Supplementary Document of “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*

This is the supplementary document to the paper entitled “Enhancing Robustness and Resilience of Multiplex Networks against Node-community Cascading Failures” and submitted to IEEE Transactions on Systems, Man, and Cybernetics: Systems. Some theoretical and experimental analyses are shown in this supplementary document due to page limitations of paper.

I. THEORETICAL ANALYSES

For simplicity and without loss of generality, we consider a multiplex network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}^{[1]}, \mathcal{E}^{[2]}\}$ with $|\mathcal{V}| = n$ nodes and $q = 2$ layers of edges. Each network $\mathcal{G}^{[\alpha]} = \{\mathcal{V}, \mathcal{E}^{[\alpha]}\}$, $\alpha \in \{1, 2\}$, follows a degree distribution $P_0^{[\alpha]}(k)$ and a community size distribution $Q_0^{[\alpha]}(s)$, where k and s denote the node degree and community size, respectively. In our robustness (or resilience) evaluation model, nodes and links are normally functional in $\mathcal{G}$ if and only if they are in the largest connected component (LCC) and their community is functional. We call the functional LCC in our evaluation model as the community-aware LCC.

We assume that a fraction p/n of nodes are removed from $\mathcal{G}$ due to failures. In this case, the node failures may first cause node cascading failures, and then may further trigger community failures. These failures occur recursively until there are no further node failures. We call this failure model as the node-community cascading failures (NCCFs).

Under the NCCFs, we let P^∞ and $\overline{P_c^\infty}$ denote the fractions of community-aware LCC after the first round of node cascading failures (NCFs) and the first round of community failure, respectively. Moreover, we let P_c^∞ be the final fraction of community-aware LCC after all cascades of node and community failures. For a given multiplex network $\mathcal{G}$ with q (e.g., $q = 2$) layers, P_c^∞ can be approximately computed by the following expression:

$$\overline{P_c^\infty} = \rho \cdot (P^\infty + P_c^\infty), \tag{1}$$

where $\rho \in [0, 1]$ is a control parameter used to determine the relation among $P^\infty, \overline{P_c^\infty}$ and P_c^∞. This approximate expression is inspired by some real phenomena: for example, the final failures of social systems caused by natural disasters (like earthquakes and tsunamis) are highly related to the first round of cascading failures, as has been validated by several experiments. In further work, we will further study the theoretical analyses of this relation.

Here, P^∞ can be computed as follows:

$$\begin{aligned} P^\infty = (1 - p/n) \cdot \sum_{k_1=0}^{\infty} \left[P_0^{[1]}(k_1) - P_0^{[1]}(k_1)\mathbf{G}_0^{[1]}(1 - u_0^{[1]})\right] \\ \cdot \sum_{k_2=0}^{\infty} \left[P_0^{[2]}(k_2) - P_0^{[2]}(k_2)\mathbf{G}_0^{[2]}(1 - u_0^{[2]})\right] \end{aligned}, \tag{2}$$

where $P_0^{[\alpha]}(k)$ is the degree distribution of $\mathcal{G}^{[\alpha]}$, while $\mathbf{G}_0^{[\alpha]}(x)$ is the generating function of $P_0^{[\alpha]}(k)$, $\alpha = 1, 2, \ldots, q$. $\mathbf{G}_0^{[\alpha]}(x)$ is evaluated as follows:

$$\mathbf{G}_0^{[\alpha]}(x) = \sum_{k=0}^{\infty} P_0^{[\alpha]}(k) \cdot x^k, \tag{3}$$

while $u_0^{[\alpha]}$ is the fraction of the LCC of $\mathcal{G}^{[\alpha]}$ under NCFs, which follows the following self-consistent probability equations (see [1]):

$$\begin{aligned} u_0^{[1]} = (1 - p/n) \cdot \sum_{k_1=0}^{\infty} \frac{P_0^{[1]}(k_1) \cdot k_1}{< k_0^{[1]} >} \cdot [1 - (1 - u_0^{[1]})^{k_1 - 1}] \\ \cdot \sum_{k_2=0}^{\infty} P_0^{[2]}(k_2) \cdot [1 - (1 - u_0^{[2]})^{k_2}] \end{aligned}, \tag{4}$$

$$\begin{aligned} u_0^{[2]} = (1 - p/n) \cdot \sum_{k_2=0}^{\infty} \frac{P_0^{[2]}(k_2) \cdot k_2}{< k_0^{[2]} >} \cdot [1 - (1 - u_0^{[2]})^{k_2 - 1}] \\ \cdot \sum_{k_1=0}^{\infty} P_0^{[1]}(k_1) \cdot [1 - (1 - u_0^{[1]})^{k_1}] \end{aligned}, \tag{5}$$

where $< k_0^{[\alpha]} >$ denotes the average node degree of $\mathcal{G}^{[\alpha]}$, $\alpha \in \{1, 2\}$.

For each $\alpha \in \{1, 2\}$, we let $P^{[\alpha]}(k)$ denote the degree distribution of the failed network $\mathcal{G}^{[\alpha]}$ which undergone node cascading failures. As known from [2], for each $\alpha = 1, 2 \ldots, q$, we can obtain the following relationship:

$$\mathbf{G}^{[\alpha]}(x) = \mathbf{G}_0^{[\alpha]}(1 - P^\infty \cdot (1 - x)), \tag{6}$$

where $\mathbf{G}^{[\alpha]}(x)$ is the generating function of the degree distribution $P^{[\alpha]}(k)$.

The node cascading failures cause the failures of a fraction $1 - P^\infty$ of nodes, and theses failures will further result in the failures of a fraction $1-P_r$ of communities. This fraction $1-P_r$ is computed as follows:

$$1-P_r=\sum_{s^{[\alpha]}=1}^{\infty} P_f^{[\alpha]}(s^{[\alpha]})\cdot Q_0^{[\alpha]}(s^{[\alpha]}), \tag{7}$$

where $P_f^{[\alpha]}(s^{[\alpha]})$ is the failure probability of a community c with size $s^{[\alpha]}$ in the multiplex network at layer α. Formally, $P_f^{[\alpha]}(s^{[\alpha]})$ is computed as follows:

$$P_f^{[\alpha]}(s^{[\alpha]})=\sum_{s=0}^{\lfloor(1-\lambda)\times s^{[\alpha]}\rfloor}\binom{s^{[\alpha]}}{s}\cdot(P^{\infty})^{s}\cdot(1-P^{\infty})^{s^{[\alpha]}-s}, \tag{8}$$

where λ is the threshold of community failures.

Subsequently, the failures of a fraction $1-P_r$ of communities may further trigger a cascade of community failures. To further study these failures, we first construct a novel multiplex network $\mathcal{G}_c$ with a set of supernodes, in which each supernode is a community of the original multiplex network $\mathcal{G}$, while the links are the edges of $\mathcal{G}$ that are connected two nodes in different communities. Fig. 1 gives a schematic illustrations of the construction of a novel multiplex network $\mathcal{G}_c$ with a set of supernodes.

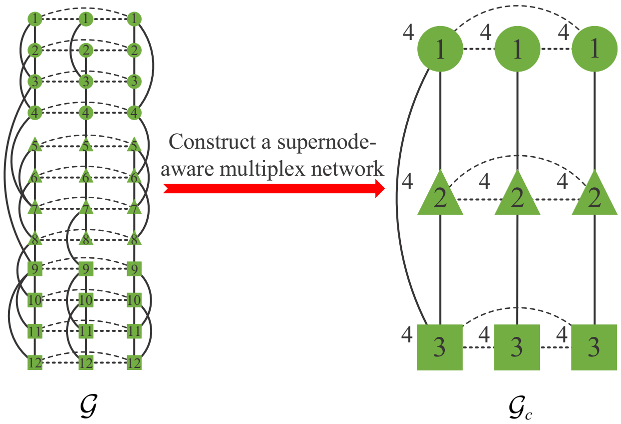


Fig. 1: Schematic illustrations of the construction of a novel multiplex network $\mathcal{G}_c$ with a set of supernodes. Each supernode in $\mathcal{G}_c$ is a community of the original multiplex network $\mathcal{G}$, and each link in $\mathcal{G}_c$ is the links between two communities of $\mathcal{G}$. Nodes with the same shapes are in the same communities, while the numbers around supernodes are the size (or number of nodes) of the supernodes.

Then, we approximately model community cascading failures in $\mathcal{G}$ as node cascading failures in $\mathcal{G}_c$. We let $Q(s^{[1]},s^{[2]})$ denote the joint community size distribution of $\mathcal{G}$ at all layers after node cascading failures are occurred, and let $\mathbf{D}(x,y)$ be the generating function of $Q(s^{[1]},s^{[2]})$. $Q(s^{[1]},s^{[2]})$ can be evaluated as follows:

$$Q(s^{[1]},s^{[2]})=\begin{cases}0 & \text{if } s^{[1]}\neq s^{[2]}\\ Q^{[1]}(s^{[1]})=Q^{[2]}(s^{[2]}) & \text{if } s^{[1]}=s^{[2]}\end{cases}, \tag{9}$$

where $Q^{[\alpha]}(s)$ denotes the community size distribution of the failed network $\mathcal{G}^{[\alpha]}$ after node cascading failures are occurred, $\alpha=1,2$. Formally, $Q^{[\alpha]}(s)$ is evaluated as follows:

$$Q^{[\alpha]}(s)=\sum_{s_0=s}^{\infty} Q_0^{[\alpha]}(s_0)\cdot\binom{s_0}{s}\cdot(P^{\infty})^{s}\cdot(1-P^{\infty})^{s_0-s}. \tag{10}$$

$\mathbf{D}(x,y)$ of $Q(s^{[1]},s^{[2]})$ can be computed as follows:

$$\mathbf{D}(x,y)=\sum_{s^{[1]}=1}^{\infty}\sum_{s^{[2]}=1}^{\infty} Q(s^{[1]},s^{[2]})\cdot x^{s^{[1]}}\cdot y^{s^{[2]}}. \tag{11}$$

Moreover, we let $P_c(k^{[1]},k^{[2]})$ denote the probability that a supernode in $\mathcal{G}_c^{[1]}$ has a community degree $k^{[1]}$ while its corresponding supernode in $\mathcal{G}_c^{[2]}$ has a community degree $k^{[2]}$, and let $\mathbf{G}(x,y)$ be the generating function of $P_c(k^{[1]},k^{[2]})$. Here, $\mathbf{G}(x,y)$ can be computed as follows [3]:

$$\mathbf{G}(x,y)=\sum_{k^{[1]}=0}^{\infty}\sum_{k^{[2]}=0}^{\infty} P_c(k^{[1]},k^{[2]})\cdot x^{k^{[1]}}\cdot y^{k^{[2]}}, \tag{12}$$

and we have the following relation [3]:

$$\mathbf{G}(x,y)=\mathbf{D}(\mathbf{G}^{[1]}(x),\mathbf{G}^{[2]}(y)). \tag{13}$$

Next, we can compute $\overline{P_c^{\infty}}$ of $\mathcal{G}_c$ with a fraction $1-P_r$ of failed supernodes under supernode cascading failures by the following self-consistent probabilities equations [3]:

$$\begin{aligned}u^{[1]}=P^{\infty}\cdot P_r\cdot\Big[&1-(\mathbf{G}_x(1-u^{[1]},1)+\mathbf{G}_x(1,1-u^{[2]})\\ &-\mathbf{G}_x(1-u^{[1]},1-u^{[2]}))/\mathbf{G}_x(1,1)\Big],\end{aligned} \tag{14}$$

$$\begin{aligned}u^{[2]}=P^{\infty}\cdot P_r\cdot\Big[&1-(\mathbf{G}_y(1-u^{[1]},1)+\mathbf{G}_y(1,1-u^{[2]})\\ &-\mathbf{G}_y(1-u^{[1]},1-u^{[2]}))/\mathbf{G}_y(1,1)\Big],\end{aligned} \tag{15}$$

$$\begin{aligned}\overline{P_c^{\infty}}=P^{\infty}\cdot P_r\cdot\Big[&1-\mathbf{F}^{[1]}(1-u^{[1]},1)\\ &-\mathbf{F}^{[1]}(1,1-u^{[2]})+\mathbf{F}^{[1]}(1-u^{[1]},1-u^{[2]})\Big],\end{aligned} \tag{16}$$

where $\mathbf{G}_x(\cdot)=\partial\mathbf{G}(x,y)/\partial x$ and $\mathbf{G}_y(\cdot)=\partial\mathbf{G}(x,y)/\partial y$ are the partial derivative of $\mathbf{G}(x,y)$ with respect to x and y, respectively. Moreover,

$$\mathbf{F}^{[1]}(x,y)=\frac{\mathbf{T}^{[1]}(\mathbf{G}^{[1]}(x),\mathbf{G}^{[2]}(y))}{\mathbf{T}^{[1]}(1,1)}, \tag{17}$$

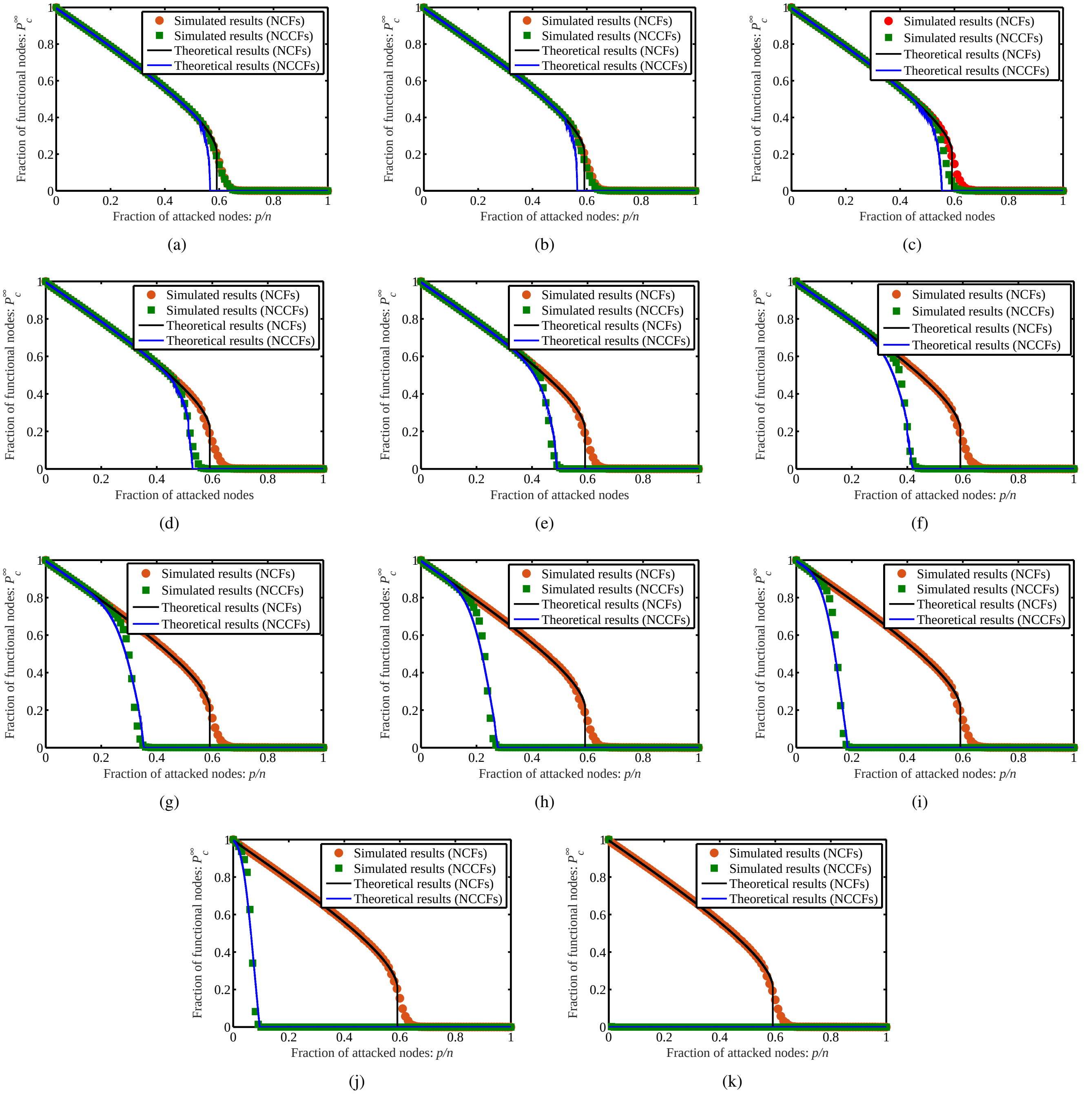
and

$$\begin{aligned}\mathbf{T}^{[1]}(x,y)&=x\cdot\frac{\partial\mathbf{D}(x,y)}{\partial x}\\ &=\sum_{s^{[1]}=1}^{\infty}\sum_{s^{[2]}=1}^{\infty} s^{[1]}\cdot Q(s^{[1]},s^{[2]})\cdot x^{s^{[1]}}\cdot y^{s^{[2]}}.\end{aligned} \tag{18}$$

Here, $\mathbf{T}^{[1]}(1,1)$ is the average community size of failed network $\mathcal{G}$ which undergone node cascading failures.

Finally, we can evaluate P_c^{∞} based on (1), (14), (15) and (16).

An illustration of the P_c^{∞} computation on ER-ER multiplex networks with $q=2$ is then given as follows. As ER multiplex



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k)

Fig. 2: Schematic illustrations of the variations of the fraction of functional nodes with the fraction p/n of randomly attacked nodes on ER-ER networks under NCFs and NCCFs with $\rho = 0.5$. The ER-ER networks with $n = 500$ and $\bar{k} = 6$ under (a) $\lambda = 1.0$, (b) $\lambda = 0.9$, (c) $\lambda = 0.8$, (d) $\lambda = 0.7$, (e) $\lambda = 0.6$, (f) $\lambda = 0.5$, (g) $\lambda = 0.4$, (h) $\lambda = 0.3$, (i) $\lambda = 0.2$, (j) $\lambda = 0.1$, and (k) $\lambda = 0.01$, where $\bar{k}$ is the average degree of the network while λ is the threshold of community failure.

networks follow a Poisson distribution, we can evaluate the generating function of the degree distribution of $\mathcal{G}^{[\alpha]}$, $\alpha = 1, 2$, as follows:

$$\mathbf{G}_0^{[1]}(x) = e^{<k_0^{[1]}>\cdot(x-1)}, \tag{19}$$

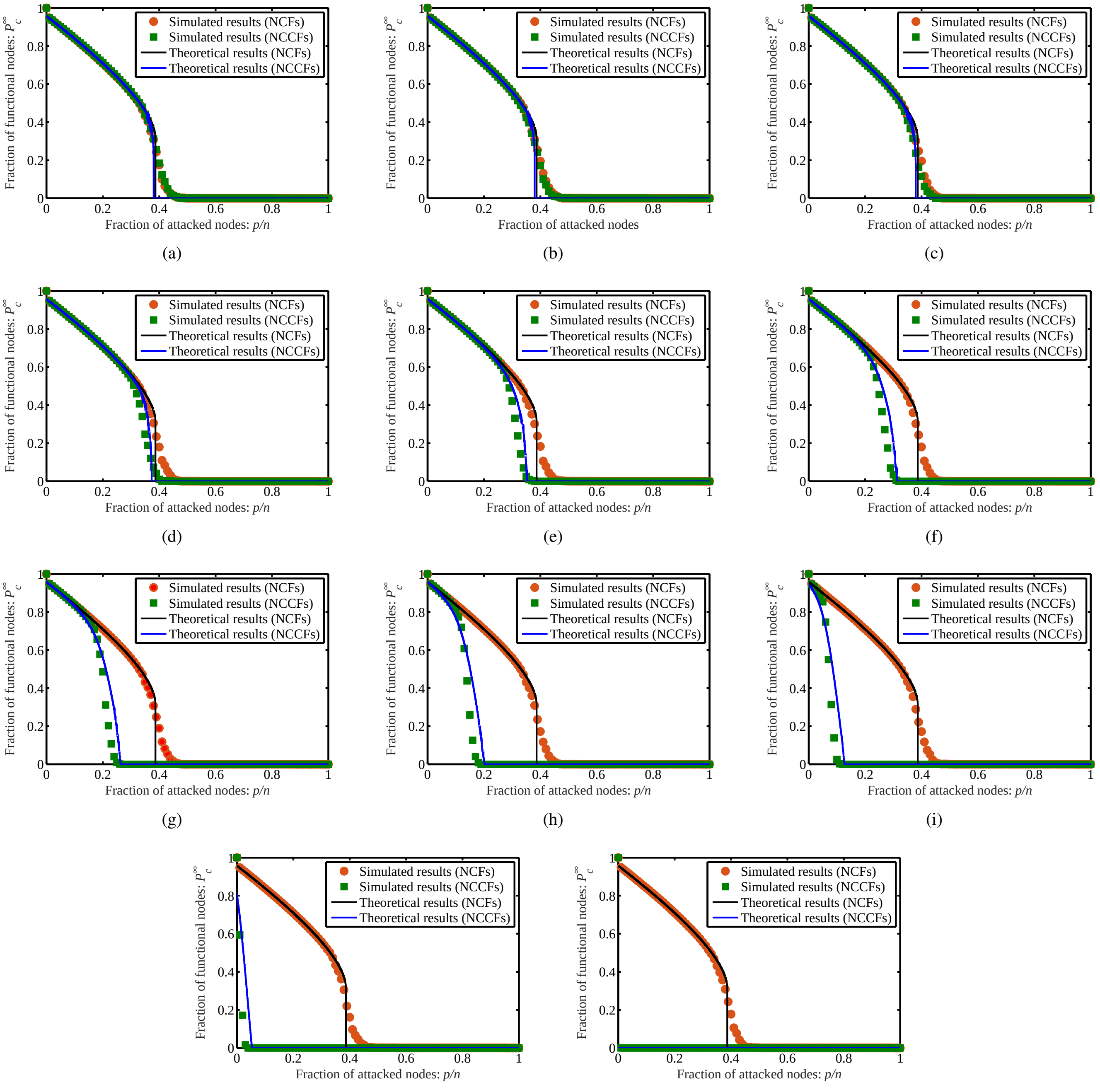
$$\mathbf{G}_0^{[2]}(x) = e^{<k_0^{[2]}>\cdot(x-1)}, \tag{20}$$

where $< k_0^{[\alpha]} >$ is the average degree of $\mathcal{G}^{[\alpha]}$, $\alpha = 1, 2$.

Then, we can obtain the implicit equation of P^∞ based on (2), (4), and (5). Formally, the implicit equation of P^∞ is represented as follows:

$$P^\infty = (1 - p/n) \cdot \left[1 - e^{-<k_0^{[1]}>\cdot P^\infty}\right] \cdot \left[1 - e^{-<k_0^{[2]}>\cdot P^\infty}\right]. \tag{21}$$

This implicit equation can be solved by using numerical methods. After this implicit equation is solved, we can obtain the P^∞ value.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k)

Fig. 3: Schematic illustrations of the variations of the fraction of functional nodes with the fraction p/n of randomly attacked nodes on ER-ER networks under NCFs and NCCFs with $\rho = 0.5$. The ER-ER networks with $n = 500$ and $\bar{k} = 4$ under (a) $\lambda = 1$, (b) $\lambda = 0.9$, (c) $\lambda = 0.8$, (d) $\lambda = 0.7$, (e) $\lambda = 0.6$, (f) $\lambda = 0.5$, (g) $\lambda = 0.4$, (h) $\lambda = 0.3$, (i) $\lambda = 0.2$, (j) $\lambda = 0.1$, and (k) $\lambda = 0.01$, where $\bar{k}$ is the average degree of the network while λ is the threshold of community failure.

Subsequently, we can obtain the implicit equation of $\overline{P_c^\infty}$ based on (16). Formally, the implicit equation of $\overline{P_c^\infty}$ is represented as follows:

$$\overline{P_c^\infty} = P^\infty \cdot P_r \cdot \left[1 - \frac{\sum_{s=1}^{\infty}\left[s \cdot Q^{[1]}(s) \cdot f(\overline{P_c^\infty})\right]}{\sum_{s=1}^{\infty} s \cdot Q^{[1]}(s)}\right], \tag{22}$$

where $Q^{[1]}(s)$ is the community size distribution of the failed network $\mathcal{G}^{[1]}$ which undergone node cascading failures, while $f(\overline{P_c^\infty})$ is evaluated as follows

$$\begin{aligned} f(\overline{P_c^\infty}) = {} & e^{-<k_0^{[1]}>\cdot P^\infty \cdot s \cdot \overline{P_c^\infty}} + e^{-<k_0^{[2]}>\cdot P^\infty \cdot s \cdot \overline{P_c^\infty}} \\ & - e^{-(<k_0^{[1]}>+<k_0^{[2]}>)\cdot P^\infty \cdot s \cdot \overline{P_c^\infty}}. \end{aligned} \tag{23}$$

Similarly, the implicit equation in (22) can be solved by using numerical methods. After this implicit equation is solved, we can obtain the $\overline{P_c^\infty}$ value.

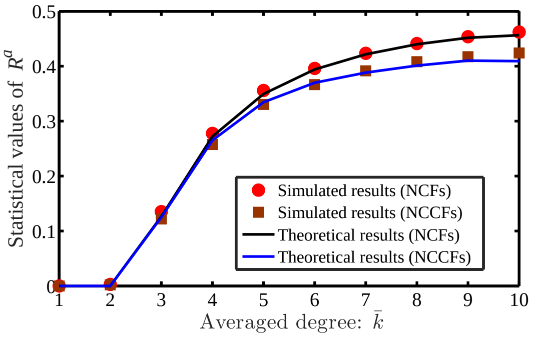


Fig. 4: Variations of the attack robustness R_a of ER-ER multiplex networks with $n = 500$ and $\lambda = 0.3$ with the average degree $\bar{k}$.

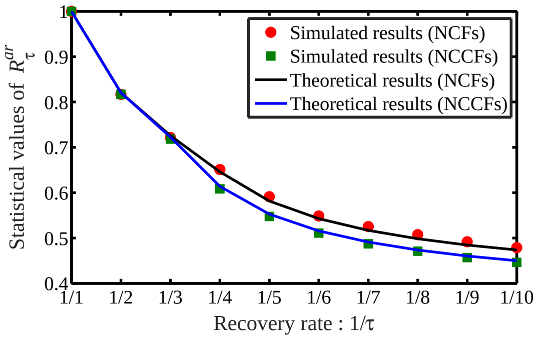


Fig. 5: Variations of R_τ^{ar} with $1/\tau$ on the ER-ER networks with $n = 500$, $\bar{k} = 6$ and $\lambda = 0.3$.

Finally, we can obtain the P_c^∞ value based on the computed P^∞ and $\overline{P_c^\infty}$ values, and (22).

To demonstrate the effectiveness of the aforementioned theoretical analyses, Figs. 2 and 3 show the variations of $\overline{P_c^\infty}$ with fraction (p/n) of randomly damaged nodes on two types of ER-ER multiplex networks with $n = 500$. All results in Figs. 2 and 3 are averaged over 100 ER-ER networks with each network tested over 10,000 independent runs. These results show that the simulated results approximate the theoretical results well, and that the ER-ER networks are more fragile to NCCFs than to NCFs. Moreover, the ER-ER multiplex networks with higher node degrees are more robust to attacks.

Fig. 4 shows the variations of the attack robustness R_a of ER-ER multiplex networks with $n = 500$ as the average degree $\bar{k}$ ranging from 1 to 10. The results show that the simulated results approximate the theoretical results well in different $\bar{k}$ values. Moreover, the ER-ER networks become more robust to attacks as $\bar{k}$ increases. This is because intra-layer node failures decrease as the number of intra-layer links increases.

II. ROBUSTNESS OF MULTIPLEX NETWORKS DURING THE MIXING OF ATTACKS AND RECOVERIES

In some real-world cases, a mix of attacks and recoveries occur simultaneously, and the mixing weight is controlled by a recovery rate $1/\tau$. $1/\tau$ represents one recovery after each τ attacks. To analyze this mixing case, we first define an attack and recovery robustness R^{ar} of a multiplex network, and then give some theoretically and experimentally analyses of the robustness of the ER-ER multiplex networks under different recovery rates.

The attack and recovery robustness R_τ^{ar} evaluates the resilience (or fraction) of functional nodes during all n possible mixing attacks $\mathbf{T}^a$ and recoveries $\mathbf{T}^r$ with a recovery rate $1/\tau$. Formally, R_τ^{ar} is computed as follows:

$$R_\tau^{ar}(\mathcal{G}, \mathbf{T}^a, \mathbf{T}^r) = \frac{1}{n}\Big[\sum_{t=1}^{\lfloor n/(1+\tau)\rfloor} \sum_{p=(t-1)\cdot(1+\tau)+1}^{t\cdot(1+\tau)-1} P_{a,c}^\infty(p) \\ + \sum_{p=\lfloor n/(1+\tau)\rfloor\cdot(1+\tau)+1}^{n} P_{a,c}^\infty(p) + \sum_{t=1,p=t\cdot(1+\tau)}^{t=\lfloor n/(1+\tau)\rfloor} P_{r,c}^\infty(p)\Big], \tag{24}$$

where $P_{a,c}^\infty(p)$ and $P_{r,c}^\infty(p)$ are the final fractions of the community-aware LCC when the p-th operation is an attack and a recovery, respectively, while the operator $\lfloor n/(1+\tau)\rfloor$ is the floor of $n/(1+\tau)$. In (24), $1/n$ is a normalization factor, which enables fair comparison of the robustness of networks with different scales. Generally, the R^{ar} value is in the range of $[0, 1]$, and networks with a higher R^{ar} are more robust to the failures during the mixing of attacks and recoveries.

In our system model, a damaged node is randomly recovered at each recovery, while an undamaged node (a functional node or a fail node) is randomly attacked at each attack. In this case, for each $p = t \cdot (1+\tau)$, $t = 1, 2, \ldots, \lfloor n/(1+\tau)\rfloor$, $P_{r,c}^\infty(p)$ at the $t \cdot (1+\tau)$-th recovery is equal to $P_{a,c}^\infty(p-2)$ of the $(t \cdot (1+\tau)-2)$-th attack. Therefore, R_τ^{ar} can also be evaluated as follows:

$$R_\tau^{ar}(\mathcal{G}, \mathbf{T}^a, \mathbf{T}^r) = \frac{1}{n}\Big[\sum_{t=1}^{\lfloor n/(1+\tau)\rfloor} \sum_{p=(t-1)\cdot(1+\tau)+1}^{t\cdot(1+\tau)-1} P_{a,c}^\infty(p) \\ + \sum_{p=\lfloor n/(1+\tau)\rfloor\cdot(1+\tau)+1}^{n} P_{a,c}^\infty(p) + \sum_{t=1,p=t\cdot(1+\tau)}^{t=\lfloor n/(1+\tau)\rfloor} P_{a,c}^\infty(p-2)\Big]. \tag{25}$$

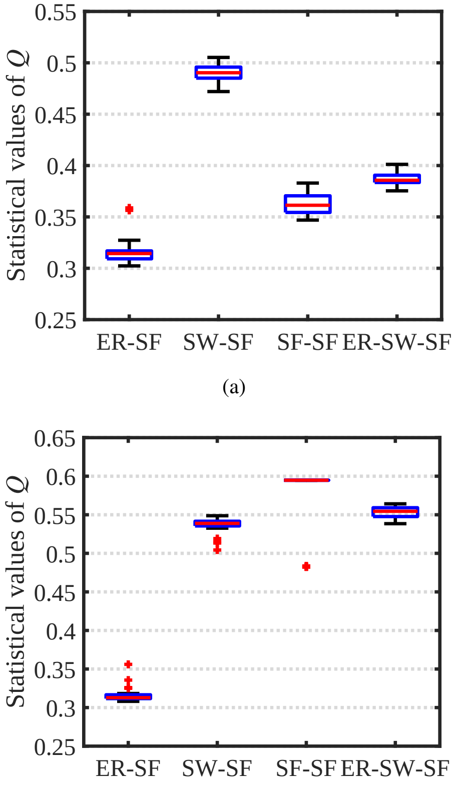
Here, $P_{a,c}^\infty(p)$ is the same as P_c^∞ in (1) under a fraction p/n of damaged nodes, and it can be computed by the aforementioned theoretical analyses.

To analyze the impacts of the recovery rate $1/\tau$ on the attack and recovery robustness analyses, Fig. 5 gives the variations of R_τ^{ar} with $1/\tau$ on the ER-ER networks with $n = 500$ and $\bar{k} = 6$ under both NCFs and NCCFs. The results show that the simulated results approximate the theoretical results well and the ER-ER networks are more vulnerable to NCCFs than to NCFs. Moreover, the R_τ^{ar} values decrease as the $1/\tau$ value increases. 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. DETAILS OF EXPERIMENTAL SETTINGS

A. Statistics of tested synthetic multiplex networks

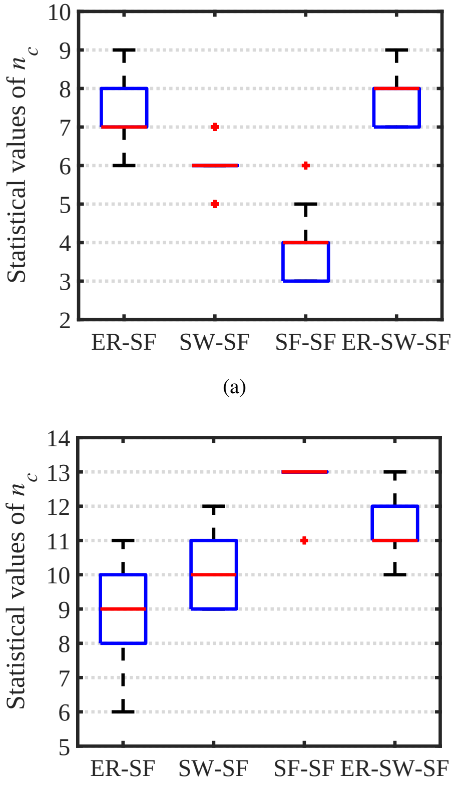
In this part, the statistics of communities for the tested synthetic networks such as average modularity and average number of communities are given (see Figs. 6 and 7).



(a)

(b)

Fig. 6: Box plot of the statistic Q of all tested networks with different scales (n). (a) $n = 200$ and (b) $n = 500$. The box plots are adopted to show the distribution of statistic Q values of all tested synthetic networks. On each box, the red line denotes the median while the symbol '+' represents the outlier.



(a)

(b)

Fig. 7: Box plot of the statistic number of communities n_c of all tested networks with different scales (n). (a) $n = 200$ and (b) $n = 500$. The box plots are adopted to show the distribution of statistic n_c values of all tested synthetic networks. On each box, the red line denotes the median while the symbol '+' represents the outlier.

Multiplex modularity Q has been widely used to evaluate the quality of communities of multiplex networks. It evaluates the difference between the fraction of links falling into communities over layers and the expected fraction in an equivalent network with links placed at random. The Q value is in the range of [-1, 1]. When $Q = 0$, it indicates that links of the networks are randomly placed at random. When $Q > 0$, it indicates that the networks have certain community structures. When $Q > 0.3$, it indicates that the networks have clear community structures.

The results in Fig. 6 show that the tested multi-layered ER-SF, SF-SF, SW-SF and ER-SW-SF networks show certain community properties as their Q values are generally larger than 0.3. The results in Fig. 7 illustrate that the numbers of communities of these networks are in the range of [3, 13].

The results in Figs. 6 and 7 of this document and Table III in the manuscript 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.

B. Details of comparison Algorithms

In this part, the details of some comparison algorithms such as PA, Betweenness, Degree, PageRank, CI and GA are given.

PA [4]: The PA algorithm aims to decrease the degree of cascading failures in coupled networks by establishing 10% of autonomous nodes. Each of these autonomous nodes has a specific operation system, which avoids inter-layer failures between autonomous nodes [4].

Betweenness [5], [6]: The Betweenness algorithm tries to protect 5% of nodes based on their betweenness centrality. For a given node i, its betweenness $\mathbf{B}(i)$ evaluates the extent to which node i falls on the shortest paths between pairs of nodes in the network [5], and it is computed as follows:

$$\mathbf{B}(i) = \sum_{j \neq i \neq w} \frac{\sigma_{jw}(i)}{\sigma_{jw}},$$

where σ_{jw} ($\sigma_{jw}(i)$) represents the number of the shortest paths from node j to node w (which pass through i).

Degree [5], [6]: The Degree centrality $\mathbf{D}(i)$ of a node i measures the number of the nodes in the network linked with

i, and it is defined as follows:

$$\mathbf{D}(i) = \sum_{\alpha=1}^{q} \sum_{w \neq i} \mathrm{A}_{iw}^{[\alpha]},$$

$\mathrm{A}_{iw}^{[\alpha]} \in \{0, 1\}$ represents the link state between the nodes i and w in layer α of network $\mathcal{G}$. Specifically, if there is a link between i and w in layer α, $\mathrm{A}_{iw}^{[\alpha]} = 1$, and $\mathrm{A}_{iw}^{[\alpha]} = 0$ otherwise.

PageRank [7], [8]: The PageRank algorithm, which is the most famous ranking technique, is used by Google to rank the impacts of web pages. The PageRank centrality $\mathbf{P}^t(i)$ of a node i for a network at time t is computed as follows:

$$\mathbf{P}^t(i) = \frac{1-\xi}{n} + \xi \sum_{w} \frac{\mathrm{A}_{iw}\mathbf{P}^{t-1}(i)}{d_o(w)}.$$

where $1 - \xi$ is the transition probability for a random walker to jump to the next node, while $d_o(w)$ represents the output degree of w.

CI [9]: The CI algorithm aims to rank the nodes in a network according to their collective influence on belief propagation. For a node i, its collective influence $\mathbf{CI}_\varsigma(i)$ is computed as follows:

$$\mathbf{CI}_\varsigma(i) = (\mathbf{D}(i) - 1) \sum_{w \in \partial Ball(i,\varsigma)} (\mathbf{D}(w) - 1),$$

where $Ball(i, \varsigma)$ denotes the set of nodes in the ball of i with radius ς, while $\partial Ball(i, \varsigma)$ represents the frontier of the ball [9].

GA [10], [11]: The GA algorithm, which is simply an extended version of memetic algorithms [10], [11] without local search, aims to find the influential nodes by evaluating a population of individuals simultaneously. It first adopts a binary string $X = \{x_i \in \{0, 1\}\}_n$ to represent a possible solution, in which x_i denotes whether or not node i is an influential node. It then uses a two-way crossover, a random swapping mutation, and an elite update strategy to iteratively evolve the population until the maximum number of iterations is reached. Finally, the solution with the highest network robustness is chosen to determine the influential nodes.

REFERENCES

[1] L. Feng, C. P. Monterola, and Y. Hu, "The simplified self-consistent probabilities method for percolation and its application to interdependent networks," *New Journal of Physics*, vol. 17, no. 6, p. 063025, 2015.

[2] M. E. Newman, "Spread of epidemic disease on networks," *Physical review E*, vol. 66, no. 1, p. 016128, 2002.

[3] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *Physical Review E*, vol. 97, no. 3, p. 032306, 2018.

[4] 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.

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

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

[7] 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.

[8] 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.

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

[10] 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, no. 2, pp. 121–133, 2014.

[11] 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.