Enhancing community integrity of networks against multilevel targeted attacks

Lijia Ma, Maoguo Gong,* Qing Cai, and Licheng Jiao

Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, Xidian University, Xi’an, Shaanxi Province 710071, China

(Received 6 May 2013; revised manuscript received 22 July 2013; published xxxx)

The community structure and the robustness are two important properties of networks for analyzing the functionality of complex systems. The community structure is crucial to understand the potential functionality of complex systems, while the robustness is indispensable to protect the functionality of complex systems from malicious attacks. When a network suffers from an unpredictable attack, its structural integrity would be damaged.

Earlier studies focused on the integrity of the node structure or the edge structure when a network suffers from a single-level malicious attack on the nodes or the edges. In this study, we model the attack on the network as a two-level targeted one. Then, we propose a community robustness index to evaluate the integrity of the community structure when the network suffers from the modeled attack. The proposed index plays an important role in analyzing the ability of the real systems to resist unpredictable failures. Finally, based on the proposed community robustness index, a greedy algorithm is devised to mitigate the network attack. Experiments on three real network systems show that with minor changes in links the community robustness of networks can be greatly improved. The results also demonstrate that the community structures in the optimized networks remain practically unchanged compared with the original ones.

DOI: 10.1103/PhysRevE.00.002800 PACS number(s): 89.75.Hc, 89.75.Fb, 87.23.Ge

I. INTRODUCTION

Many real systems can be well represented as complex networks composed of vertices and edges [1–3]. Vertices represent objects of real systems, and edges (or links) denote the interactions or relations among these objects [4]. Among the properties of complex networks, the community structure is an important one for reflecting and understanding the potential functionality of complex systems [5]. Moreover, the community structure is a very important issue to be considered for preventing most efficiently the spreading of epidemics [6]. Communities in networks are composed of a set of nodes that have more intracommunity links than intercommunity links [7,8]. Generally, the vertices that have similar properties are in the same community [9]. The community structures appear in numerous real network systems. For instance, communities in the airports’ networks are sets of airlines with more frequent air traffic.

In recent years, more and more researchers have been focused on the robustness of networks under random failures or malicious attacks [10–13]. The robustness of networks is of great importance to guarantee the security of network systems, such as the airports, transportation, the World Wide Web, power grids, resource distribution, and disease control networks. The structural integrity of networks would be damaged when unpredictable failures or attacks occur on them. This results in the loss of the functionalities of complex systems to some extent. For instance, in world airports networks, some airlines cannot work normally due to the terrible weather or the terrorist attacks. In power grids networks, the electricity cannot be transmitted due to the failures of generators.

The robustness of networks is usually measured by a criterion that considers the critical fraction of networks when they collapse completely [12]. This measure overlooks situations in which the networks suffer from a big damage but they are not completely collapsing [14]. Recently, Schneider et al. [14] proposed a measure, node robustness ($R_n$), to evaluate the robustness of networks under node attacks. When nodes are gradually damaged due to random failures or targeted attacks, a network may be split into several unconnected parts. The node robustness ($R_n$) considers the size of the largest connected component during all possible node attacks, namely $R_n = \frac{1}{N} \sum_{q=1}^{N} s(q)$, where $N$ is the number of nodes in the network and $s(q)$ is the integrity of nodes in the largest connected part after removing $q$ nodes [14]. The normalization factor $1/N$ makes it possible to make a comparison of the node robustness between networks with different sizes. Generally, the larger the value of $R_n$, the more robust the network is. Schneider et al. [14,15] and Wu et al. [16] proposed some greedy techniques to optimize $R_n$. In their studies, they found that (1) the node robustness of networks can be greatly improved by modifying small parts of links without changing the total links and the degree of each node; (2) the optimal network for node robustness shares a common onion structure in which high-degree nodes are hierarchically surrounded by rings of nodes with decreasing degree [14,15]. Zeng and Liu extended their works and proposed a measure, link robustness $R_l$, for network robustness under malicious attacks on the links [17]. Similarly, the link robustness of networks can also be greatly improved by changing small parts of links. Moreover, there were a few studies working on the catastrophic cascade of failures in interdependent networks [18–23]. In addition, Schneider et al. proposed a method that identifies the autonomous nodes based on their degrees and centrality to maximize the robustness of coupled networks [24]. The robustness of coupled networks can be largely enhanced by establishing a few autonomous nodes. Their researches are crucial to create robust networks against possible malicious attacks in practical applications.

*Electronic address: gong@ieee.org

1539-3755/2013/00(0)/002800(10) 002800-1 ©2013 American Physical Society
Note that the works in Refs. [14,16,17] only consider the integrity of the node structure or the edge structure when the network suffers from malicious attacks. None of them considers the integrity of the community structure. When a network suffers from significant attacks, its communities may be damaged at different degrees. Correspondingly, the potential functionalities of real systems are destroyed at different degrees. The functional integrity of networks is crucial to judge whether the systems can work normally when they suffer from unpredictable damages. Moreover, their works [14,16,17] are simply based on single-level targeted attacks on nodes or links. In reality, there exist more complicated attacks. In addition, under the original constraints, keeping the total links and the degree of each node invariant for link changes, the optimized networks for network robustness may have changed their original community structures.

In this study, we first model the malicious attack on the network as a two-level targeted one. The first level is a small-scale targeted node attack, and the second level is a large-scale targeted community attack. Second, we propose a community-robustness criterion \( R \), to measure the functional integrity of networks when they suffer from the modeled attacks. Third, to make the optimized networks for network robustness have the similar community structures with the original ones, we propose new constraints for link changes. Finally, we devise a greedy algorithm to improve the community robustness of networks by modifying small parts of links. Experiments on the electronic circuits [25], the USAir [26], and the road [27] networks demonstrate that both the node robustness and the community robustness of networks can be greatly improved even though a small number of links are changed. They also show that the improved networks under the new constraints still retain their original functionalities.

II. COMMUNITY ROBUSTNESS OF NETWORKS UNDER MULTILEVEL TARGETED ATTACKS

A. Model malicious attack on the network as a two-level targeted one

From the microscopic view, a network can be modeled as an undirected and unweighted graph \( G = (V, E) \) with \(|V| = N\) nodes and \(|E| = M\) edges. The microscopic connections among nodes can be represented as an adjacency matrix \( A \). If there is a connection between node \( v_i \) and \( v_j \), the entry \( A_{ij} \) is 1 and 0 otherwise. From the macroscopic view, a network can also be modeled as \( G = (S, E') \), where \( S = \{s_1, s_2, \ldots, s_k\} \) is the set of communities of networks, and \( E' \) is the set of connections between different communities. The macroscopic connections among communities can also be represented as an adjacency matrix \( w \). If there are connections between community \( s_i \) and \( s_j \), the entry \( w_{ij} \) is larger than or equal to 1 and otherwise 0.

A schematic illustration of the microscopic and macroscopic representations of a network is given in Fig. 1 with a toy network. The toy network \( G_1 \), which is the largest component of the Santa Fe Institute Network, consists of 118 nodes and 200 edges [1]. Nodes represent resident scientists coming from different fields at the Santa Fe Institute and their collaborators, and edges correspond to their collaborations in publishing at least one article during any part of calendar year 1999 or 2000. The toy network can be divided into 8 communities by the community detection algorithm BGLL [28]. As shown in Fig. 1, the toy network \( G_1 \) is composed of 118 nodes and 200 connections in microscopic view or 8 communities and 19 connections in macroscopic view.

It is possible for the nodes or the edges of networks to suffer from damages. There may be a situation in which a set of nodes that have similar properties are damaged at the same time. Namely, the communities of networks could also possibly suffer from damages. As shown in Fig. 1, the toy network will be divided into several unconnected parts when a few nodes, edges, or communities are removed. Moreover, the damages caused by removing communities are greater than the damages caused by removing nodes or edges.

The network property having dense interconnections makes the real system resilient against random failures but vulnerable to targeted attacks [14]. Therefore, the studies on the robustness of networks under targeted attacks are useful to the security of real systems. In this study, we model the attack on the network as a two-level targeted one. The first level is the small-scale targeted attack that occurs on nodes with the largest degrees. The second level is the large-scale targeted attack under which the most influential communities that have the maximal number of intercommunity links are removed gradually. We use a dynamic approach that recalculates the degrees of each node and the importance of each community during the attack. The dynamic way corresponds to a more harmful attack strategy [12].

In the real world, it is possible for attacks on nodes and communities to happen. According to whether they can occur simultaneously, the attack strategies can be classified into two categories. The first one is the weighted strategy that simulates the situation in which the attacks on nodes and communities cannot happen simultaneously. In this case, the small-scale attacks on nodes and the large-scale attacks on communities are possible to occur but not simultaneously. In the absence of prior knowledge about which attacks will
ENHANCING COMMUNITY INTEGRITY OF NETWORKS . . .

FIG. 2. (Color online) The weighted and the mixed attack strategies on the toy network $G_2$. (a) The weighted attack strategy. (b) The mixed attack strategy. Nodes with different shapes are in different communities. The red dash circles represent an attack.

... happen, it is necessary to consider the community robustness of networks under targeted attacks at both levels. By introducing a weighting parameter $\alpha$, the community robustness of networks under both the small-scale and the large-scale attacks are considered. In the weighted strategy, the nodes with the largest degrees will be gradually removed when the network suffers from the small-scale attacks and the most important communities will be gradually cut when the network suffers from the large-scale attacks. The second one is the mixed strategy that simulates the situation in which the attacks on nodes and communities can happen simultaneously. In the mixed strategy, the nodes with the largest degrees will be removed with probability $f$ and the most important communities will be cut with probability $1 - f$. The procedure ends when the largest connected component reaches 1 (in this case, the remaining network consists of a set of isolated nodes). In this study, we mainly focus on the weighted strategy because it is more general in the real world. We also take into account the mixed strategy when considering the community robustness of a network.

A schematic illustration about the weighted and the mixed attack strategies on a toy network $G_2$ is shown in Fig. 2. The toy network, which has 12 nodes and 15 links, is divided into 3 communities (plotted with different shapes). Assuming the network suffers from attacks three times, for the weighted strategy, the attacks are either the small-scale attacks on nodes or the large-scale attacks on communities. For the mixed strategy, the attacks on nodes and communities can happen simultaneously, e.g., attacks on nodes two times and the other one on communities, shown in Fig. 2(b).

B. Community robustness of networks

The measures in Refs. [14,17] for the robustness of networks consider the integrality of the node structure or the edge structure. However, these measures can hardly reflect the functional integrity of the network. We thus propose a measure, the community robustness $R_c$, to evaluate the community integrity of networks under malicious attacks.

The community robustness of a network is defined as

$$R_c = \frac{1}{m} \sum_{q=1}^{m} \left[ \frac{k}{k} \sum_{p=1}^{k} \frac{S_{pq}}{S_p} \right],$$

where $m$ is the number of the possible malicious attacks on the network, $k$ is the number of communities, $S_p$ is the number of nodes in the community $p$, and $S_{pq}$ is the number of the remaining nodes in the community $p$ when the $q$th attack happens. The normalization factors, $1/m$ and $1/k$, make it possible to make a comparison of the community robustness between networks with different sizes and different numbers of communities. A larger value of $R_c$ usually indicates more robust community structure of the network.

For the weighted attack strategy, the community robustness of networks under the small-scale node attacks and the large-scale community attacks is necessary to be considered, respectively. The community robustness of a network under the small-scale targeted attack can be written as

$$R_{\alpha} = \frac{1}{N} \sum_{q=1}^{N} \left[ \frac{k}{k} \sum_{p=1}^{k} \frac{S_{pq}}{S_p} \right],$$

where $N$ is the number of the nodes in the network and $S_{pq}$ is the number of the remaining nodes in the community $p$ when $q$ nodes are removed. $S_1(q) = \frac{1}{k} \sum_{p=1}^{k} \frac{S_{pq}}{S_p}$ is the community integrality of the network after removing $q$ nodes. When each community of the network has the same size, $R_{\alpha}$ would be equal to $R_c$.

The community robustness of a network under the large-scale targeted attack can be written as

$$R_{\alpha} = \frac{1}{k} \sum_{u=1}^{k} S_2(u),$$

where $S_2(u)$ is the community integrality of the network after removing $u$ communities. As shown in Fig. 1(b), $R_{\alpha}$ measures the node integrality of the new generated network whose nodes are the communities of its original network and edges are the connections among these communities.

In practical applications, it is necessary to consider the malicious attacks at both levels because they are possible to happen but we cannot know which attack will occur in advance. Accordingly, the community robustness of a network under the weighted attack is modeled as

$$R_\alpha = \alpha R_{\alpha} + (1 - \alpha) R_{\alpha},$$

where $\alpha$, $0 \leq \alpha \leq 1$, is a weighting coefficient. When $0.5 < \alpha \leq 1$, the measure mainly focuses on the community robustness of a network under the small-scale targeted node attack. When $0 < \alpha < 0.5$, the measure mainly considers the community robustness of a network under the large-scale targeted community attack.

For the mixed attack strategy, the community robustness of a network can be defined as follows:

$$R_m = \frac{L}{L} \sum_{q=1}^{L} \left[ \frac{k}{k} \sum_{p=1}^{k} \frac{S_{pq}}{S_p} \right],$$

where $L$ is the total number of steps to reduce the size of the giant component to 1 [17]. $R_m$ evaluates the community robustness of a network when the network suffers from the small-scale and the large-scale attacks simultaneously. The probability with which the attack at each level occurs is controlled by a mixing parameter $f (0 \leq f \leq 1)$. When $f = 0$, it means that the network is more likely to suffer from the
large-scale attack. When $f = 1$, it indicates that the network is more likely to suffer from the small-scale attack.

C. Constraints for improving networks

For a given network, there are many ways to enhance the robustness of networks. A simple way is to add links without any constraints [14]. However, in practical applications, it is difficult to achieve due to the extra cost to create a link. Moreover, changing the degree of a node is more expensive than changing edges. In order to avoid producing additional cost as far as possible, Schneider et al. [14] propose two constraints that keep the number of links and the degree of each node invariant for link changes.

Note that the above constraints are difficult to guarantee that the optimized networks for network robustness have the similar community structures with the original ones. Comparing the community structure in the optimized network for node robustness [in Fig. 3(a)] with that in the original one [in Fig. 1(a)], we are not easy to find the similarity between them. It means that the $R_n$-optimized network has changed the original community structure of the toy network $G_1$.

In order to identify that the optimized networks for network robustness and the original networks have the similar community structures, we add a constraint that keeps the number of intracommunity links of each community invariant for link changes. As shown in Figs. 1(a) and 3(b), under the new constraints the optimized network for node robustness has the similar community structure with the original one. The new constraints for link changes are much closer to practical applications.

D. Enhancing community robustness of networks

The framework to enhance the community robustness of networks under the above constraints is shown in Fig. 4. First, the network is divided into a set of communities, using any community detection algorithms. In this study, we choose the community detection algorithm BGLL [28]. The algorithm BGLL is effective and efficient for uncovering the community structures of networks. More importantly, in the absence of prior knowledge of the number of communities, it can automatically detect the “right” number of communities.

Then, we devise a greedy algorithm to optimize $R_c$ under the proposed constraints. It works as follows: Starting from an original network $G$, two edges $e_{ab}$ and $e_{cd}$ are randomly selected. Swap the connections of $e_{ab}$ and $e_{cd}$ to $e_{ad}$ and $e_{bc}$, if the swap satisfies the constraints for link changes, and set the resulting network as $G'$. Update $G$ with $G'$ at a certain probability, which is decided by the difference between $R_c$ and $R_c'$, where $R_c$ and $R_c'$ are the community robustness of $G$ and $G'$, respectively. As shown in Fig. 4, $G$ is updated with $G'$ at the probability $\exp\left(-\frac{R_c-R_c'}{T}\right)$, where $T$ is a parameter, which controls the convergence speed of the algorithm to an optimal solution. The algorithm is easier to converge to an optimal solution when the value of $T$ is small (here, we set it as $10^{-4}$). The above operations will not stop until no further improvement can be achieved for a given large number of consecutive swapping trials $t_{\text{max}}$ (here, we set it as $10^4$).

![FIG. 3. (Color online) The community structures of the optimized toy networks for node robustness under (a) the original constraints and (b) the new constraints for link changes. Nodes with different colors and shapes are in different communities. The optimized network under the original constraints for link changes has different community structure with the original one. Under the new constraints, the optimized network has the similar community structure with the original one.](image)

![FIG. 4. Framework to enhance community robustness of networks.](image)
ENHANCING COMMUNITY INTEGRITY OF NETWORKS...

PHYSICAL REVIEW E 00, 002800 (2013)

III. EXPERIMENTAL RESULTS

In this section, first, we introduce the evaluation metrics. This framework, for the toy network $G_1$, under the weighted attack, the improvement of the community robustness can reach 92.51%. Meanwhile, its node robustness is also increased by 94.15%. Under the mixed attack, the improvements of the community robustness and the node robustness can reach 162.3% and 8.04%, respectively.

A. Evaluation metrics

In this study, beside using $R_n$ and $R_c$ to evaluate the robustness of networks, the following criteria are also adopted to illustrate the difference between the optimized and the original networks.

Normalized mutual information. Normalized mutual information ($I$) [29] is to estimate the similarity between two network partitions. If the original and the optimized network partitions are $p_1$ and $p_2$, respectively, the normalized mutual

International E-road Network. It has 1177 nodes and 1417 edges (1469 edges for directed network). Nodes represent European cities and edges correspond to the road connections among them. All the networks considered here are undirected and unweighted. The results obtained by the algorithm [14] are also given for comparison.
The spectrum index. The spectrum index ($\lambda_1/\lambda_2$), namely the ratio of the largest and second-largest eigenvalue of the adjacency matrix of the network, is adopted to evaluate the robustness of networks [31]. The researches in Ref. [16,17] indicate that the spectrum index has a certain positive correlation with $R_n$. It is also found that the optimization of $R_n$ tends to generate an onion structure in which nodes with almost the same degree are connected [14–17]. In this study, we try to find the relation between $\lambda_1/\lambda_2$ and $R_c$.

The relative robustness improvement. The relative robustness improvement is computed as $R/R_0 - 1$, where $R$ and $R_0$ represent the robustness of the optimized and the original networks, respectively. When $R = R_0$, the criterion $R/R_0 - 1$ represents the improvement of the node robustness of networks. When $R < R_0$, the criterion $R/R_0 - 1$ represents the improvement of the community robustness of networks under the modeled attacks. We also study the improvement of the community robustness of networks under the small-scale and the large-scale attacks, respectively. The relation between $R/R_0 - 1$ and the parameter $\alpha$ is analyzed to choose a suitable value of $\alpha$ for practical applications.

Modularity. Modularity ($Q$), proposed by Girvan and Newman [8], is widely adopted to evaluate the quality of the partition dividing a network into communities. Let $k$ be the number of communities found, the modularity is defined as

$$Q = \sum_{i=1}^{k} \left[ \frac{l_{m}}{m} - \frac{K_{m}}{2m} \right]^2,$$

where $l_{m}$ is the total intracommunity links, and $K_{m}$ represents the total degree of the community $s_{j}$. High values of $Q$ correspond to subjectively good partitions.

The difference of intracommunity links. The difference of intracommunity links ($\Delta E_{i}$) is to estimate the difference of the number of intracommunity links between the original and the optimized networks. Assuming that the optimized network can be represented as an adjacency matrix $A$, the criterion $\Delta E_{i}$ is computed as:

$$\Delta E_{i} = \left( \sum_{j=1, j \neq i}^{k} (A'_{ij} - A_{ij}) \right)/2.$$

When $\Delta E_{i}$ is smaller than 0, it indicates that at least $|\Delta E_{i}|$ intracommunity links have been changed into intercommunity links in the optimized networks. When $\Delta E_{i}$ is larger than 0, it means that at least $\Delta E_{i}$ intercommunity links have been changed into intracommunity links. When $\Delta E_{i}$ is equal to 0, it indicates that the number of intracommunity links in the original and the optimized networks has not changed.

B. Experiment on real-world networks under the weighted attacks

In this section, we test our algorithm on three real-world networks, the electronic circuits, the USAir, and the road networks, to illustrate that the community robustness of networks can be largely enhanced when they suffer from the weighted attacks. The related results of the $R_{n}$-optimized and the $R_{c}$-optimized networks are recorded in Table I. The $R_{c}$-optimized networks are generated by optimizing $R_{c}$ under

![Graph showing the integrity of communities versus the number of removed vertices](image-url)

![Graph showing the difference of intracommunity links](image-url)
the original constraints for link changes. The $R_n$-optimized networks are generated by optimizing $R_n$ under the new constraints. As shown in Table I, optimizing $R_n$ can greatly improve the node robustness of networks. More specifically, $R_n$ is increased by 59.95% in the electronic circuit network.

In the USAir and the road networks, the improvements of $R_n$ can reach 43.85% and 28.83%, respectively. However, the $R_n$-optimized networks can hardly keep their original community structures. As shown in Table I, in the $R_n$-optimized networks, the average values of $\Delta E_r$ over 100 independent trials are $-33.83$, $-86.37$, and $-23.85$ for the electronic circuit, the USAir, and the road networks, respectively. This means that an average of 33.83, 86.37, and 23.85 intra-community links have been changed into inter-community links for the electronic circuit, the USAir, and the road networks, respectively. This would result in the change of community structures between the optimized and the original networks. The above opinion is confirmed by the criterion $I$. The similarities between the optimized and the original network partitions are only 58.45% and 59.37% for the electronic circuit and the USAir networks, respectively. Therefore, it is meaningless to make a comparison of the community robustness between the optimized and the original networks since the original community structures have changed.

In this study, one constraint keeping the total intra-community links of each community invariant is added. The related results of the $R_n$-optimized networks generated by optimizing $R_n$ under the new constraints are also recorded in Table I. The results in Table I clearly show that the $R_n$-optimized network partitions are more similar to the original ones. The similarities between the $R_n$-optimized and the original network partitions can reach 79.08%, 79.71%, and 98.96% for the electronic circuit, the USAir, and the road networks, respectively. Moreover, the improvement of node robustness can reach 45.68% for the electronic circuit network, 29.63% for the USAir network, and 14.96% for the road network. In addition, the changed links in the $R_n$-optimized networks are less than that in the $R_c$-optimized networks.

As we can see from Table I, under the new constraints, optimizing $R_n$ can largely enhance both the node robustness and community robustness of networks. Optimizing $R_n$ can largely enhance the node robustness of networks. However, optimizing $R_n$ can hardly improve the community robustness of networks. The values of $R_c$ in the $R_n$-optimized networks are only increased by 8.80% for the electronic circuit network, 1.60% for the USAir network, and 5.60% for the road network. The improvements of $R_c$ in the $R_n$-optimized networks can reach even 35.92% for the electronic circuit network, 19.09% for the USAir network, and 34.77% for the road network. In order to further illustrate the above opinions, the community integrity of the tested networks under attacks at each level is plotted in Figs. 5, 6, and 7. By analyzing and comparing the results in Figs. 5, 6, and 7, we note that the $R_n$-optimized networks are the most robust. It means that the community robustness of networks can be enhanced by optimizing $R_n$. Moreover, the results also illustrate that the $R_n$-optimized networks are more robust than the original ones under the small-scale node attacks. Under the large-scale community attacks, the $R_n$-optimized networks have the similar community integrity with the original ones. It indicates that optimizing $R_n$ can hardly improve the community robustness of networks under the large-scale community attacks.

The results in Table I show that the values of $R_n$ and $R_c$ in the $R_n$-optimized networks are larger and smaller than that in the $R_c$-optimized networks, respectively, which indicate that under the new constraints optimizing $R_n$ cannot guarantee the improvement of $R_c$ and vice versa.

The spectrum index $\lambda_1/\lambda_2$ has been used to evaluate the node robustness of networks [16,17,31]. The studies in Refs. [16,17] indicated that the spectrum index has a certain positive correlation with $R_n$. However, the results in Table I show that under the new constraints there is no obvious connection between $R_n$ and $\lambda_1/\lambda_2$. Without the added constraint, it is found that both the $R_n$ and $\lambda_1/\lambda_2$ values of the $R_n$-optimized networks are larger than that of the original ones. Moreover, we observe that the spectrum index $\lambda_1/\lambda_2$ has no obvious relation with $R_c$. Therefore, the spectrum index cannot represent the node and the community robustness of networks under the new constraints.

\begin{table}[h]
\centering
\caption{Results on different real-world networks: the node-robustness criterion $R_n$, the community-robustness index $R_c$, the normalized mutual information ($I$), the spectrum index $\lambda_1/\lambda_2$, the difference of intra-community links $\Delta E_c$, the ratio of removed links $E_r$, and the number of communities $k$. Results are averaged over 100 independent trials.}
\begin{tabular}{|l|c|c|c|c|c|c|c|}
\hline
Networks & Algorithms & $R_n$ & $R_c$ & $I$ & $\lambda_1/\lambda_2$ & $\Delta E_c$ & $E_r$ & $k$ \\
\hline
Electronic circuit & Original & 0.1261 & 0.2272 & 1 & 1.131 & 0 & 0 & 13 \\
& $R_n$-optimized & 0.2017 & 0.3034 & 0.5845 & 1.171 & -33.83 & 0.2431 & 15.71 \\
& $R_c$-optimized & 0.1837 & 0.2472 & 0.7908 & 1.130 & 0 & 0.2200 & 14.72 \\
& $R_c$-optimized & 0.1549 & 0.3088 & 0.7958 & 1.135 & 0 & 0.3201 & 14.60 \\
USAir & Original & 0.1090 & 0.2436 & 1 & 2.382 & 0 & 0 & 9 \\
& $R_n$-optimized & 0.1568 & 0.2942 & 0.5937 & 2.463 & -86.37 & 0.0557 & 8.570 \\
& $R_c$-optimized & 0.1413 & 0.2475 & 0.7971 & 2.390 & 0 & 0.0412 & 8.030 \\
& $R_c$-optimized & 0.1388 & 0.2901 & 0.7913 & 2.392 & 0 & 0.0640 & 7.870 \\
Road & Original & 0.0548 & 0.0768 & 1 & 1.023 & 0 & 0 & 206 \\
& $R_n$-optimized & 0.0706 & 0.0971 & 0.9550 & 1.024 & -23.85 & 0.0220 & 203.1 \\
& $R_c$-optimized & 0.0630 & 0.0811 & 0.9896 & 1.023 & 0 & 0.0211 & 205.5 \\
& $R_c$-optimized & 0.0597 & 0.1035 & 0.9672 & 1.020 & 0 & 0.0342 & 204.5 \\
\hline
\end{tabular}
\end{table}
In the following, the effects of the parameter $\alpha$ on the robustness of networks are analyzed. The relative robustness improvements of networks with different $\alpha$ are reported in Fig. 8. As we can see from Fig. 8, in the electronic circuit network, the improvement can at least reach 21% for $R_n$, 40% for $R_{c1}$, 30% for $R_{c2}$, and 35% for $R_c$ when $0.1 \leq \alpha \leq 0.6$. The largest improvement of $R_n$, $R_{c1}$, $R_{c2}$, and $R_c$ can reach 25% ($\alpha = 0.6$), 51% ($\alpha = 0.9$), 37% ($\alpha = 0.1$), and 50% ($\alpha = 1$), respectively. In the USAir network, the improvement can at least reach 24% for $R_n$, 35% for $R_{c1}$, 13% for $R_{c2}$, and 16% for $R_c$ when $0.1 \leq \alpha \leq 0.6$. The largest improvement of $R_n$, $R_{c1}$, $R_{c2}$, and $R_c$ can reach 32% ($\alpha = 0.2$), 40% ($\alpha = 0.2$), 16% ($\alpha = 0.1$), and 38% ($\alpha = 1$), respectively. In the road network, the improvement can at least reach 8% for $R_n$, 14% for $R_{c1}$, 36% for $R_{c2}$, and 30% for $R_c$ when $0.3 \leq \alpha \leq 0.6$. The largest improvement of $R_n$, $R_{c1}$, $R_{c2}$, and $R_c$ can reach 12% ($\alpha = 0.6$), 23% ($\alpha = 0.8$), 43% ($\alpha = 0.2$), and 41% ($\alpha = 0.0$), respectively. They indicate that when the network suffers from targeted attacks under various cases, both the node robustness and community robustness of the network can be improved by optimizing $R_c$.

The $Q$, $I$, and $\lambda_1/\lambda_2$ values of the $R_0$-optimized networks with different $\alpha$ are also reported in Fig. 9. The results in Fig. 9 show that the community structures obtained by optimizing $R_n$ are not sensitive to $\alpha$. Generally, the values of $Q$ are 0.653, 0.350, and 0.739; the values of $I$ are 0.800, 0.790, and 0.965; and the values of $\lambda_1/\lambda_2$ are 1.13, 2.39, and 1.02, for the electronic circuit, the USAir, and the road networks, respectively. As both the node robustness and the community robustness of networks can be greatly improved and the community structures in the optimized networks basically remain unchanged compared with the original ones when $\alpha = 0.4$, we set the parameter $\alpha$ as 0.4 in this study.

C. Experiment on real-world networks under the mixed attacks

In this section, we test our algorithm on two real-world networks, the electronic circuits network and the USAir network, to illustrate that the community robustness of networks can be largely enhanced when they suffer from the mixed attacks. The $R_m$ values of the tested networks under different $f$ are reported in Fig. 10. The results in Fig. 10 clearly show that optimizing $R_n$ can improve the community robustness of networks when $f$ is large. However, it can hardly improve the values of $R_m$ when $f$ is small. More specifically, the $R_m$ values of the $R_0$-optimized networks are similar to that of the original networks when $f$ is smaller than 0.8 and 0.9 for the electronic circuits and the USAir networks, respectively. These phenomena indicate that optimizing $R_n$ can enhance
ENHANCING COMMUNITY INTEGRITY OF NETWORKS . . .

PHYSICAL REVIEW E 80, 002800 (2013)

FIG. 10. (Color online) The $R_n$ values of the tested networks when $f$ changes from 0 to 1. We compare three types of networks: the original network, the $R_n$-optimized network and the $R_m$-optimized network. The experimental networks are (a) the Electronic Circuit network and (b) the USAir network. Results are averaged over 100 independent trials.

As many real systems are fragile under random failures or malicious attacks, the robustness of networks has received an enormous amount of attentions in the last few years. In this study, we propose a community robustness index to evaluate the integrity of the community structure when the network suffers from the modeled two-level targeted attacks. Moreover, we propose new constraints for link changes. The optimized networks under the new constraints have the similar community structures with the original ones. Finally, a greedy algorithm is devised to improve the community robustness of networks. Experiments on three real-world networks show that both the node robustness and the community robustness of networks under the modeled attacks can be greatly improved by optimizing $R_c$ ($R_m$). Optimizing $R_n$ can greatly improve the node robustness of networks under the small-scale node attacks. However, it can hardly enhance the community robustness of networks under the large-scale community attacks. The results also demonstrate that without the added constraint, the optimized networks for network robustness cannot keep their original community structures. Under the new constraints, the optimized networks can effectively retain their original community structures.

In the work of Schneider et al. [24], it is found that the robustness of a couple of interdependent networks can be enhanced by establishing a minimum number of autonomous nodes. Following this work, we can extend our work to design a pair of interdependent networks with high community robustness by establishing a set of autonomous nodes and communities. Therefore, our future work will aim at considering the community robustness in interdependent networks.

IV. CONCLUSION

ACKNOWLEDGMENTS

The authors thank the reviewers for their valuable comments and suggestions, which greatly improved the paper’s quality. This work was supported by the National Natural Science Foundation of China (Grant No. 61273317), the National Top Youth Talents Support Program of China, and the Fundamental Research Fund for the Central Universities (Grants No. K50510020001 and No. K5051202053).