}(\phi_{\alpha}^{b,l}(p))$ can be calcluated as follows:

$$\begin{cases} \phi_{q}^{b,l,0}(p) = \phi_{\alpha}^{b,l}(p) \\ \phi_{1}^{b,l,t+1}(p) = S_{q}^{b,l,t}(\phi_{q}^{b,l,t}(p)) \cdot \phi_{q}^{b,l,t}(p) \\ \phi_{\alpha}^{b,l,t+1}(p) = S_{\alpha-1}^{b,l,t+1}(\phi_{\alpha-1}^{b,l,t+1}(p)) \cdot \phi_{\alpha-1}^{b,l,t+1}(p), \ \alpha = 2, ..., q \end{cases} \tag{3}$$

where $\phi_{\alpha}^{b,l,t}(p)$ represents the fraction of functional nodes in the multiplex network at the α-th layer following the t-th iteration of node cascading failures at the l-th iteration of node-community cascading failures caused by the p-th attack or recovery. $S_{\alpha}^{b,l,t}(\phi_{\alpha}^{b,l,t}(p))$ is the fraction of the functional nodes in the remaining $\phi_{\alpha}^{b,l,t}(p)$ parts of the network that are in the LCC. When $t = 0$ and $l = 1$, $\phi_{1}^{a,l,t}(p) = 1 - p/n$ and $\phi_{1}^{r,l,t}(p) = p/n$. The cascading failures in (3) are iterated until there are no further node failures caused by the node cascading failures. In this case, we obtain $\phi_{\alpha}^{b,l+1}(p)$ of the network after l-th node cascading failures.

Moreover, $\mathbf{F}_{c}^{b}(\phi_{\alpha}^{b,l+1}(p))$ can be mathematically expressed as follows:

$$\phi_{\alpha}^{b,l+1,t+1}(p) = T^{b,l,t+1}(\phi_{\alpha}^{b,l+1,t}(p)) \cdot \phi_{\alpha}^{b,l+1,t}(p), \ \alpha = 1, \ldots, q, \tag{4}$$

where $T^{b,l,t}(\phi_{\alpha}^{b,l+1,t}(p))$ is the fraction of the functional nodes in the remaining $\phi_{\alpha}^{b,l+1,t}(p)$ parts of the network that are in the community-aware LCC following the t-th iteration of l-th community failures. The cascading failures in (4) are iterated until there are no further node failures caused by the community failures. In this case, we get $\phi_{\alpha}^{b,l+1}(p)$ of the network after l-th node and community cascading failures.

The key difference between NCCFs expressed in (2-4) and the standard cascading failure model (NCFs) is as follows: in addition to the node cascading failures in NCFs, NCCFs also consider community failures (see (4)) and a cascade of node and community failures (see (2)).

Under the aforementioned NCCFs, we let $P_{c}^{\infty}(p)$ be the final fraction of the community-aware LCC of $\mathcal{G}$ after p operations (whether attacks or recoveries). The theoretical and experimental analyses of P_{c}^{∞} with a fraction p/n of removed

nodes can be found in the supplementary document. These analyses show that the simulated results can approximate the theoretical results well, and that multiplex networks with higher node degrees are more robust to attacks.

D. Functional robustness and resilience of multiplex networks

Similar to [8], [11], the functional attack robustness (or recovery resilience) of a multiplex network used here evaluates the fraction of functional nodes during all possible attacks (or recoveries). Unlike [8], [11], the functionality of a multiplex network in our robustness (or resilience) measure is reflected by the community-aware LCC model rather than the LCC model. Moreover, our functional attack robustness (or recovery resilience) is evaluated under cascading failures, modeled as NCCFs different from the use of NCFs in [8], [11].

Following the community-aware LCC model, the random attack (or recovery) model and the NCCFs in (2), for each $b \in \{a, r\}$, we evaluate the functional attack ($b = a$) robustness or recovery ($b = r$) resilience $R^b(\mathcal{G}, \mathbf{T}^b)$ of a multiplex network $\mathcal{G}$ as follows:

$$\begin{aligned} R^b(\mathcal{G}, \mathbf{T}^b) &= \frac{1}{n}\sum_{p=1}^{n}\frac{|\mathcal{V}_p^b|}{n} = \frac{1}{n}\sum_{p=1}^{n}P_c^{\infty}(p) \\ &= \frac{1}{n}\sum_{p=1}^{n}\sum_{i=1}^{n}\frac{z_{ip}^b}{n} \end{aligned}, \tag{5}$$

where the operator $|.|$ evaluates the number of elements in the set, while $|\mathcal{V}_p^b|/n$ and $\sum_{i=1}^{n} z_{ip}^b/n$ compute the fraction of functional nodes in $\mathcal{G}$ after p attacks ($b = a$) or recoveries ($b = r$). Moreover, $\sum_{p=1}^{n}(.)$ reflects all possible attacks (or recoveries). Recall that $P_c^{\infty}(p)$ is the final fraction of the community-aware LCC after p operations (whether attacks or recoveries), and $\mathbf{T}^b$ is the attack ($b = a$) or recovery ($b = r$) strategy. In (5), $1/n$ is a normalization factor, which enables fair comparison of the robustness (or resilience) of networks with different scales. Generally, the R^b value is in the range of $[0, 1]$, and networks with a higher R^b are more robust to failures during attacks (or recoveries).

In some real-world cases, a mix of attacks and recoveries may occur simultaneously, and the mixing weight is controlled by a recovery rate. In the supplementary document, we present some theoretical and experimental analyses of the resilience of the ER-ER multiplex networks under different recovery rates. The results demonstrate that the resilience of the ER-ER multiplex increases with the recovery rate. This is to be expected that the number of damaged nodes and intra-layer node failures decrease as an increasing number of damaged nodes recover.

III. Problem formulation and our solution

A. Scope of Problem

The main context of this work is as follows. A complex system acquires a specific configuration (entities, links and layers) following years of development. Nevertheless, small parts of such a configuration could be modified when considering the system's function and the limited cost. While the function of a system under the original layer configuration is very vulnerable to unpredictable damages, its robustness and resilience can be greatly improved by changing small parts of the configuration.

To evaluate system robustness and resilience, we first use a multiplex network with multiple layers to represent this system, and then model the failure prorogations in a real scenario as cascades of node and community failures (NCCFs). Next, we study the robustness and resilience of the modeled multiplex network to damage under NCCFs. A representative example of NCCFs is failures in the functionality of social systems (like schools, factories, etc.) due to COVID-19. An infected person may first infect people within their own system, resulting in a failure of functionality within this specific system. Then, the movement of infected people results in failures of functionality across all social systems. Moreover, when the infected people exceed the tolerance threshold of a social system, the social system will fail or even be closed down. In fact, in the situation unfolding today, some schools or factories are being closed down after a number of students or workers have become infected by the node-community cascading propagation of COVID-19.

The multiplex networks are vulnerable to unpredictable attacks as nodes in different layers work collaboratively to perform their intractable functionality. Many strategies have been proposed for enhancing network robustness and resilience, including exchanging links [13], [25], [26], reducing coupling [28], constructing autonomous nodes [29], self-healing [37], and protecting influential nodes [11]. However, in real-world applications, all strategies have costs in terms of resources (e.g., money, time, bandwidth, place, material, etc.), meaning that the network improvement budget is generally limited. For example, constructing a financial regulatory agency and a backup power station requires time and money to establish trade systems and power systems, respectively, while monitoring virtual machines of cloud networks in data centers requires bandwidth and energy for allocation and consolidation.

In this work, we try to enhance the robustness and resilience of multiplex networks for resisting NCCFs by protecting a small number of influential nodes at a limited cost. In real-world applications, this protection strategy has been widely used to protect systems' function from unpredictable damages. For example, during the COVID-19 outbreak, susceptible people are asked to stay at home, while some cities that typically experience heavy traffic have protected themselves by closing the air, sea and land transportation routes with other cites. In hospitals, there are backup power generations that enable severely ill patients to continue to receive treatment during power cuts. In financial systems, certain security strategies (encryption, blockchain, etc.) are utilized to protect sensitive data from attacks.

B. Problem formulation

Given a multiplex network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}^{[1]}, \mathcal{E}^{[2]}, \ldots, \mathcal{E}^{[q]}\}$, a random attack strategy $\mathbf{T}^a$ (or a random recovery strategy $\mathbf{T}^r$), the cost C of protecting a node, and the limited cost C^*, our problem is to discover a minimum set $\mathcal{S}$ of influential nodes, which will be protected with a maximum cost C^* to resist

NCCFs during attacks (or recoveries), so as to maximize the attack robustness R^a (or the recovery resilience R^r) of the multiplex network. This problem can be formulated as follows:

$$\begin{aligned} \max \quad & R^a(\mathcal{G}, \mathbf{T}^a) \text{ or } R^r(\mathcal{G}, \mathbf{T}^r) \\ \text{s.t.} \quad & C \cdot |\mathcal{S}| \leq C^*, \end{aligned} \tag{6}$$

where $|\mathcal{S}|$ denotes the number of nodes in $\mathcal{S}$. Here, C^* and C determine the number of protected nodes.

C. Our Solution

Many centrality-based greedy algorithms have been proposed to find a minimum set $\mathcal{S}$ of influential nodes, including Degree [30], Betweenness [30], Pagerank [31], [32], Collective Influence [33], H-index [50], etc. They normally begin with an empty set, followed by adding the nodes with a high centrality to the dominant set iteratively. Their performance has been widely verified, especially in terms of convergence and effectiveness. However, it is easy for these algorithms to get trapped in local optima due to their greedy strategies.

Here, we present a degree-based SA algorithm for improving the robustness and resilience of multiplex networks with a cost constraint. The SA algorithm first chooses a minimum number n_β of nodes with high degrees as the initial influential nodes $\mathcal{S}$, and then iteratively replaces a node $i \in \mathcal{S}$ with another node $j \in \mathcal{V} - \mathcal{S}$ at a probability $p^t(i,j)$, where t denotes the current index of iterations. This probability $p^t(i,j)$ allows the algorithm to accept a worse solution, which can effectively avoid getting trapped into local optima. The swapping step is executed until the current iteration reaches a predefined maximum number t_m (e.g., here, we set it to 10^3).

For each $b \in \{a, r\}$, let ΔR^b denote the difference of R^b between the current solution and the refined solution. The probability $p^t(i,j)$ is generally computed as follows:

$$p^t(i,j) = \exp^{\Delta R^b / T}, \tag{7}$$

where T is a control parameter used to determine the decline probability of accepting a worse solution and the convergence rate of the SA algorithm to an optimal solution. Generally, an SA algorithm with a smaller T value can more easily converge to a good solution (here, we set it to 10^{-4}). As known from (7), $p^t(i,j)$ is larger than 1 when the refined solution has a larger objective value than the current solution. In this case, the refined solution will replace the current solution. Moreover, $p^t(i,j)$ is smaller than 1 when the refined solution has a smaller objective value than the current solution. In this case, the refined solution will replace the current solution with a probability $p^t(i,j) \leq 1$.

As known from the model of NCCFs in Section II-C, the computation of the objective R^b needs to have some *a priori* knowledge of the communities of multiplex networks. However, in reality, the community structures of most multiplex networks are unknown *a priori*, but they can be well reflected by the networks' link structures [40].

Many clustering algorithms can be used for community detection in single-layered networks. Most of them can be found in the toolbox "Matlab Tools for Network Analysis" constructed by the MIT Strategic Engineering Research Group (SERG, http://strategic.mit.edu/downloads.php?page=matlab_networks). However, the heterogenous link structures of multiplex networks make it difficult to detect their community structures. In recent years, many community detection algorithms for multiplex networks have been proposed, and their performance has been verified, especially regarding Genlouvin [40]. The Genlouvin algorithm first models the community detection in multiplex networks as the optimization of multiplex modularity Q, and then uses a multilevel community grouping technique together with a community division technique to solve this optimization problem.

Genlouvin is selected for community detection in multiplex networks for the following reasons. Firstly, Genlouvin is effective at uncovering the community structures of multiplex networks. Moreover, it can automatically detect the number of communities without knowing the real number of communities *a priori*. In addition, it has low computational complexity, and it is also able to tackle multiplex networks with hundreds of nodes and dozens of layers. Finally, extensive experiments in [40] have demonstrated the effectiveness of Genlouvin on community detection in multiplex networks.

Algorithm 1 Framework of the SA algorithm for improving attack robustness (or recovery resilience)

1: **Input**: multiplex network: $\mathcal{G}$, minimum cost: C^*, and maximum number of generations: t_m.
2: $\mathcal{S} \leftarrow$ Select a minimum number n_β of nodes with high degrees under the cost constraint C^*.
3: Detect communities of $\mathcal{G}$ using Genlouvin [40], and compute R^a (or R^r) based on (5).
4: **for** ($t = 1$ to t_m) **do**
5: Select a node i from $\mathcal{S}$ randomly, and choose a node j from $\mathcal{V} - \mathcal{S}$ randomly.
6: Replace $i \in \mathcal{S}$ by j, thus generating a refined set $\mathcal{S}'$. Then, compute $(R^a)'$ (or $(R^r)'$) based on (5).
7: Compute $p^t(i,j)$ based on (7), and generate a random value μ in $[0,\ 1]$.
8: **if** $\mu \leq p^t(i,j)$ **then**
9: $\mathcal{S} \leftarrow \mathcal{S}'$ and $R^a \leftarrow (R^a)'$ (or $R^r \leftarrow (R^r)'$).
10: **end if**
11: **end for**

The framework of the SA algorithm for improving the robustness and resilience of multiplex networks is shown in **Algorithm 1**. In line 2 of **Algorithm 1**, the nodes are sorted based on their degrees, which has a computational complexity $O(n \cdot \log n)$. Moreover, in line 3, the Genlouvin algorithm has a computational complexity $O(n \cdot \log^2 n)$ (shown in [40]) for community detection. Finally, the loop in lines 4-11 is executed t_m times at most. In this loop, the objective computation in (5) is the most time-consuming part, with a computational complexity $O(q \cdot n^2 \cdot \log n)$. Therefore, the SA algorithm has a total computational complexity of $O(t_m \cdot n^2 \cdot \log n)$.

IV. Experimental Results

In this section, we evaluate the robustness and resilience of synthetic scale-free multiplex networks and three real multiplex networks during both attacks and recoveries under

NCCFs, aiming to demonstrate that NCCFs make networks more vulnerable to unpredictable damage than classical NCFs. Moreover, we test the proposed SA algorithm on the tested networks, and further compare it with six classical algorithms to demonstrate the superiority of the proposed SA algorithm in enhancing the functional robustness and resilience of networks. The experimental settings are first provided, after which the comparison results are analyzed. Finally, the effects of some parameters on the performance of the SA algorithm are discussed.

A. Experimental Settings

1) Experimental networks: **Synthetic multiplex networks**: Many traditional systems are modeled as Erdős-Rényi (ER) networks [51], in which two entities are connected with a probability p^r and the average degree of the systems is $p^r \cdot n$, where n is the number of entities. Moreover, many real systems (such as wireless sensor networks, power grid systems, economic systems, etc. [39], [47]) show a scale-free property, i.e., the distribution $P(k) = k^{-\gamma}$ of the nodes' degree k follows a power law $k^{-\gamma}$, where γ is the exponent of the power law distribution within the range $[2,\ 2.6]$ generally. In these systems, their functionality is often controlled by a few nodes with a high degree. These systems can be well modeled using scale-free (SF) networks [52]. In addition, some modern systems (like the World Wide Web and the metabolic networks of cells) exhibit a small-world property, in which two arbitrary entities are linked by only six degrees of separation. These systems are represented by the small-world (SW) networks [53].

To achieve more reliable statistical results, we test our method on four types of multiplex networks (ER-SF, SW-SF, SF-SF, ER-SW-SF). Moreover, we test all algorithms on the modeled networks using various settings. More specifically, we take the numbers of nodes as $n = 200$ and $n = 500$, the numbers of layers as ranging from 1 to 10 with an interval of 1, the average degree $p^r \cdot n$ as 4 for ER networks, and the exponent γ as 2.2 for SF networks. In addition, for each network type, we independently generate 100 networks and achieve statistical results over them.

All synthetic and real networks have no prior knowledge about the real community structures. In this case, the Genlouvin algorithm is used for detecting communities of all these networks, and it will return a non-overlapping community division. More specifically, every node in a multiplex network is divided into a set (or) cluster, and the nodes in the same set (or cluster) are divided into the same community. The statistics of communities for these synthetic networks such as average modularity and average number of communities can be found in the supplementary document.

Real multiplex networks: The real CKM physicians innovation (CKM) [54], Celegans (Celegans) [55] and Food and Agriculture Organization (FAO) [56] multiplex networks are selected as the test networks. These networks are derived from various complex systems (e.g., social, genetic and economic systems). Some basic structural information regarding these networks is provided in Table I, while more detailed descriptions are provided below.

TABLE I
BASIC INFORMATION OF THREE REAL-WORLD MULTIPLEX NETWORKS. Q IS THE MULTIPLEX MODULARITY, AND n_c IS THE NUMBER OF COMMUNITIES DETECTED BY GENLOUVIN [40].

Networks	n	q	m	Q	n_c
CKM	246	2	921	0.7549	12
Celegans	279	3	3105	0.4864	5
FAO	183	4	706	0.5414	54

TABLE II
PARAMETER SETTINGS OF ALL TEST ALGORITHMS.

Algorithm	Parameter	Meaning	Setting
SA	T	Control parameter	10^{-4}
	t_m	Maximum number of iterations	10^3
PA	r_a	Fraction of autonomous nodes	0.10
PageRank	$1-\xi$	Transition probability	0.15
CI	ς	Radius	1
GA	n_p	Population size	50
	n_m	Size of mating pool	20
	p_c	Crossover probability	0.9
	p_m	Mutation probability	0.15
	t_m	Maximum number of iterations	50
Betweenness		No parameter	
Degree		No parameter	

CKM: This network was constructed by Coleman et al. [54] as a medical innovation to analyze the effect of network links on the adoption of a new drug (tetracycline) by physicians. In CKM, nodes denote physicians in five towns (i.e., Illinois, Peoria, Bloomington, Quincy and Galesburg), while edges at different layers are constructed based on certain common questions (e.g., what advice you would give about the therapy, who do you usually have discussions with among the three or four physicians, etc.) [54]. Here, two layers of the CKM network are generated, containing 246 nodes and 921 edges.

Celegans: This network was generalized from the genetic interactions of certain organisms (Caenorhabditis Elegans [55]) collected from a famous and public database (BioGRID 3.2.108). This network consists of 279 nodes and 8,181 edges with 6 layers, and the network at each layer represents a certain association. Here, the test Celegans network consists of 279 organisms and 3,105 links on three layers (i.e., the layers of direct interaction, physical association, and additive genetic interaction defined by inequality).

FAO: This network was collected from the FAO (Food and Agriculture Organization) in 2010 [56]. The FAO network depicts various trade relationships among multiple countries on the conducts of the United Nations. In this network, nodes represent the countries, while edges in different layers represent the trade relationships among countries on different conducts. The test FAO multiplex network contains 706 trade relationships of 183 countries on the 4 conducts with the maximum trade.

The functional robustness and resilience of these systems can be improved by using certain protection strategies. Generally speaking, for the CKM network, physicians with many common questions are protected from false information about tetracycline by their professional knowledge. For the Celegans network, organisms with many genetic interactions are protected from virus by some drugs. For the FAO network,

TABLE III
COMPARISONS OF ALL ALGORITHMS IN IMPROVING THE ATTACK ROBUSTNESS AND RECOVERY RESILIENCE OF SYNTHETIC MULTIPLEX NETWORKS UNDER $\lambda = 0.3$. THE BEST RESULT IS MARKED IN BOLDFACE FOR EACH NETWORK. ALL RESULTS ARE AVERAGED OVER 100 TRIALS.

Indexes	Networks	n	q	WC	Origin	Betweenness	Degree	PageRank	CI	PA	GA	SA
R^a	ER-SF	200	4	0.2182	0.1808	0.4373	0.4317	0.4405	0.1868	0.3519	0.4334	**0.4734**
	ER-SF	500	4	0.3287	0.2789	0.4650	0.4646	0.4634	0.4655	0.2905	0.4152	**0.4792**
	SW-SF	200	4	0.2795	0.2233	0.4408	0.4409	0.4473	0.4412	0.2779	0.4297	**0.4682**
	SW-SF	500	4	0.2845	0.2571	0.4517	0.4482	0.4484	0.4525	0.2645	0.4343	**0.4649**
	SF-SF	200	3	0.2931	0.2196	0.4665	0.4681	0.4661	0.4631	0.2336	0.4508	**0.4826**
	SF-SF	500	3	0.3046	0.2300	0.4792	0.4792	0.2268	0.4792	0.2348	0.4385	**0.4881**
	ER-SW-SF	200	3	0.2286	0.2175	0.4331	0.4321	0.4367	0.4391	0.2482	0.4473	**0.4608**
	ER-SW-SF	500	3	0.2289	0.2003	0.4448	0.4459	0.4428	0.4429	0.2220	0.4515	**0.4597**
R^r	ER-SF	200	4	0.2432	0.2227	0.2575	0.2466	0.2555	0.2389	0.2276	0.3904	**0.4053**
	ER-SF	500	4	0.2293	0.2006	0.2793	0.2177	0.2423	0.2559	0.2185	0.3712	**0.3883**
	SW-SF	200	4	0.2960	0.2690	0.2733	0.2836	0.2818	0.2793	0.2819	0.4037	**0.4145**
	SW-SF	500	4	0.2769	0.2486	0.2899	0.2582	0.2647	0.2707	0.2553	0.3860	**0.3952**
	SF-SF	200	3	0.3158	0.2481	0.2805	0.2868	0.2779	0.2761	0.2588	0.4061	**0.4235**
	SF-SF	500	3	0.2975	0.2196	0.2758	0.2554	0.2531	0.2566	0.2294	0.3916	**0.4033**
	ER-SW-SF	200	3	0.2927	0.2760	0.2971	0.3048	0.2736	0.2770	0.2899	0.4076	**0.4142**
	ER-SW-SF	500	3	0.3359	0.3052	0.3082	0.3104	0.3058	0.3128	0.2982	0.4079	**0.4177**

countries with many trade relationships are protected from a trade war by certain economic terms.

2) Baseline algorithms: Firstly, to demonstrate the vulnerable of tested networks, the Origin method [8] with NCCFs is adopted to evaluate the robustness and resilience of tested networks without adopting any improvement strategy.

Secondly, to validate the destructiveness of the proposed cascading failures, a robustness and resilience comparison is made between the multiplex networks under NCFs (referred to as WC) and those under NCCFs.

Finally, to demonstrate the effectiveness of the proposed SA, the construction of autonomous nodes (PA) [29], the protection of influential nodes with different greedy rules [11] (like Betweenness [11], [30], Degree [11], [30], PageRank [31], [32] and Collective Influence (CI) [33]), and the protection of influential nodes with a genetic algorithm (GA) [57], [58], are chosen as the baseline algorithms for comparative studies. Similar to the work in [11], 5% of influential nodes are protected by all centrality-based greedy algorithms, the GA algorithm and the proposed SA.

Due to the page limitation, the details of aforementioned algorithms such as PA, Betweenness, Degree, PageRank, CI and GA are given in the supplementary document. Note that, due to the high computational complexity ($O(q \cdot n^2 \cdot \log n)$) of computing the objective R^b, $b = a, r$, our SA optimization strategy can only be applicable to networks with $n \leq 5,000$ nodes, while the other optimization strategies (PA, Betweenness, Degree, PageRank and CI) can be applicable to networks with $n \geq 10,000$ nodes.

For the degree-based protection methods (Betweenness, Degree, PageRank and CI), the nodes with high centrality values are protected from damages and failures. For the GA algorithm and the proposed SA, the nodes in the influential set $\mathcal{S}$ are protected from failures.

For each network, all algorithms are tested over 100 trials, with key parameter settings as outlined in Table II.

B. Experiments on synthetic multiplex networks

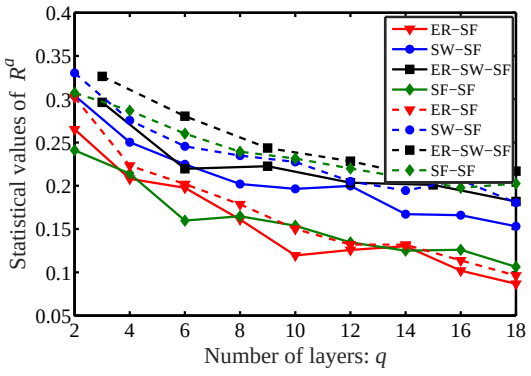
Firstly, all algorithms are tested on synthetic multiplex networks (ER-SF, SW-SF, SF-SF and ER-SW-SF) with $n = 200, 500$, and the corresponding attack robustness R^a and recovery resilience R^r under $\lambda = 0.3$ are recorded in Table III. The results demonstrate that all networks under NCCFs (Origin) have lower R^a and R^r values than those under NCFs (WC). This validates the superiority of the proposed NCCFs over NCFs in generating failures on multiplex networks. These results also illustrate that the SF multiplex networks are vulnerable to random attacks and recoveries, while SA can significantly improve both their attack robustness and recovery resilience. More specifically, the improvements of R^a and R^r can reach 108.5% and 63.94%, respectively. This is reasonable as the 5% of influential nodes protected by SA will not fail directly by attacks and cascading failures, thus suppressing the node-community failures in the network. The results also show that SA achieves higher R^a and R^r values than GA, PA, Betweenness, Degree, PageRank and CI. This demonstrates the effectiveness of the node protection strategy, as well as the superiority of SA over the other baseline algorithms in discovering influential nodes.

As shown in Table III, although they improve the robustness and resilience of multiplex networks, the centrality-based greedy algorithms (Betweenness, Degree, PageRank, CI and PA) can easily get trapped into local optima. This is reasonable as the greedy algorithms facilitate exploitation but they conduct inadequate exploration. Moreover, the population based optimization method (GA) has higher R^a and R^r values than these greedy algorithms in most cases, which validates the effectiveness of GA in improving the robustness and resilience of multiplex networks. However, it is also difficult to find the solution with the highest R^a and R^r values in a limited number of iterations. This is because GA facilitates exploration , but it is lacking in terms of exploitation. By using the probabilistic search strategy in (7), SA can effectively achieve a good robustness and resilience improvement performance.

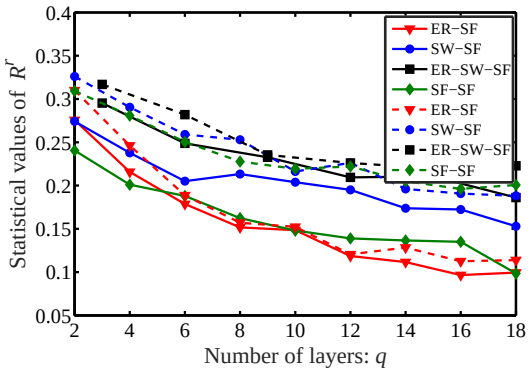
Secondly, to further investigate the vulnerability of ER-SF, SW-SF, ER-SW-SF and SF-SF multiplex networks to random attacks, Fig. 5 shows the variations of the attack robustness R^a and the recovery resilience R^r with the number of layers q of the networks ($n = 500$). The results show that the R^a and R^r values of all networks decrease as q

TABLE IV
COMPARISONS OF ALL ALGORITHMS IN IMPROVING THE ATTACK ROBUSTNESS R^a AND THE RECOVERY RESILIENCE R^r OF TESTED REAL-WORLD MULTIPLEX NETWORKS UNDER $\lambda = 0.3$.

Indexes	Networks	WC	Origin	Betweenness	Degree	PageRank	CI	PA	GA	SA
R^a	CKM	0.0502	0.0459	0.1045	0.1034	0.1078	0.1049	0.0467	0.1107	**0.1117**
	Celegans	0.1762	0.1562	0.2239	0.2305	0.2278	0.2310	0.1587	**0.2636**	0.2476
	FAO	0.0068	0.0002	0.0584	0.0564	0.0581	0.0566	0.0012	0.0531	**0.0615**
R^r	CKM	0.1364	0.1187	0.1282	0.1410	0.1486	0.1404	0.1197	**0.1887**	0.1772
	Celegans	0.2628	0.2247	0.2348	0.2394	0.2301	0.2427	0.2263	**0.2958**	0.2630
	FAO	0.0496	0.0040	0.0416	0.0355	0.0398	0.0372	0.0191	0.0586	**0.0881**



(a)



(b)

Fig. 5. Robustness of the simulated multiplex networks with $n = 500$ vs. Number of layers. (a) the attack robustness R^a and (b) the recovery resilience R^r. The full lines and the dotted lines correspond to the results of all networks under NCCFs and NCFs, respectively.

increases. This is reasonable as it is easier for inter-layer node failures and the community failures to be triggered as the number of layers increases. The results also show that in most cases, the SF-SF networks are the network type most vulnerable to random attacks. This is because the SF networks have clear community structures and their links are mainly distributed to a few high-degree nodes, meaning that failures occurring these communities and nodes may be more likely to trigger cascading failures. Moreover, the ER-SF networks are more vulnerable than the SW-SF and ER-SW-SF networks to random attacks. This is because the ER networks have fewer clear link structures than the SF networks, while the SW networks are more robust to random attacks than the ER and SF networks due to its property having a small average shortest path length among nodes. The results in Table III and Figs. 6 and 7 in the supplementary document show that the tested networks with lesser communities and higher modularity generally have a higher robustness and resilience. This is reasonable as the networks with less communities can restrain community cascading failures, and these with clear community structures can restrain node cascading failures.

Fig. 5 also compares R^a and R^r of tested simulated multiplex networks under NCFs and NCCFs. The results show that all networks under NCCFs have lower R^a and R^r values than those under NCFs. This indicates that all networks are more vulnerable to NCCFs than to NCFs. Moreover, the SW-SF and SF-SF networks have a larger variation in R^a and R^r values than the other networks under NCFs and NCCFs. This is because the SW and SF networks have more clear communities than the ER networks, and community failures decrease in clear communities.

C. Experiments on real multiplex networks

To demonstrate the vulnerable of multiplex networks and the superiority of SA, comparisons between SA and all baseline algorithms are made on three real multiplex networks. The statistical R^a and R^r results of all algorithms over 100 independent trials under $\lambda = 0.3$ are recorded in Table IV. From Table IV, we can make the following observations.

1) The real multiplex networks are very vulnerable to damage during both attacks and recoveries, while the R^a and R^r values vary inversely with the number of communities in the multiplex networks. More specifically, among the test networks, the Celegans multiplex network has the lowest number of communities and the highest R^a and R^r values, while the FAO trade multiplex network has the highest number of communities and the lowest R^a and R^r values. This is because, as the number of communities increases, the size of communities becomes smaller while node failures can more easily cause community failures.

2) All networks under NCFs (Origin) have lower R^a and R^r values than those under NCCFs (WC). This validates that the proposed NCCFs make all tested real multiplex networks more fragile than NCFs. This is reasonable as community failures will trigger both more node failures and more subsequent community failures during both attacks and recoveries.

3) SA significantly improves the robustness and resilience of all real multiplex networks during both attacks and recoveries. More specifically, the improvement of the attack robustness R^a reaches 143%, 59% and 30650% for the CKM, Celegans and FAO multiplex networks, respectively. Moreover, the recovery resilience R^r in the CKM, Celegans and FAO multiplex networks is increased by 49%, 17% and 2103%, respectively.

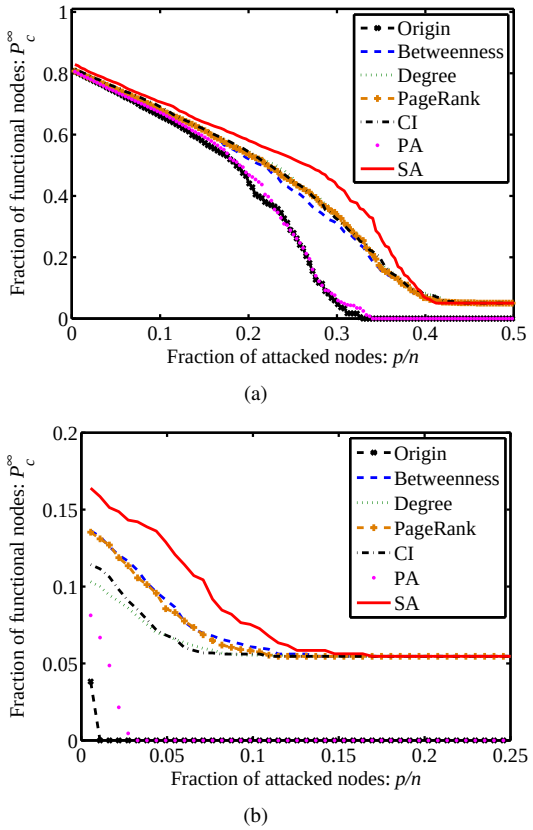


Fig. 6. Variations of the fraction of functional nodes in the real-world multiplex networks protected by SA with the fraction of attacked nodes. (a) the Celegans multiplex network and (b) the FAO multiplex network.

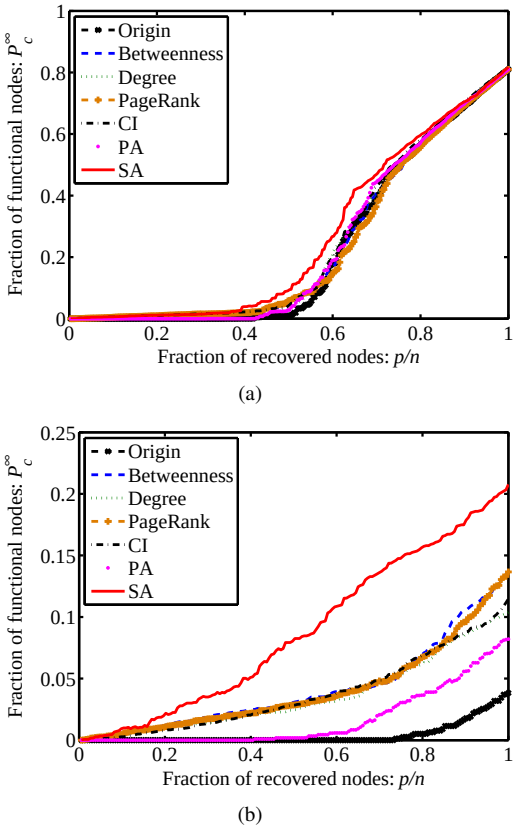


Fig. 7. Variations of the fraction of functional nodes in the real-world multiplex networks protected by SA with the fraction of recovered nodes. (a) the Celegans multiplex network and (b) the FAO multiplex network.

4) All baseline algorithms can improve both the R^a and R^r values of all networks. However, in most cases, they achieve lower R^a and R^r values than SA, which demonstrates the superiority of SA in improving the robustness and resilience of multiplex networks. In baseline algorithms, the autonomous node construction method (PA) shows a worse performance than the node protection methods (Degree, Betweenness, PageRank, CI, GA, and SA). This is to be expected that the autonomous nodes are sensitive to NCCFs trigged by community failures. Moreover, GA and CI show a good performance in improving both the attack robustness and recovery resilience of the CKM and Celegans multiplex networks. This is because these two networks contain only a few of community structures, and GA and CI can effectively find good solutions for optimization problems with a smaller scale (e.g., $n \leq 300$ and $q \leq 3$) and simpler search space ($Q \geq 0.45$ and $n_c \leq 15$).

5) The tested multiplex networks have lower R^a and R^r values than the synthetic SF multiplex networks, which further validates the fragility of real multiplex networks. This is because the real multiplex networks have more complex link structures than the SF multiplex networks. For example, in real multiplex networks, influential nodes are densely linked to the other nodes of the same community.

To further show the network fragility and the effectiveness of SA, the fractions of functional nodes of the Celegans and FAO multiplex networks during each attack and recovery are plotted in Figs. 6 and 7, respectively. The results show that an initial attack will cause failures of 20% and 96% of nodes for the Celegans and FAO multiplex networks, respectively. Moreover, the Celegans and FAO network functionality will collapse when only 32% and 1.5% of nodes are attacked, respectively. However, after protecting 5% of nodes using SA, the damage to these networks caused by the initial attack is decreased, while these networks become able to resist more attacks. More specifically, the Celegans and FAO multiplex networks only lose the functionality of 17% and 83% of nodes after an initial attack, and they can resist random attacks on 42% and 17% of functional nodes, respectively. From Fig. 7, we can reveal similar observations from Fig. 6, i.e., it is easier for networks protected by SA to recover their functionality, and SA can effectively improve the resilience of tested networks.

D. Effects of parameter settings

In the proposed system and SA algorithm, there are two key parameters: the fraction (β) of protected nodes and the threshold (λ) of community failures. Here, we test SA on the FAO multiplex network with different β and λ, and compare R^a and R^r between the original network (i.e., Attack or Recovery) and the network protected by SA (i.e., Attack with SA or Recovery with SA).

Fig. 8 plots the variations of R^a and R^r with different β values. The results illustrate that both R^a and R^r of the

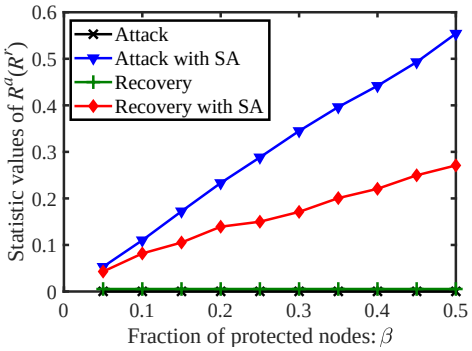


Fig. 8. Statistic robustness of the FAO multiplex network during both attacks and recoveries vs. Fraction β of protected nodes.

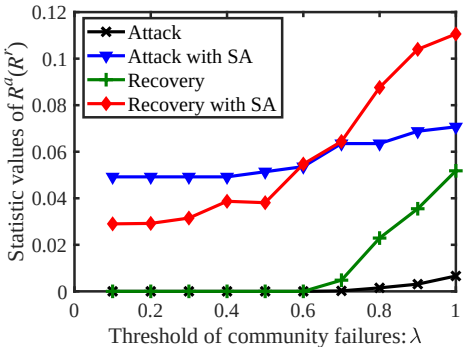


Fig. 9. Statistic robustness and resilience of the FAO multiplex network vs. Threshold λ of community failures.

network protected by SA increase with β. Moreover, the improvement rate of R^r drop sharply when $\beta > 0.25$. Note that, the budget of protecting a network is always finite, and a protection strategy with a higher β results in higher costs. In this study, β is set to 0.05 as both R^a and R^r can be greatly increased by SA at low cost. More specifically, the attack robustness and recovery resilience are improved by 30650% and 2103%, respectively.

Fig. 9 illustrates the R^a and R^r of the FAO multiplex network with different λ values. Generally, with the decrease of λ, it is easier for community failures to occur, which causes more NCCFs. Therefore, the network is more vulnerable to damage during both attacks and recoveries when λ is smaller. This is further validated by the results in Fig. 9. The results also demonstrate the effectiveness of SA in improving the robustness and resilience of the FAO multiplex network under different values of λ.

V. Conclusions

In this paper, we studied the robustness and resilience of multiplex networks, considering the effects of coupling node relationships and community structures on cascading failures. We first modeled the node failure processes of multiplex networks as NCCFs, which combine node cascading failures (triggered by coupling node relationships) with community failures (induced by community structures). Subsequently, we modeled the robustness and resilience improvement of multiplex networks as a constrained optimization problem. To solve this problem, we devised the node protection strategy to protect a minimum set of influential nodes from damage and failure, and further proposed the SA algorithm to find the influential nodes. Extensive experiments on both the simulated SF-multiplex networks and three real multiplex networks demonstrated that the proposed NCCFs make networks more vulnerable to unpredictable damage than classical NCFs. Moreover, they validated the superiority of the proposed SA over six classical algorithms in improving the robustness and resilience of the networks.

In future work, we will analyze the feasibility of the modeled NCCFs and the robustness and resilience improvement strategy in more systems, like social systems under novel COVID-19 attacks [59], nonlinear neural networks under adversarial attacks [60], nonlinear synchronization systems under random perturbance [18]–[20], etc. Moreover, we plan to develop a more rigorous analysis of our theoretical result on more types of multiplex networks (such as ER-SF, SW-SF, SF-SF and ER-SW-SF), and give some theoretical analyses to our optimization problem. In addition, we will study data-driven robustness and resilience optimization, and apply our SA optimization strategy for tackling large-scale networks. Finally, we will study the impacts of the recovery rate on the recovery processes of multiplex networks, as well as the robustness and resilience of interdependent networks with dependent nodes and edges.

References

[1] M. De Domenico, A. Solé-Ribalta, E. Cozzo, M. Kivelä, Y. Moreno, M. A. Porter, S. Gómez, and A. Arenas, "Mathematical formulation of multilayer networks," *Physical Review X*, vol. 3, no. 4, p. 041022, 2013.

[2] B. Yang, J. Liu, and D. Liu, "Characterizing and extracting multiplex patterns in complex networks," *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 42, no. 2, pp. 469–481, 2012.

[3] S. Boccaletti, G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, and M. Zanin, "The structure and dynamics of multilayer networks," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.

[4] W. He, G. Chen, Q.-L. Han, W. Du, J. Cao, and F. Qian, "Multiagent systems on multilayer networks: Synchronization analysis and network design," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 7, pp. 1655–1667, 2017.

[5] J. Zhuang, J. Cao, L. Tang, Y. Xia, and M. Perc, "Synchronization analysis for stochastic delayed multilayer network with additive couplings," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 11, pp. 4807–4816, 2020.

[6] M. M. Danziger, I. Bonamassa, S. Boccaletti, and S. Havlin, "Dynamic interdependence and competition in multilayer networks," *Nature Physics*, vol. 15, no. 2, p. 178, 2019.

[7] J. Liu, X. Wu, J. Lü, and X. Wei, "Infection-probability-dependent interlayer interaction propagation processes in multiplex networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 1085–1096, 2021.

[8] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, p. 1025, 2010.

[9] D. Duan, C. Lv, S. Si, Z. Wang, D. Li, J. Gao, S. Havlin, H. E. Stanley, and S. Boccaletti, "Universal behavior of cascading failures in interdependent networks," *Proceedings of the National Academy of Sciences*, vol. 116, no. 45, pp. 22 452–22 457, 2019.

[10] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, no. 7291, p. 984, 2010.

[11] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Scientific Reports*, vol. 5, p. 8439, 2015.

[12] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, p. 045104, 2004.

[13] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[14] X. Zhang, D. Liu, C. Zhan, and C. K. Tse, "Effects of cyber coupling on cascading failures in power systems," *IEEE Journal of Emerging and Selected Topics in Circuits and Systems*, vol. 7, no. 2, pp. 228–238, 2017.

[15] X. Guan and C. Chen, "General methodology for inferring failure-spreading dynamics in networks," *Proceedings of the National Academy of Sciences*, vol. 115, no. 35, pp. E8125–E8134, 2018.

[16] A. Solé-Ribalta, S. Gómez, and A. Arenas, "Congestion induced by the structure of multiplex networks," *Physical Review Letters*, vol. 116, no. 10, p. 108701, 2016.

[17] W. Sun, S.-F. Su, J. Xia, and Y. Wu, "Adaptive tracking control of wheeled inverted pendulums with periodic disturbances," *IEEE Transactions on Cybernetics*, vol. 50, no. 5, pp. 1867–1876, 2018.

[18] X. F. Wang and G. Chen, "Synchronization in scale-free dynamical networks: robustness and fragility," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 1, pp. 54–62, 2002.

[19] Y. Wei, J. Qiu, P. Shi, and L. Wu, "A piecewise-markovian lyapunov approach to reliable output feedback control for fuzzy-affine systems with time-delays and actuator faults," *IEEE Transactions on Cybernetics*, vol. 48, no. 9, pp. 2723–2735, 2018.

[20] Y. Wei, H. Yu, H. R. Karimi, and Y. H. Joo, "New approach to fixed-order output-feedback control for piecewise-affine systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 9, pp. 2961–2969, 2018.

[21] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 41, no. 6, pp. 1244–1252, 2011.

[22] Y. Huang, J. Wu, W. Ren, K. T. Chi, and Z. Zheng, "Sequential restorations of complex networks after cascading failures," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 400–411, 2021.

[23] X.-L. Ren, N. Gleinig, D. Helbing, and N. Antulov-Fantulin, "Generalized network dismantling," *Proceedings of the National Academy of Sciences*, vol. 116, no. 14, pp. 6554–6559, 2019.

[24] Q. Cai, S. Alam, M. Pratama, and J. Liu, "Robustness evaluation of multipartite complex networks based on percolation theory," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, p. doi:10.1109/TSMC.2019.2960156, 2020.

[25] L. Ma, M. Gong, Q. Cai, and L. Jiao, "Enhancing community integrity of networks against multilevel targeted attacks," *Physical Review E*, vol. 88, no. 2, p. 022810, 2013.

[26] M. Zhou and J. Liu, "A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks," *IEEE Transactions on Cybernetics*, vol. 47, no. 2, pp. 539–552, 2017.

[27] W. Liu, M. Gong, S. Wang, and L. Ma, "A two-level learning strategy based memetic algorithm for enhancing community robustness of networks," *Information Sciences*, vol. 422, pp. 290–304, 2018.

[28] 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, p. 048701, 2010.

[29] C. M. Schneider, N. Yazdani, N. A. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Scientific Reports*, vol. 3, p. 1969, 2013.

[30] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215–239, 1978.

[31] S. Pei and H. A. Makse, "Spreading dynamics in complex networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2013, no. 12, p. P12002, 2013.

[32] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," *Computer Networks and ISDN Systems*, vol. 30, no. 1-7, pp. 107–117, 1998.

[33] F. Morone and H. A. Makse, "Influence maximization in complex networks through optimal percolation," *Nature*, vol. 524, no. 7563, p. 65, 2015.

[34] S. D. Reis, Y. Hu, A. Babino, J. S. Andrade Jr, S. Canals, M. Sigman, and H. A. Makse, "Avoiding catastrophic failure in correlated networks of networks," *Nature Physics*, vol. 10, no. 10, p. 762, 2014.

[35] 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, no. 1, p. 34, 2014.

[36] X. Wang, J. Lü, and X. Wu, "Recovering network structures with time-varying nodal parameters," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 7, pp. 2588–2598, 2020.

[37] Y. Shang, "Impact of self-healing capability on network robustness," *Physical Review E*, vol. 91, no. 4, p. 042804, 2015.

[38] G. Dong, J. Fan, L. M. Shekhtman, S. Shai, R. Du, L. Tian, X. Chen, H. E. Stanley, and S. Havlin, "Resilience of networks with community structure behaves as if under an external field," *Proceedings of the National Academy of Sciences*, vol. 1, p. 588, 2018.

[39] T. Qiu, A. Zhao, F. Xia, W. Si, D. O. Wu, T. Qiu, A. Zhao, F. Xia, W. Si, and D. O. Wu, "Rose: Robustness strategy for scale-free wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2944–2959, 2017.

[40] P. J. Mucha, T. Richardson, K. Macon, M. A. Porter, and J.-P. Onnela, "Community structure in time-dependent, multiscale, and multiplex networks," *Science*, vol. 328, no. 5980, pp. 876–878, 2010.

[41] B. Wellman, "The network community: An introduction," in *Networks in the Global Village*. Routledge, 2018, pp. 1–47.

[42] S. Wang and J. Liu, "Constructing robust community structure against edge-based attacks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 582–592, 2018.

[43] S. Wang and J. Liu, "Community robustness and its enhancement in interdependent networks," *Applied Soft Computing*, vol. 77, pp. 665–677, 2019.

[44] S. Wang and J. Liu, "Designing comprehensively robust networks against intentional attacks and cascading failures," *Information Sciences*, vol. 478, pp. 125–140, 2019.

[45] S. Kirkpatrick, C. D. Gellatt, and M. P. Vecchi, "Optimisation by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1982.

[46] N. Mamano and W. B. Hayes, "Sana: simulated annealing far outperforms many other search algorithms for biological network alignment," *Bioinformatics*, vol. 33, no. 14, pp. 2156–2164, 2017.

[47] N. Dehmamy, S. Milanlouei, and A.-L. Barabási, "A structural transition in physical networks," *Nature*, vol. 563, no. 7733, p. 676, 2018.

[48] M. Newman and M. Girvan, "Finding and evaluating community structure in networks," *Physical Review E*, vol. 69, no. 2, p. 026113, 2004.

[49] Y. Hu, D. Zhou, R. Zhang, Z. Han, C. Rozenblat, and S. Havlin, "Percolation of interdependent networks with intersimilarity," *Physical Review E*, vol. 88, no. 5, p. 052805, 2013.

[50] L. Lü, T. Zhou, Q.-M. Zhang, and H. E. Stanley, "The h-index of a network node and its relation to degree and coreness," *Nature Communications*, vol. 7, p. 10168, 2016.

[51] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, no. 1, pp. 17–60, 1960.

[52] A.-L. Barabási, "Scale-free networks: a decade and beyond," *Science*, vol. 325, no. 5939, pp. 412–413, 2009.

[53] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-worldnetworks," *Nature*, vol. 393, no. 6684, p. 440, 1998.

[54] J. Coleman, E. Katz, and H. Menzel, "The diffusion of an innovation among physicians," *Sociometry*, vol. 20, no. 4, pp. 253–270, 1957.

[55] C. Stark, B.-J. Breitkreutz, T. Reguly, L. Boucher, A. Breitkreutz, and M. Tyers, "Biogrid: A general repository for interaction datasets," *Nucleic Acids Research*, vol. 34, no. suppl_1, pp. D535–D539, 2006.

[56] M. De Domenico, V. Nicosia, A. Arenas, and V. Latora, "Structural reducibility of multilayer networks," *Nature Communications*, vol. 6, p. 6864, 2015.

[57] L. Ma, M. Gong, J. Liu, Q. Cai, and L. Jiao, "Multi-level learning based memetic algorithm for community detection," *Applied Soft Computing*, vol. 19, pp. 121–133, 2014.

[58] M. Gong, C. Song, C. Duan, L. Ma, and B. Shen, "An efficient memetic algorithm for influence maximization in social networks," *IEEE Computational Intelligence Magazine*, vol. 11, no. 3, pp. 22–33, 2016.

[59] L. Peeples, "News feature: Avoiding pitfalls in the pursuit of a covid-19 vaccine," *Proceedings of the National Academy of Sciences*, vol. 117, no. 15, pp. 8218–8221, 2020.

[60] D. Zügner, A. Akbarnejad, and S. Günnemann, "Adversarial attacks on neural networks for graph data," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018, pp. 2847–2856.

Lijia Ma received the B.S. degree in communication engineering from Hunan Normal University, Changsha, China, and the Ph.D. degree in electronic science and technology from Xidian University, Xi'an, China, in 2010 and 2015, respectively.

From 2015 to 2016, he was a Postdoctoral Fellow with Hong Kong Baptist University, Hong Kong, and with Nanyang Technological University, Singapore, from 2016 to 2017. He is an assistant professor at the College of Computer and Software Engineering of Shenzhen University. His research interests mainly include evolutionary computation, machine learning and complex networks.

Xiao Zhang received the B.S. and M.S. degree in computer science from Shenzhen University, Shenzhen, China, in 2017 and 2020, respectively.

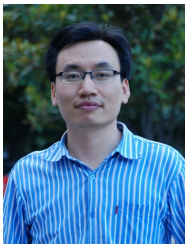
He is currently a Research Assistant with the College of Computer Science and Software Engineering, Shenzhen University. His current research interests are in complex network, machine learning and evolutionary computation.

Jianqiang Li received his B.S. and Ph.D. Degree in automation major from South China University of Technology, Guangzhou, China, in 2003 and 2008, respectively.

He is a professor at the College of Computer and Software Engineering of Shenzhen University. He led three projects of the National Natural Science Foundation of China. His major research interests include embedded systems and Internet of Things.

Qiuzhen Lin (M'18) received the B.S. degree from Zhaoqing University and the M.S. degree from Shenzhen University, China, in 2007 and 2010, respectively. He received the Ph.D. degree from Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong, in 2014.

He is currently an associate professor in College of Computer Science and Software Engineering, Shenzhen University. His current research interests include artificial immune system, multi-objective optimization and dynamic system.



Maoguo Gong (M'07-SM'14) received the B.S. degree and Ph.D. degree in electronic science and technology from Xidian University, Xi'an, China, in 2003 and 2009, respectively.

Since 2006, he has been a Teacher with Xidian University. In 2008 and 2010, he was promoted as an Associate Professor and as a Full Professor, respectively, both with exceptive admission. His research interests are in the area of computational intelligence with applications to optimization, learning, data mining and image understanding.

Dr. Gong received the prestigious National Program for the support of Top-Notch Young Professionals from the Central Organization Department of China, the Excellent Young Scientist Foundation from the National Natural Science Foundation of China, and the New Century Excellent Talent in University from the Ministry of Education of China. He is the Vice Chair of the IEEE Computational Intelligence Society Task Force on Memetic Computing, an Executive Committee Member of the Chinese Association for Artificial Intelligence, and a Senior Member of the Chinese Computer Federation. He is also the associate editor of *IEEE Trans. Evolutionary Computation*.

Carlos A. Coello Coello (M'98-SM'04-F'11) received Ph.D. degree in computer science from Tulane University, USA, in 1996. He is currently Professor (CINVESTAV-3F Researcher) at the Computer Science Department of CINVESTAV-IPN, in Mexico City, Mxico. Dr. Coello has authored and co-authored over 450 technical papers and book chapters. He has also co-authored the book *Evolutionary Algorithms for Solving Multi-Objective Problems* (Second Edition, Springer, 2007). His publications report over 55,000 citations in Google Scholar (his h-index is 95). Currently, he is associate editor of the *IEEE Transactions on Evolutionary Computation* and serves in the editorial board of 12 other international journals. His major research interests are: evolutionary multi-objective optimization and constraint-handling techniques for evolutionary algorithms. He received the *2007 National Research Award* from the Mexican Academy of Sciences in the area of Exact Sciences, the *2013 IEEE Kiyo Tomiyasu Award* and the *2012 National Medal of Science and Arts* in the area of *Physical, Mathematical and Natural Sciences*. He is a Fellow of the IEEE, and a member of the ACM, Sigma Xi, and the Mexican Academy of Science.

Asoke K. Nandi (F'11) received Ph.D. degree in Physics from the University of Cambridge (Trinity College), Cambridge (UK). He held academic positions in several universities, including Oxford (UK), Imperial College London (UK), Strathclyde (UK), and Liverpool (UK) as well as Finland Distinguished Professorship in Jyvaskyla (Finland). In 2013, he moved to Brunel University London (UK), to become the Chair and Head of Electronic and Computer Engineering. Professor Nandi is a Distinguished Visiting Professor at Shenzhen University (China) and an Adjunct Professor at University of Calgary (Canada).

In 1983, Professor Nandi co-discovered the three fundamental particles known as W^+, W^- and Z^0 (by the UA1 team at CERN), providing the evidence for the unification of the electromagnetic and weak forces, for which the Nobel Committee for Physics in 1984 awarded the prize to his two team leaders for their decisive contributions. His current research interests lie in signal processing and machine learning, with applications to communications, image segmentations, biomedical data, etc. He has made many fundamental theoretical and algorithmic contributions to many aspects of signal processing and machine learning. He has much expertise in Big and Heterogeneous Data, dealing with modelling, classification, estimation, and prediction.

He has authored over 600 technical publications, including 250 journal papers as well as five books, entitled Condition Monitoring with Vibration Signals: Compressive Sampling and Learning Algorithms for Rotating Machines (Wiley, 2020), Automatic Modulation Classification: Principles, Algorithms and Applications (Wiley, 2015), Integrative Cluster Analysis in Bioinformatics (Wiley, 2015), Blind Estimation Using Higher-Order Statistics (Springer, 1999), and Automatic Modulation Recognition of Communications Signals (Springer, 1996). The H-index of his publications is 80 (Google Scholar) and his ERDOS number is 2.

Professor Nandi is a Fellow of the Royal Academy of Engineering (UK) as well as a Fellow of seven other institutions, including the IEEE and the IET. Among the many awards he received are the Institute of Electrical and Electronics Engineers (USA) Heinrich Hertz Award in 2012, the Glory of Bengal Award for his outstanding achievements in scientific research in 2010, the Water Arbitration Prize of the Institution of Mechanical Engineers (UK) in 1999, and the Mountbatten Premium, Division Award of the Electronics and Communications Division, of the Institution of Electrical Engineers (UK) in 1998. Professor Nandi is an IEEE EMBS Distinguished Lecturer (2018-19).