SCIENTIFIC REPORTS

OPEN

Maximizing Network Resilience against Malicious Attacks

Wenguo Li[1,2], Yong Li[1], Yi Tan[1], Yijia Cao[1], Chun Chen[1], Ye Cai[3], Kwang Y. Lee[4] & Michael Pecht[5]

Received: 5 July 2018
Accepted: 7 January 2019
Published online: 19 February 2019

The threat of a malicious attack is one of the major security problems in complex networks. Resilience is the system-level self-adjusting ability of a complex network to retain its basic functionality and recover rapidly from major disruptions. Despite numerous heuristic enhancement methods, there is a research gap in maximizing network resilience: current heuristic methods are designed to immunize vital nodes or modify a network to a specific onion-like structure and cannot maximize resilience theoretically via network structure. Here we map complex networks onto a physical elastic system to introduce indices of network resilience, and propose a unified theoretical framework and general approach, which can address the optimal problem of network resilience by slightly modifying network structures (i.e., by adding a set of structural edges). We demonstrate the high efficiency of this approach on three realistic networks as well as two artificial random networks. Case studies show that the proposed approach can maximize the resilience of complex networks while maintaining their topological functionality. This approach helps to unveil hitherto hidden functions of some inconspicuous components, which in turn, can be used to guide the design of resilient systems, offer an effective and efficient approach for mitigating malicious attacks, and furnish self-healing to reconstruct failed infrastructure systems.

Maximizing network resilience is of great importance because it helps to mitigate the impact of perturbations or failures and suggests an emergency solution to repair the network[1–4]. Recently, considerable research effort has been devoted to enhancing network resilience against malicious attacks[5–25], including immunization strategies[5,6,10–16] and topological construction methods[17–25]. Most of the immunization strategies map the problem onto the identification of vital nodes, which, if immunized, would mitigate the diffusion of a large scale failure. However, the strategies cannot essentially improve network resilience from a topological structure, and it is impossible to find a universal index to quantify the importance of a node well in every situation[16].

The problem of maximizing network resilience with topological construction is to find an optimal set of edge swaps (or edge additions). The heuristic edge-swap (ES) methods[17–21] can enhance network resilience by modifying a network to a specific onion-like structure. However, the computations of these methods become prohibitively expensive, especially for the large scale networks; on the other hand, the networks optimized by the ES methods have a great change in topological structures (onion-like structures), which has an impact on the functionality of the original networks. In the heuristic edge-addition (EA) methods[22–25], for a given network, the new edges between the nodes with lowest degrees are added into the original network. The EA methods have a good performance on computational complexity; however, they possess few effect on resilience optimizations. Furthermore, both the ES and the EA methods cannot optimize network resilience globally. As a consequence, they cannot well maintain the topological functionality of a network and their performance on resilience improvement cannot be guaranteed.

Measurement of resilience is essential for addressing the resilience optimization problem, yet there are no universally accepted indices of network resilience. Conventionally, the resilience (or robustness) of networks is measured by critical (percolation) threshold[2–6] which is equivalent to the maximum external force in physical elastic systems. Hence, the measurement cannot fully characterize the elastic properties of nonlinear networks (see also Fig. S1). Ref.[17] defined a robustness measurement R, but without mathematical deductive inference and

[1]College of Electrical and Information Engineering, Hunan University, Changsha, 410082, China. [2]School of Information and Electronic Engineering, Hunan City University, Yiyang, 413000, China. [3]School of Electrical and Information Engineering, Changsha University of Science and Technology, Changsha, 410114, China. [4]Department of Electrical and Computer Engineering, Baylor University, Waco, Texas, 76798-7356, USA. [5]CALCE Electronics Products and Systems Center, University of Maryland, College Park, Maryland, 20742, USA. Wenguo Li, Yong Li and Yijia Cao contributed equally. Correspondence and requests for materials should be addressed to Y.L. (email: yongli@hnu.edu.cn) or Y.T. (email: yibirthday@126.com)

physical properties. Other defined resilience metrics[7,8] vary between extremes such as recoverability, adaptability and absorptivity[9]. Therefore, the problem of maximizing network resilience remains unsolved despite an abundance of heuristic methods[17–25]. More efforts are required for a general approach to maximize network resilience.

Here we address the problem of optimal resilience by finding an optimal (that is, minimal) set of structural edges. After introducing network resilience indices that can reflect the most essential resilience properties of network structure, we provide an optimal solution of the problem by means of a unified theoretical framework and the proposed indices. Further, we propose an algorithm of posteriorly adding (PA) edges to solve the resilience-optimization problem in artificial random networks and real networks[26–28]. Compared with competing approaches[17,23], our algorithm achieves better network resilience performance. The main contributions of this paper are as follows: (1) by mapping a complex network onto a physical elastic system, we introduce indices of network resilience, which can better characterize the elastic properties for nonlinear networks, compared with the conventional metrics; (2) based on the proposed indices, we present a unified theoretical framework and a PA algorithm, which can maximize network resilience with minimal costs (i.e., with an optimal (that is, minimal) set of structural edges), in contrast to the heuristic ES[17] and EA[23] methods.

Methods

Resilience indices. The resilience metrics of networks in this paper were formulated by mapping a complex network onto a physical elastic system and can be commonly used in complex networks. For a physical elastic system, resilience is defined as the capacity of a material to absorb energy during elastic deformation, which can be measured by elastic potential energy (elastic strain energy), i.e.,

$$E_p = \int_{\sigma=0}^{\sigma_c} -F\mathrm{d}\sigma \tag{1}$$

where F is external force (stress), σ is elastic deformation and σ_c is critical elastic deformation. For a linear physical elastic system, the external force (or elastic deformation) is also a resilience metric, and it has the identity with the elastic potential energy. The value of Ep of Equations (1) lies in the range $[0, \infty)$.

In analogy with the physical elastic system, the proposed network resilience refers to the network deformation under external force including initial attacks, disruptions or perturbations. Let the fraction of the removed nodes, q, represent external force; and let the fraction of failed nodes, $1-G(q)$, denote elastic deformation under external force, where $G(q)$ is the fraction of the largest (giant) connected component[3,12,29]. And support that the size and shape of a complex network can be restored during elastic deformation if the external force is withdrawn. The elastic potential energy of a complex network, E_p, can be given by (see also Fig. S1a, and detailed explication in Supplementary Information Section S1).

$$E_p = \int_{1-G(q)=0}^{1-G(q)=1} -q\mathrm{d}(1-G(q)) = \int_{G(q)=0}^{G(q)=1} q\mathrm{d}G(q) = \int_{q=0}^{q=1} G(q))\mathrm{d}q \tag{2}$$

where $q \in [0, 1]$, $G(q) \in [0, 1]$ and $1-G(q) \in [0, 1]$. If $q=0$ (the network is not attacked), $G(q)=1$ and $1-G(q)=0$; If $q > q_c$ (the network breaks down), $G(q)=0$ and $1-G(q)=1-G(q_c)=1$, where q_c is the critical external force (the critical threshold) and $G(q_c)$ is the critical giant connected component[29]. The value of E_p of Equations (2) E_p lies strictly in the range $[0, 0.5]$.

Considering that the network system is a nonlinear discrete-time system, the quadrature formula (2) can but be solved by numerical integration method, here we provide the numerical versions of Equation (2) by rectangular and trapezoid approximation methods respectively

$$E_p = \frac{1}{N}\sum_{q=\frac{1}{N}}^{1} G(q) \tag{3}$$

$$E_p = \frac{1}{N}\sum_{q_l=\frac{1}{N}}^{1} \frac{G(q_l) + G(q_{l-1})}{2} \tag{4}$$

where N is the total number of nodes in the network, $1/N$ is the normalized minimum-step integral size which corresponds to $\mathrm{d}q$ in the Equation (2), and q, q_l and q_{l-1} are the fractions of the removed nodes and $q_l - q_{l-1} = 1/N$. The value of E_p of Equations (3) and (4) E_p lies strictly in the range $[1/N, 0.5]$, where the two limits correspond to a star network and a fully connected graph respectively. This is because (1) a star network breaks down if a vital node is removed from it, and (2) if a fully connected graph is attacked maliciously (or randomly), its fraction of the largest (giant) connected component is equal to 1 minus the fraction of the attacked nodes, i.e., $G(q) = 1-q$. Though the error of numerical integration in Equation (4) is smaller than that in Equation (3) (see the detailed explication in Supplementary Information Section S1), we select the Equation (3) as numerical integration version of Equation (2) in the following simulations in Result Section, for comparing with the method in ref.[17]. Note that in ref.[17], the right side of Equation (3) is defined only as a robustness measure R without mathematical deductive inference and physical properties.

Beyond that, the complex networks have other resilient indices such as an elastic coefficient (also called the modulus of elasticity), the critical external force (critical threshold, q_c) and the elastic complementary energy (all of which are defined in Supplementary Information Section S1), the same as the physical elastic systems do. The traditional measurement for resilience of networks, critical threshold (q_c), can just reflect the critical external force, which is unsuitable for nonlinear systems. For a nonlinear network, the elastic potential (or complementary) energy can better characterize its elastic properties due to its advantages covering the elastic coefficient and critical threshold (see Fig. S1b, and detailed explication in Supplementary Information Section S1).

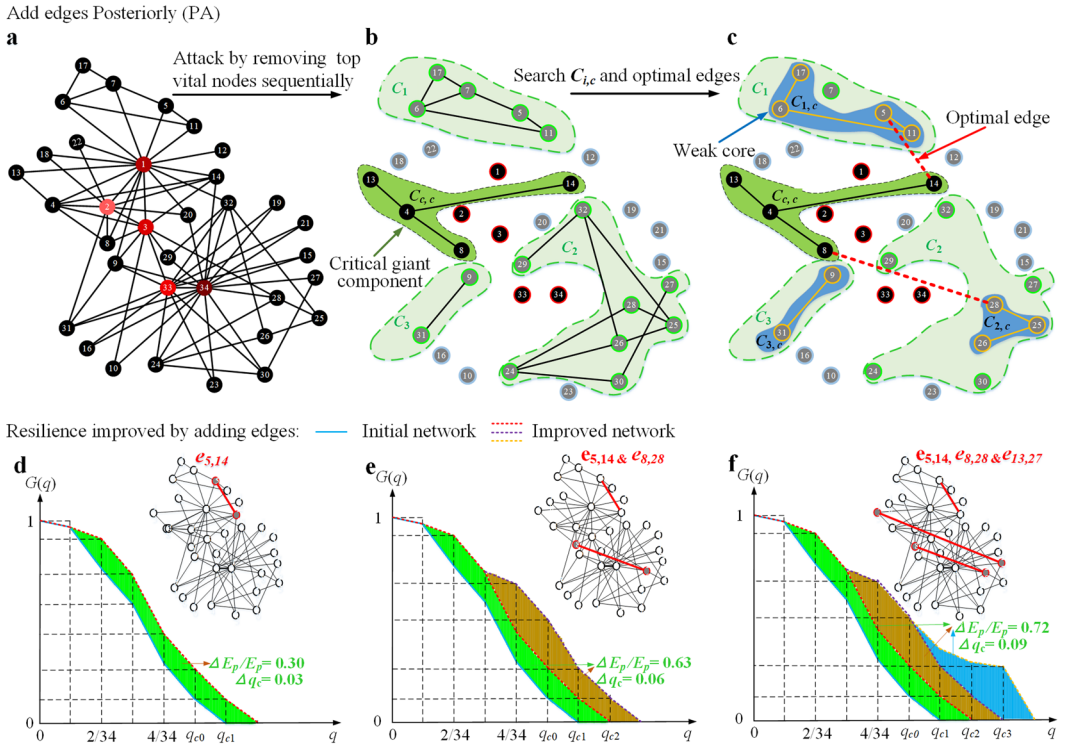

Figure 1. Optimal edges and weak cores: (**a**) an original network (Zachary network[26]). (**b**) The collapsed network including the isolated nodes, the finite components C_i and the critical giant component $C_{c,c}$, by sequentially removing top vital nodes (34, 1, 3, 33 and 2). The size and sequence of finite components (s_i, q_i) and the critical threshold (q_c) have been conserved in the process of malicious attacks. (**c**) The search of critical finite components ($C_{i,c}$, "weak cores") and optimal edges. The optimal set of edges including $e_{5,14}$, $e_{8,28}$ and $e_{13,27}$ is identified, where the optimal edges are adaptively connected between the least influencer in the critical finite component with the top latent resilience and the critical giant component. (**d**–**f**) The ratios of increments of resilience and critical threshold by adding one, two and three of the optimal edges $e_{5,14}$, $e_{8,28}$, $e_{13,27}$, respectively, where $\Delta q_c = q_{cI} - q_c$.

Theoretical framework. If a certain fraction (q) of vital nodes is intentionally removed from a network and the network breaks down into many finite (disconnected) components, i.e., $q = q_c$, the network will undergo a structural collapse and no giant connected component will exist, i.e., $G(q_c) = 0$. Let the vector $\boldsymbol{C} = (C_1, \ldots, C_k, \ldots, C_K)$ represent the finite components, whose normalized sizes are $s_1, \ldots, s_k, \ldots, s_K$ ($s_1 > \ldots > s_k > \ldots > s_K$), where k is the serial number of a finite component ordered by size, and K is the number of finite components in the collapsed network. Similar to the definition of the critical giant components, we define the "weak cores" (e.g., $C_{1,c}$, $C_{2,c}$ in Fig. 1) as the critical finite components. A critical finite component is a special critical giant component caused by an attack, as a finite component is regarded as a subnet. If an edge between the "weak cores" and the critical giant component ($C_{c,c}$ in Fig. 1) is added, the failure of the finite component can be avoided unless the critical giant component $G(p_c)$ fails. Therefore, the weak cores can be used for maximizing network resilience.

For simplicity, we investigated the case of adding only one optimal edge, e_{ij}, to maximize the network resilience (elastic potential energy); an optimal set of edges is provided in the follow-up section. There are only 4 ways to add this edge e_{ij}: (i) in the same finite component C_k ($i, j \in C_k$, $s_k > 2/N$), (ii) in the same critical giant component $C_{c,c}$ ($i, j \in C_{c,c}$), (iii) between two different finite components C_a, C_b ($i \in C_a$, $j \in C_b$, $s_a > s_b$), where s_a and s_b are the sizes of C_a and C_b, respectively, and (iv) between a finite component C_a ($i \in C_a$) and the critical giant component $C_{c,c}$ ($j \in C_{c,c}$). After adding an edge in any of the above 4 ways, from Equation (2), the increment of elastic potential energy of network can be given by

$$\Delta E_p = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]\mathrm{d}q \tag{5}$$

where $G_I(q)$ and $G_O(q)$ are the elastic potential energies of the modified network by adding the edge e_{ij} and the original network respectively, and $\Delta E_p \in [0, 0.5)$. Note that the least important nodes in the "weak cores" ($C_{i,c}$) and the critical giant components should be selected as the terminal nodes of edge e_{ij} to avoid being attacked maliciously in cases (iii) and (iv).

For cases (i) and (ii), due to $G_I(q) \approx G_O(q)$ and $q_a - q_1 = 1/N$ (where q_a and q_1 are the fractions of the removed nodes) (see Fig. 2a), the increment of elastic potential energy can be obtain from Equation (5) by

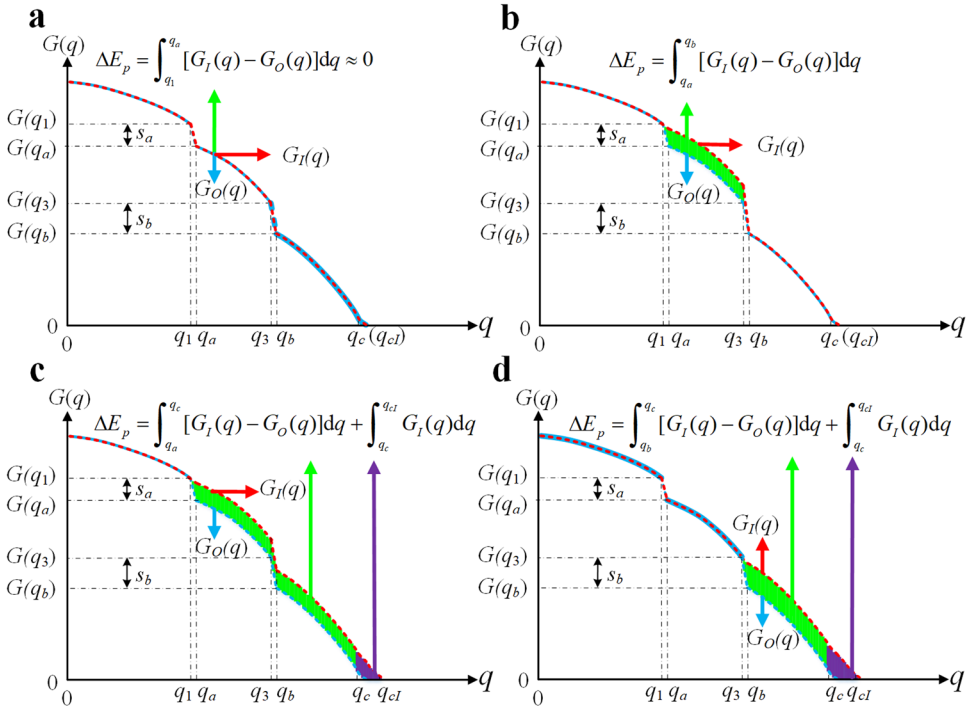

Figure 2. Comparisons of increments of elastic potential energy by adding edges in 4 possible ways. Here, $q_1 = q_a - 1/N$, $q_3 = q_b - 1/N$. (**a**) The increment of elastic potential energy by adding an edge between the two different nodes in the same finite component C_a (case (i)) (or in the critical giant component $C_{c,c}$ (case (ii))). (**b**) The increment of elastic potential energy by adding an edge between the two nodes from two different finite components (case (iii)). (**c**) The increment of elastic potential energy by adding an edge between the "weak core" $C_{a,c}$ (or $C_{b,c}$ in **d**) and the critical giant component $C_{c,c}$ (case (iv)).

$$\Delta E_p^{\mathrm{i,ii}} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]\mathrm{d}q = \int_{q_1}^{q_a} [G_I(q) - G_O(q)]\mathrm{d}q \approx 0 \tag{6}$$

Suppose that the two finite components C_a and C_b fail at q_a and q_b ($q_a < q_b$) respectively, where q_b is the fraction of the removed nodes, and $C_{a,c}$ and $C_{b,c}$ are the corresponding "weak cores" of C_a and C_b respectively. Accordingly, the increment of elastic potential energies in case (iii) and (iv) are respectively given by (see Fig. 2b,c)

$$\Delta E_p^{\mathrm{iii}} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]\mathrm{d}q = \int_{q_a}^{q_b} [G_I(q) - G_O(q)]\mathrm{d}q \tag{7}$$

$$\Delta E_p^{\mathrm{iv}} = \int_{q=0}^{q=1} [G_I(q) - G_O(q)]\mathrm{d}q = \int_{q_a}^{q_c} [G_I(q) - G_O(q)]\mathrm{d}q + \int_{q_c}^{q_{cI}} G_I(q) \tag{8}$$

where q_{cI} is the critical threshold of the modified network, $\Delta E_p^{\mathrm{iii}} \in [0, 0.5)$ and $\Delta E_p^{\mathrm{iv}} \in [0, 0.5)$. Comparing Equation (8) (case (iv), Fig. 2c) with Equation (7) (case (iii), Fig. 2b), one can see that the increment of elastic potential energy in case (iv) is greater than that in case (iii), due to $q_c > q_b$.

Algorithm. The above analysis shows that the optimal edge, e_{ij}, must be located between a "weak core" and the critical giant component (i.e., case (iv)) (strict theoretical proof in Supplementary Information Section S4). Moreover, from Equation (8), it can be observed that increment of the elastic potential energy in case (iv) depends on two key factors: the size and the failed sequence (such as q_a in Fig. 2c and q_b in Fig. 2d) of the finite component. Greater finite component size and smaller failed sequence result in greater increment of elastic potential energy, as shown in Fig. 2c,d.

By comparing the increment of the elastic potential energy from Equation (8) for every finite component, the sequence of the set of increments of the elastic potential energy $\Delta E = \{\Delta E_p^{1,c}, \ldots, \Delta E_p^{k,c}, \ldots, \Delta E_p^{K,c}\}$ can be given, where $\Delta E_p^{1,c} > \ldots > \Delta E_p^{k,c} > \ldots > \Delta E_p^{K,c}$. Accordingly, the sequential set of edges, $e = \{e_{i,j}^1, \ldots, e_{i,j}^k, \ldots, e_{i,j}^K\}$, can be obtained, here, $i \in C_k$ and $j \in C_{c,c}$ (or $C'_{c,c}$, the critical giant component of the modified network). Undoubtedly, the first element in the set of edges, $e_{i,j}^1$, is an optimal edge which, if added into the network, would improve the resilience of network maximally. The sequential set of optimal edges can be obtained naturally by repeating the above procedure. In this regard, a highly scalable algorithm, PA, is proposed for maximizing resilience. The algorithm is terminated if the number of added edges reaches a predefined limit, Fig. 3 shows the overall flowchart of the algorithm (more detailed depiction of the PA algorithm is shown in

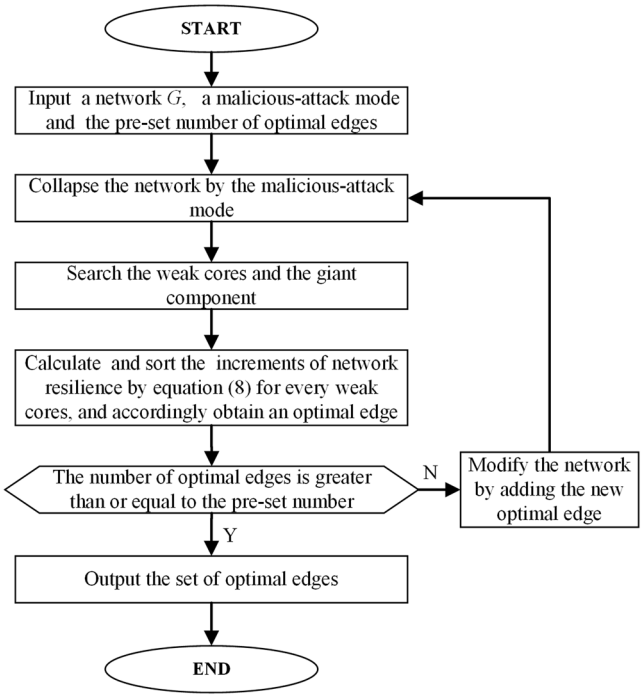

Figure 3. The overall flowchart of the proposed PA algorithm.

Supplementary Information section S5). Naturally, by adding the edges from the optimal set sequentially, the resilience of network can be enhanced maximally.

The resilience-improvement algorithm scales as $O(2\alpha K(M+N)\log(M+N))$, where M is the number of edges of the network, $\alpha(\alpha \ll N)$ is the number of pre-set optimal edges and $K(K \ll M)$ is the number of large finite components (more detailed explanation in Supplementary Information section S5). Generally, the number of large finite components K in a collapsed network is small, because the size distribution of the finite components follows the power law at the tail[29]. This high scalability allows us to find the edges to enhance the network resilience optimally in large-scale networks.

Results

Effectiveness. We demonstrate the efficiency of our approach on the Zachary (Karate club) network[26], the Gansu (GS)[27] and Henan (HN) power grids[28] as well as artificial random networks, i.e., scale-free (SF) networks and Erdös-Rényi (ER) networks. Figure 1d–f demonstrates the effectiveness of the proposed algorithm in maximizing the resilience of a simple network (Zachary network[26]) against malicious attack (high degree adaptive, HDA). The network resilience is increased by 30%, 63% and 72%, by adding one, two and three edges, respectively. Figure 4a–c shows the structures of SF, GS and HN network optimized by the proposed method (the structure of the optimized ER network in Fig. S2). For example, in Fig. 4c, before optimization, the finite components (green) C_1, C_2 will emerge if the vital nodes (such as high degree nodes (purple)) v_1, v_2 are maliciously removed from original network; after being optimized by adding optimal edges (red), the emergence of C_1, C_2 will be avoided naturally under the same attacks. This case explains why the proposed method can tremendously improve network resilience. As a practical example, the networked micro grids can enhance the power system resilience[5].

In Fig. 5a–c, we show the mitigation of malicious attacks for the SF network, GS and HN power grids (ER network in Fig. S3), respectively. The dashed lines correspond to the sizes of the giant component $G(p)$ in each original network, and the coloured solid lines correspond to the typical modified networks under the different numbers of added edges (from 20 to 180, 2 to 32 and 1 to 16 for SF, GS and HN, respectively). The coloured areas give increments of the resilience (elastic potential energy) under malicious attacks. By adding only 4.5% of edges to the SF network, GS and HN power grids under HDA attacks (Fig. 5d–f), the resilience of the three networks were increased by 44%, 187% and 740%, respectively.

We compare the proposed algorithm with the heuristic strategies, i.e., ES[17] and EA[23] in Fig. 5d–f. Remarkably, the heuristic strategies (ES and EA) improve the network resilience greatly. Furthermore, the improvement ratios of the network resilience by our algorithm are the optimal ratios and are greater than those of the heuristic strategies[17,23] under the same proportion of added (or swapped) edges. In the same three figures, we investigate the effect of the resilience improvement of our algorithm on two different malicious attacks, i.e., the widely used HDA[3] and the optimal collective influence (CI)[12] (see also Figs S4 and S5). Our algorithm performs very well under both attacks. The network resilience is improved by 36%, 223% and 762% (by adding or swapping 4.5% edges) in the SF network, GS and HN power grids, respectively, under the CI attack. Furthermore, if the critical threshold is used as the resilience measure, our algorithm also outperforms the other strategies[17,23] (Fig. 5g–i).

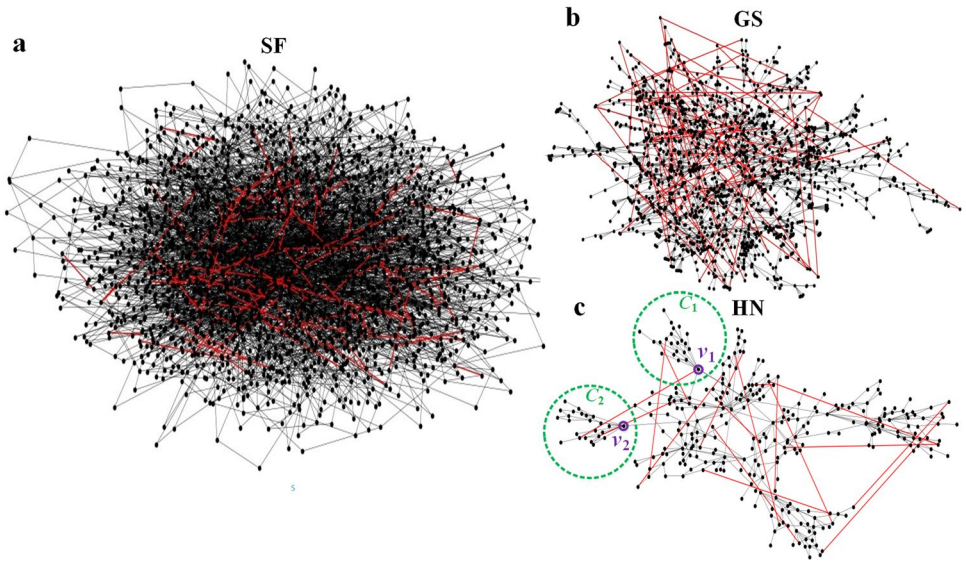

Figure 4. The optimized network structures. (**a**) The random SF network with $N = 2000$ nodes, $M = 4000$ edges, and power-law index $\gamma = 3$. (**b**) The GS power grid with $N = 1569$ nodes and $M = 2163$ edges. (**c**) The HN power grid with $N = 310$ nodes and $M = 466$ edges. In all cases, the test networks are modified by adding optimal edges (red), and the proportion of added edges to all edges of the original networks is 3.5%.

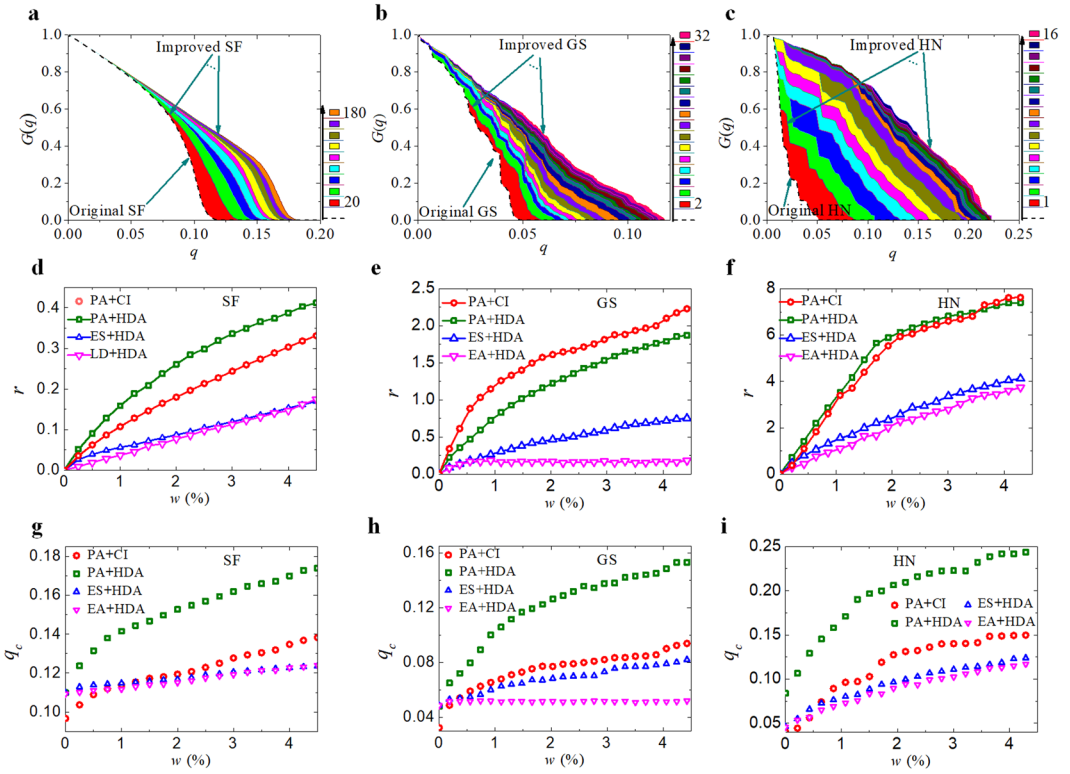

Figure 5. Mitigation against malicious attacks, improved resilience and critical threshold. (**a**–**c**) Mitigation against malicious attacks. The dashed lines correspond to the sizes of the giant components in each original network, the coloured solid lines to optimal modified networks under the different numbers of added edges and the coloured areas give the mitigation against malicious attacks (resilient increment). We compare the ratios ($r = \Delta E_p/E_p$) of increased resilience of our algorithm (PA) with other methods (ES, LD) under two modes of malicious attacks (HAD and CI) for each network in (**d**–**f**). The abscissa, w, indicates the proportion of added (or swapped in the ES method) edges to all edges of the original networks. Here CI represents CI_2 (other ratios of increased resilience and critical thresholds by CI_1, CI_2, CI_3 and CI_4 attacks are shown in Figs S4 and S5). The related comparisons of critical threshold increases for each network are shown in (**g**–**i**).

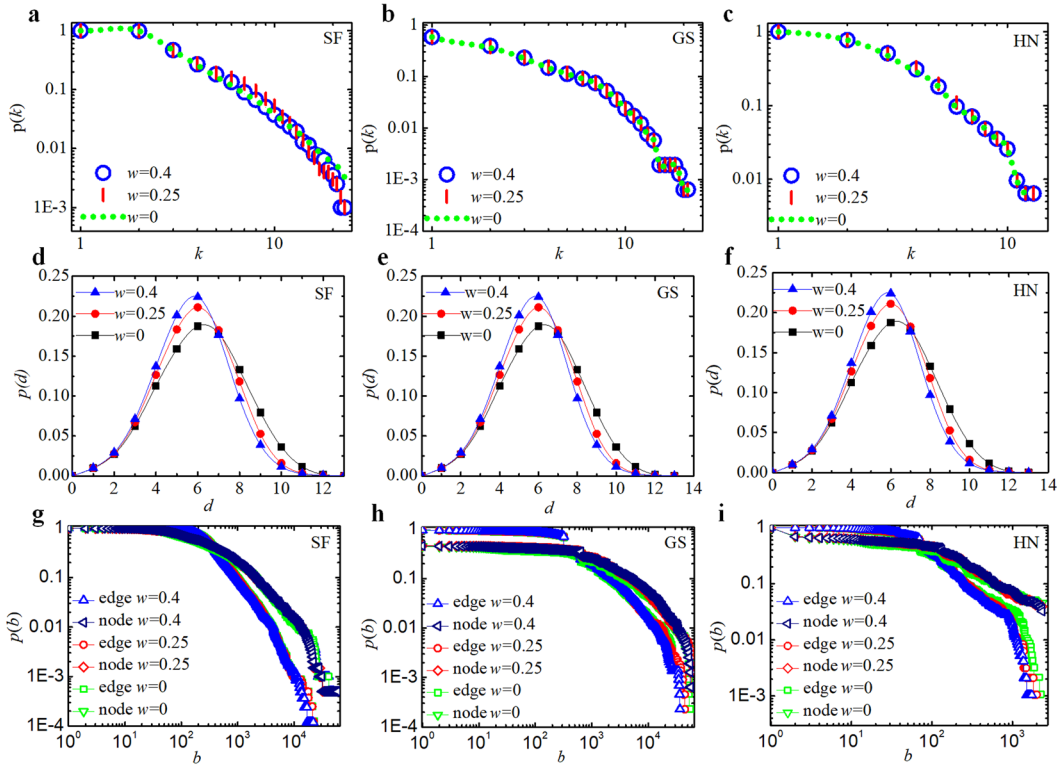

Figure 6. Unchanged network functionality. The network functionality is characterized by the network topological structure. The test networks with $w = 0.25$ and $w = 0.4$ were modified by our algorithm based on HDA attacks; the networks with $w = 0$ denote the original networks. (**a**–**c**) The cumulative degree distribution $p(k)$. (**d**–**f**) The cumulative shortest path distance distribution $p(d)$, where d is the shortest path distance between nodes. (**g**–**i**) The cumulative between-ness distribution $p(b)$, where b represents between-ness of node or edge.

For networks with a community structure[29] (such as the Zachary network, the GS and HN power grids), our algorithm produces a better network resilience and greater critical threshold than those complex networks with no community structure (such as SF and ER networks), as shown in Figs 5 and S3, because the networks lead to a few large finite components when they are attacked maliciously. In addition, better improvements of network resilience and critical percolation threshold can be obtained in the SF network (Fig. 5) than in the ER network (Fig. S3). As the top vital (hub) nodes of the SF network are removed sequentially, its serious heterogeneity will generate a few large finite components, which contributes to the consequences. Figure S6 shows that the network resilience and the critical thresholds of the original and the improved ER networks are increased, which indicates that they follow nearly the same rising trend in the original and the improved networks as the average degree. From Fig. S7, one can observe that the improvements in the network resilience and the critical threshold remain nearly unchanged regardless of the network size.

Unchanged network functionality. The functionality of a network is commonly related to its topological features[17,29]. It is fundamental and necessary to keep a network's functionality unchanged when optimizing its resilience. We tested the effects of the topological structural changes on the functionalities of the optimized networks, i.e., the SF network, and the GS and HN power grids. The distributions of cumulative degree, shortest path distance and betweenness were used for measuring the functionality. As shown in Fig. 6, those functionality measures hardly changed. Other topological characteristics including the cluster coefficient, the network diameter, *etc*., also remain unchanged (Table S2). Therefore, the networks optimized by our algorithm are not only more resilient against malicious attacks but also exhibit little change to their functionalities compared with the original networks.

Discussion and Conclusion

Intentional attacks and the corresponding defences are always the two opposite sides of network security. To enhance network resilience against malicious attacks, we introduce the network resilience indices by mapping a complex network onto a physical elastic system; then we propose a unified theoretical framework and a general approach (PA algorithm) to solve the problem of resilient optimization. As mentioned before, both the ES methods and EA methods cannot well maintain the topological functionality of a network and their performance on resilience improvement cannot be guaranteed since they are unable to optimize network resilience globally under a theoretical framework. In contrast, our algorithm can maximize network resilience by adding optimal edges between the "weak cores" and the critical giant component (Fig. 1), with minimal costs. This is because,

after being optimized by our method, the emergences of the large infinite components can effectively be avoided under the same attacks (Figs 1 and 4). Moreover, the proposed indices of network resilience can characterize the elastic properties for nonlinear networks, compared with the conventional metrics such as critical threshold. Case studies show that our algorithm achieves better performance on resilient improvement of networks, compared with competing approaches[17,23].

As edges are added to reach a certain proportion, the growth of network resilience slows down, especially for realistic networks, because the number of large-scale finite components generated by malicious attacks becomes increasingly smaller. Thus, it is necessary to balance the maximum resilience improvements with the costs of modifying a network to find an optimal compromise for the application of our method.

The proposed theory is strictly valid, and can be applied to any real network. Our solution to the optimal resilience problem demonstrates its importance because it can be used to enhance network resilience, guide the design of technological resilient systems, and offer fast and effective ways to mitigate the collapse of networks against malicious attacks, or furnish a self-healing solution to reconstruct existing failed infrastructure systems.

References

1. Barabási, A.-L. & Albert, R. Emergence of scaling in random networks. *Science* **286**, 509–512 (1999).
2. Nepusz, T. & Vicsek, T. Controlling edge dynamics in complex networks. *Nature Phys.* **8**, 568–573 (2012).
3. Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
4. Cohen, R., Erez, K., ben-Avraham, D. & Havlin, S. Breakdown of the Internet under intentional attack. *Phys. Rev. Lett.* **86**, 3682–3685 (2001).
5. Li, Z., Shahidehpour, M., Aminifar, F. & Alabdulwahab, A. Networked microgrids for enhancing the power system resilience. *Proceedings of IEEE* **105**, 1289–1310 (2017).
6. Cohen, R., Havlin, S. & ben-Avraham, D. Efficient immunization strategies for computer networks and populations. *Phys Rev Lett* **91**, 247901–247905 (2003).
7. Gao, J., Barzel, B. & Barabasi, A.-L. Universal resilience of patterns in complex networks. *Nature* **530**, 307–312 (2016).
8. Royce, F. & Behailu, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Safe.* **121**, 90–103 (2014).
9. Len, F. More than 70 ways to show resilience. *Nature* **518**, 35 (2015).
10. Zhao, J. *et al*. K-core-based attack to the internet: Is it more malicious than degree-based attack? *World Wide Web* **18**, 749–766 (2015).
11. Zdeborova, L., Zhang, P. & Zhou, H.-J. Fast and simple decycling and dismantling of networks. *Sci. Rep.* **6**, 37954 (2016).
12. Morone, F. & Makse, H. A. Influence maximization in complex networks through optimal percolation. *Nature* **524**, 65–68 (2015).
13. Kitsak, M. *et al*. Identification of influential spreaders in complex networks. *Nature Phys.* **6**, 888–893 (2010).
14. Liu, J.-G., Lin, J.-H., Guo, Q. & Zhou, T. Locating influential nodes via dynamics-sensitive centrality. *Sci. Rep.* **6**, 3 (2016).
15. Wang, J. W. Robustness of complex networks with the local protection strategy against cascading failures. *Safety Science* **53**, 219–225 (2013).
16. Lü, L. Vital nodes identification in complex networks. *Physics Report* **650**, 1–63 (2016).
17. Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S. & Herrmann, H. J. Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. USA* **108**, 3838–3841 (2011).
18. Wu, Z.-X. & Holme, P. Onion structure and network robustness. *Phys. Rev. E* **84**, 026106 (2011).
19. Zeng, A. & Liu, W. Enhancing network robustness against malicious attacks. *Phys. Rev. E* **85**, 066130 (2012).
20. Tanizawa, T., Havlin, S. & Stanley, H. E. Robustness of onionlike correlated networks against targeted attacks. *Phys. Rev. E* **85**, 046109 (2012).
21. Ma, L., Gong, M., Cai, Q. & Jiao, L. Enhancing community integrity of networks against multilevel targeted attacks. *Phys. Rev. E* **88**, 022810 (2013).
22. Paul, G., Tanizawa, T., Havlin, S. & Stanley, H. E. Optimization of robustness of complex networks. *Eur. Phy. J. B* **38**, 187–191 (2004).
23. Jiang, Z., Liang, M. & Guo, D. Enhancing network performance by edge addition. *Int. J. Mod. Phys. C* **22**, 1211 (2011).
24. Zhao, J. & Xu, K. Enhancing the robustness of scale-free networks. *J. Phy. A: Math. Theor.* **42**, 195003 (2009).
25. Louzada, V. H. P., Daolio, F., Herrmann, H. J. & Tomassini, M. Smart rewiring for network robustness. *Journal of Complex Networks* **1**, 150–159 (2013).
26. Zachary, W. W. An information flow model for conflict and fission in small groups. *J. Anthropol. Res.* **33**, 452–473 (1997).
27. Gansu Electric Power Dispatching Communication Center. Gansu Power Grid geographical wiring diagram 2011, http://wenku.baidu.com/view/29f77515e45c3b3567ec8bfd.html (Date of access: 10/05/2015) (2011).
28. Henan Electric Power Dispatching Communication Center. Henan Power Grid geographical wiring diagram, http://wenku.baidu.com/view/f1f0766c9b6648d7c1c7462d.html (Date of access: 10/05/2015) (2011).
29. Cohen, R. & Havlin, S. Complex networks: structure, stability and function. Cambridge University Press, Cambridge (2010).

Acknowledgements

This work was supported in part by the national Natural Science Foundation of China (NSFC) under Grants 51520105011 and 51822702, in part by the Key Research and Development Program of Hunan Province of China under Grant 2018GK2031, in part by the 111 project of China under Grant B17016, and in part by the Excellent Innovation Youth Program of Changsha of China under Grant KQ1707003.

Author Contributions

Prof. Y.L., Dr. W.L., Prof. Y.C. and Dr. Y.T. conceived the original ideas presented in this article. Dr. W.L. and Dr. Y.T. completed the model establishment and simulation. Dr. W.L., Dr. C.C., Dr. Y.C., Prof. Y.C., Prof. Y.L., Prof. K.Y.L. and Prof. M.P. wrote the main manuscript text and figures. Prof. Y.C., Prof. K.Y.L. and Prof. M.P. provided theoretical guidance. All authors reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at https://doi.org/10.1038/s41598-019-38781-7.

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.