communications physics

A Nature Portfolio journal

Article

https://doi.org/10.1038/s42005-025-02089-y

Graph coloring framework to mitigate cascading failure in complex networks

Check for updates

Karan Singh[1], V. K. Chandrasekar[2], Wei Zou[3], Jürgen Kurths[4,5] & D. V. Senthilkumar[1]

Cascading failures pose a significant threat to the stability and functionality of complex systems, making their mitigation a crucial area of research. While existing strategies aim to enhance network robustness, identifying an optimal set of critical nodes that mediates the cascade for protection remains a challenging task. Here, we present a robust and pragmatic framework that effectively mitigates the cascading failures by strategically identifying and securing critical nodes within the network. Our approach leverages a graph coloring technique to identify the critical nodes using the local network topology, and results in a minimal set of critical nodes to be protected yet maximally effective in mitigating the cascade thereby retaining a large fraction of the network intact. Our method outperforms existing mitigation strategies across diverse network configurations and failure scenarios. An extensive empirical validation using real-world networks highlights the practical utility of our framework, offering a promising tool for enhancing network robustness in complex systems.

Our day-to-day routines rely extensively on the performance of numerous natural and artificial networks, including neural and genetic regulatory networks, as well as communication networks, social networks, transportation networks, electric power grids, etc., to name a few[1–5]. However, most of these networks are susceptible to cascading failures, where the failure of a single node can lead to a domino effect, causing widespread breakdown and disruption of the entire network[6]. Devising mechanisms to enhance the resilience of such networks to random failures and targeted attacks is crucial for eradicating system failures with serious consequences[7]. Cascading phenomena impart either beneficial[8] or adverse effects[5,9,10] depending on the network's practical utility. Why do certain works, such as books, movies, and albums, gain widespread popularity despite limited marketing efforts[11], while similar endeavors fail to attract attention? Why do fluctuations occur in the stock market without any apparent significant news driving them[12]. How do grassroots social movements originate without centralized coordination or widespread public communication[13]. These features exemplify what economists refer to as information cascades[14], where individuals in a population exhibit herd-like behavior, basing their decisions on the actions of others.

Investigations have also explored how networks of adopters grow, particularly through social contagion processes[15–17] like adopting opinions, behaviors, emotions[18–21], or innovations, that can propagate quite rapidly[22] depending on their socioeconomical conditions. Social influence is significant in this scenario, with individuals being influenced by the viewpoints of their peers[4,18,19]. Such an effect has been represented by threshold models[6,23,24], which feature that an individual becomes an adopter when the proportion of its adopted neighbors reaches a critical level specific to their sensitivity. Such phenomena underscore the complexities of human behavior and decision-making processes[25], particularly in contexts where social influence plays a significant role.

One of the examples that underlie such a social contagion in the collapse of the top Online Social Networks (OSNs) is the Hungarian social networking site. The Hungarian social networking site iWiW[26] was operational from 2004 to 2013. In late 2010, there was a substantial increase in the number of users departing from iWiW, resulting in a significant loss and ultimately leading to the collapse of the entire network. The main reason for this downfall was later found to be that individuals left when most of their friends had already departed[27]. Understanding such a cascade effect is crucial in various applications such as marketing, advertising, spreading information, and so on. Identifying critical nodes to which the resources can be strategically allocated for an effective dissemination of the information across the network is the key. However, these processes can also have negative implications in areas like finance, healthcare, and infrastructure by causing undesired or detrimental outcomes for the community. Therefore, it is important to mitigate the cascading failure in complex networks to minimize the potential adverse consequences and to ensure the stability and resilience of such systems.

Various failure models have been extensively studied and applied to simulate failure propagation in networks across different contexts. Among

[1]School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Thiruvananthapuram, Kerala, India. [2]Department of Physics, Center for Nonlinear Science and Engineering, School of Electrical and Electronics Engineering, SASTRA Deemed University, Thanjavur, Tamil Nadu, India. [3]School of Mathematical Sciences, South China Normal University, Guangzhou, China. [4]Potsdam Institute for Climate Impact Research, Telegraphenberg Potsdam, Potsdam, Germany. [5]Institute of Physics, Humboldt University Berlin, Berlin, Germany. e-mail: skumar@iisertvm.ac.in

them, two prominent approaches commonly used to model failure dynamics in real-world networks are the k-core method[28–30] and the fractional threshold model[6,31–33]. The k-core method focuses on the structural resilience of networks by identifying subsets of nodes (or cores) that can sustain connectivity under cascading failures. On the other hand, the fractional threshold model examines node failures based on local thresholds—typically the proportion of failed neighbors required to trigger the failure of a given node—making it particularly suitable for understanding contagion processes and network diffusion dynamics. In the context of power grids, the load-capacity model serves as a pivotal framework for analyzing cascading failures in complex networks, where the failure of a single node can trigger a chain reaction affecting the entire system. This model effectively captures the balance between local resilience and global vulnerability by assigning each node a capacity proportional to its load, as demonstrated in critical infrastructures and communication networks[34,35]. This approach underscores the importance of load redistribution dynamics in mitigating large-scale disruptions. These diverse models and their underlying principles highlight the complex nature of failure propagation in networks.

In this work, we introduce a framework for mitigating cascading failures by leveraging the local environmental information of the vertices. Our methodology involves the identification of the minimal set of critical nodes from the pool of fragile nodes, which only needs to be protected to ensure near-complete network survivability from the cascades. To identify the critical set, we employ a graph coloring technique[36,37], that assigns a unique color to each node, ensuring that no two adjacent nodes share the same color, to determine the critical average degree, which is being employed as a threshold for refining the fragile nodes further. Our results demonstrate that the proposed framework is optimized in terms of both the fraction of fragile nodes and the probability of survival. That is, the refined subset of fragile nodes, the critical set, is the minimum number of nodes to be protected to retain the maximum survival probability. The effectiveness of our approach is first evaluated by employing theoretical models, namely Erdős-Rényi (ER)[38] and Scale-free networks[39], which emulate various real-world network structures. Subsequently, we assess its applicability in various practical scenarios by demonstrating its efficacy in real-world networks, namely, social networks, collaboration networks, and the US power-grid network. We show that the proposed framework not only adeptly mitigates cascading failures in basic theoretical models but also establishes robustness in intricate real-life networks. Our findings underscore the efficacy of the proposed framework in averting network collapse across diverse types of networks.

Results and discussion

Methods

A model of cascading failure. Different failure models have been extensively studied and applied in various contexts by simulating the propagation of failures. The k-core method[28–30] and the fractional threshold model[6,31–33] are the two common approaches that have been widely employed to represent failure propagation in real-life networks. In the k-core method, the threshold, which is used to identify the adopter, is determined by the absolute number of active neighbors, making it particularly applicable in epidemiological settings where an individual's actual number of contacts is crucial. On the other hand, when the fraction of active neighbors holds more significance than their absolute number, it becomes the fractional threshold model. This model finds application in various fields such as opinion formation[40], social dynamics[27], infrastructures[41], economics, finance[42], etc.

In the context of opinion formation, an individual adopts a certain behavior if a fraction m of its k immediate neighbors have already adopted it. In this case, the fractional threshold is "m/k" and not "m" as in the case of the k-core method. This results in individuals with a large number of their immediate neighbors becoming adopters to change their state. Such a process of cascading is illustrated schematically in Fig. 1. We initiate the cascade by impacting node-2 (gray node in Fig. 1a), which will be removed with all its links (dashed lines are the removed edges in Fig. 1b). This leads to a change in the degree and hence the fractional threshold (m/k) of the immediate neighbors of node-2, that is, nodes 3, 5, and 6 as shown in Fig. 1c. Now, if the fractional threshold of the latter nodes $m_i/k_i < \theta$, where m_i is the updated degree of the nodes 3, 5, and 6 after impacting node-2, k_i is their initial degree, and θ is the predefined fractional threshold, then these nodes will also fail. We consider a fractional threshold of $\theta = 0.84$ to elucidate the cascading process in Fig. 1. Now, the degrees of nodes 3, 5, and6 are updated to $m_3 = 4$, $m_5 = 4$, and $m_6 = 3$, respectively (see Fig. 1c). Their fractional thresholds are calculated as $\theta_3 = m_3/k_3 = 4/5 = 0.8 < \theta$, $\theta_5 = m_5/k_5 = 4/5 = 0.8 < \theta$, and $\theta_6 = m_6/k_6 = 3/4 = 0.75 < \theta$, leading to the failure of the nodes 3, 5, and 6, represented as gray nodes in Fig. 1c. These failures propagate further impacting nodes 7 and 4, which eventually fail due to $\theta_7 < \theta$ and $\theta_4 < \theta$ as discussed above (see Fig. 1d–f), exacerbating the cascading failure process. Ultimately, only the high-degree node (node-1) remains unaffected, surviving the cascade as shown in Fig. 1g.

Mitigation strategy. Now, our task is to identify the critical nodes that play a key role in propagating cascading effects instead of measuring a node's importance based on the damage it causes when removed. The node's importance in terms of the damage it causes will not be very useful from the mitigation perspective because, at a critical fractional threshold θ_c, even an exceedingly small impact[43] (as minor as removing a single node) could initiate a cascade effect leading to the network collapse. We now define fragile nodes as those nodes that fail when a single edge is removed, which leads to $m_i(=k_i-1)/k_i < \theta$ for all i.

In Fig. 2, we will delineate the procedure for identifying the critical nodes from the pool of fragile nodes. The first three steps are fundamental to identifying the fragile nodes. The last two steps are decisive in identifying the subset of nodes to be protected from a large pool of fragile nodes. In the results section, we will show that there is no need to protect all the fragile nodes; instead, protecting a fraction of the fragile nodes (which can be identified after the application of the last step) would ensure the full survivability of the network. We refer to this refined set of fragile nodes as the critical nodes, which only need to be protected.

A schematic representation of the colored groups (Step 5 in Fig. 2) is depicted in Fig. 3. Coloring the graph transforms it into a c-partite graph, here tripartite. Its vertices are partitioned into c different independent sets (we refer to them as colored groups), where c is the chromatic number of the graph, e.g., $c = 2$ is the bipartite graph. The lowest average degree among the color groups provides us $\langle k\rangle_c$. Now, the critical nodes are the nodes from the fragile nodes with degree greater than the critical degree, i.e., $k_i \geq \langle k\rangle_c$ for all $i \in$ fragile nodes.

A careful analysis of the set of critical nodes reveals that nodes with very high degrees are not in the critical set because they remain resilient even under very high thresholds. On the other hand, low-degree nodes become fragile relatively quickly, but they do not effectively transmit the shock and, therefore, are absent in the critical set. The most possible candidates for the critical set are the nodes with medium degrees, which are sufficiently weak to be fragile and well-connected enough to propagate the cascade significantly. Selecting this group of nodes for protection offers an effective mitigation strategy due to their minimal number.

It is essential to outline the graph coloring process mentioned in the algorithm (Step 4 in Fig. 2), which serves as a crucial step in our algorithm. Graph coloring is a most important concept in graph theory[44], renowned for its diverse applications, including scheduling problems[45,46], network security[47], register allocation in compilers[48], frequency assignment in wireless networks[49], map coloring[50], etc.

To color the graph, we have utilized the greedy coloring technique[36,37], also known as sequential coloring. It is a method of assigning color to the vertices of a graph using a greedy algorithm. This algorithm processes the vertices in a specified order, assigning each vertex the smallest available color that has not yet been assigned to its adjacent vertices. In particular, the colors are typically represented by integers (0, 1, 2, …), and each vertex is assigned the smallest integer that has not been used by its neighbor. Figure 4a illustrates the application of the greedy coloring algorithm. Here, we choose the descending order of the degree of the vertices. The process begins with

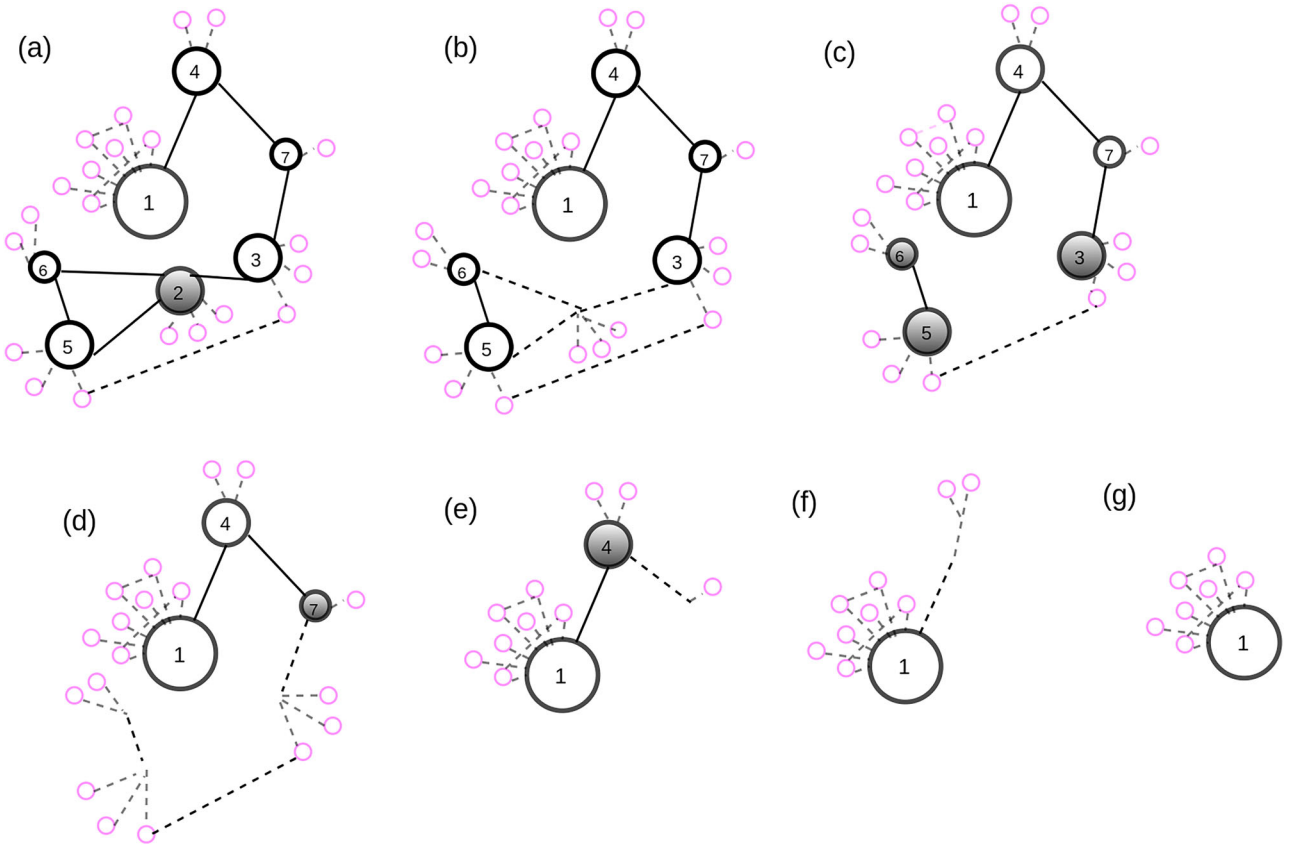

Fig. 1 | Schematic representation of the fractional failure mechanism. Node size corresponds to its degree with only the labeled nodes relevant to this description. The gradient (gray color) indicates the impacted node to be removed. **a** Node-2 is impacted to initiate the cascade, **b** impacted node's edges (represented as dashed lines) are disconnected and eliminated impacting nodes 3, 5 and 6 in (**c**), resulting in further impacted nodes in (**d**–**f**), exacerbating the cascading failure process, and ultimately leaving only the high-degree node-1 unaffected and surviving the failure in (**g**).

Fig. 2 | Proposed mitigation algorithm. Algorithm for identifying critical nodes based on local network topology and graph coloring.

Algorithm: Outputs Nodes to be Protected

1. Scan each node.
2. Check if it is fragile as per the condition defined under mitigation strategy.
3. If yes, check if it has at least two fragile neighbours.
4. Color the graph and calculate the average degree of each color subgroup.
5. Protect only those fragile nodes (fulfilling the 2nd and 3rd conditions) with degrees greater than the lowest average degree of the color group (critical degree).

coloring the highest-degree node (node-1) yellow. Node-4, being adjacent to node-1, cannot share the same color. Subsequently, the next highest degree node-2 is assigned the color yellow. Similarly, nodes 3 and 5 being adjacent to node-2, cannot be colored yellow, but leftover node-7 can be colored yellow. Once no additional nodes can be assigned the color yellow, the algorithm proceeds to the next color, which we have chosen it to be the red color, to continue coloring the graph, and this process repeats until all nodes are colored. The minimum number of colors required to color the entire graph provides the chromatic number c of the graph. Note that the small pink nodes are excluded from this coloring process to simplify the explanation.

The motivation for choosing graph coloring stems from the realization that coloring a graph divides it into c-partite (colored) groups based on the degree of the vertices. By setting the critical degree as the lowest average degree among these c-colored groups, we find that one can effectively include all the critical nodes from the fragile set, with the critical set being appreciably smaller than that of the fragile set. This is because any fragile node belonging to a color group other than the lowest average degree group (shown in green in Fig. 4) is likely to have a degree greater than the critical degree and ensured to be in the protected set.

A schematic representation of the mitigation procedure is represented in Fig. 4. We consider the same network as in Fig. 1, along with the same attributes for a better understanding.

The network is colored by applying the graph coloring technique (see Fig. 4a) to the periphery of the nodes. To simplify the explanation, small pink-colored nodes are excluded from the graph coloring. The average degrees of the color groups are determined as $\langle k \rangle_{yellow} = 5.67$, $\langle k \rangle_{red} = 4.67$, and $\langle k \rangle_{blue} = 4$. Since the blue color group has the lowest degree, its degree is referred to as the critical degree $\langle k \rangle_{blue} = \langle k \rangle_c = 4$. The fragile nodes (nodes 2, 3, 4, 5, 6, and 7) identified in Fig. 1 are represented using the dotted line to

the periphery of the color nodes (see Fig. 4b). Since nodes 2, 3, and 5 have degrees greater than $\langle k \rangle_c$, i.e., $\langle k \rangle_i > \langle k \rangle_c$ for $i = 2$, 3 and 5, these nodes are identified as the critical nodes (green shaded nodes in Fig. 4c). Upon initiating the cascade by impacting node-2, as shown in Fig. 1, only node-6 fails among its neighbors (nodes 3, 5, and 6). This is because nodes 3 and 5 belong to the protected critical set, effectively preventing widespread breakdown and disruption of the entire network.

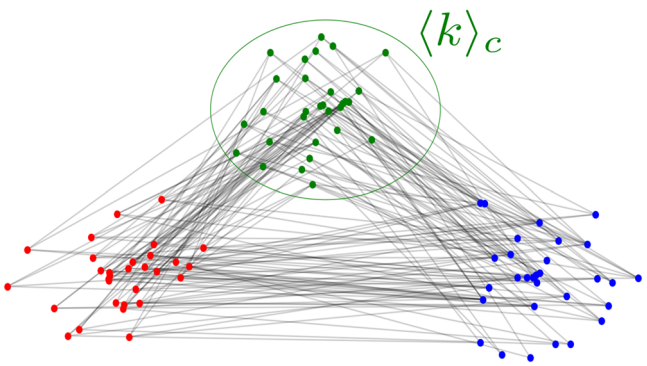

Fig. 3 | Determination of critical degree. A schematic representation of the graph coloring technique that facilitates the estimation of the critical degree (lowest average degree), $\langle k \rangle_c$, among the colored groups.

Paradigmatic network models. First, we apply the proposed mitigation strategy to the standard network models, namely Erdős-Rényi (ER) and Scale-free (SF) networks, to demonstrate its effectiveness in identifying the minimal set of critical nodes to be protected. The ER graph is generated by randomly connecting pairs of nodes to achieve a specified average degree. For this study, the ER graph consists of 20,000 nodes with an average degree of 8, corresponding to approximately 80,000 edges. This random graph generation technique ensures a uniform distribution of connections across the network. In contrast, the SF graph is created using a preferential attachment algorithm, which models network growth by preferentially attaching new nodes to the existing nodes with higher degrees. For this study, the SF graph consists of 20,000 nodes with an average degree of 6, capturing the power-law degree distribution characteristic of real-world networks.

The survival probability of the ER and the SF networks is depicted in the first and second rows of Fig. 5, respectively. The survival probability of the ER(SF) network is depicted as a function of the fractional threshold (θ) in Fig. 5a (Fig. 5c) for various degrees of protection probability. The stars connected by a blue line represent the network's survival probability for full protection probability, i.e., protecting the critical nodes with 100% probability. The dashed pink line corresponds to the fraction of protected nodes

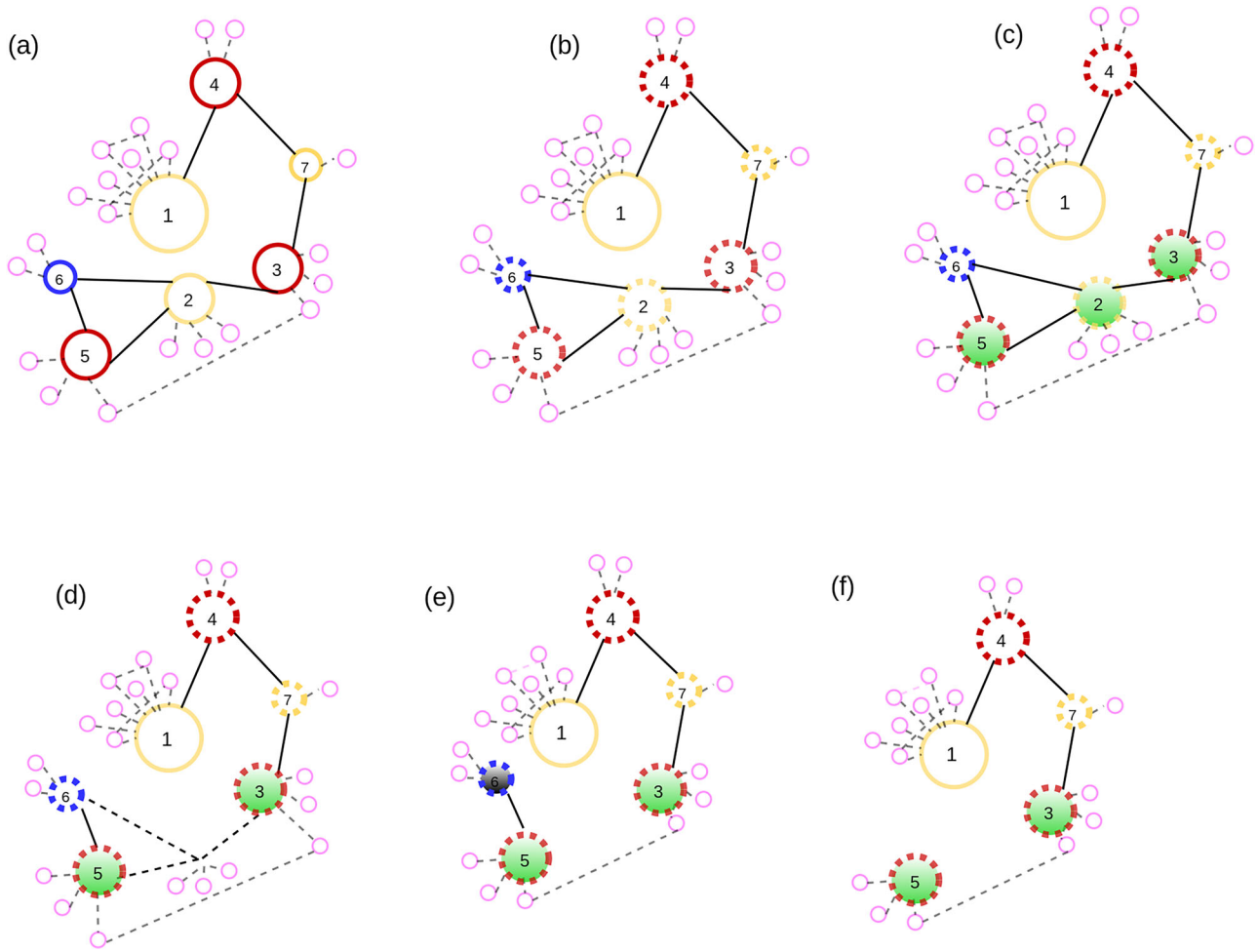

Fig. 4 | Schematic representation of the mitigation scheme using the same network as in Fig. 1 along with the same attributes. a Colored graph, **b** fragile nodes, identified in Fig. 1, are represented using the dotted line to the periphery of the nodes, **c** critical nodes are represented using green gradient, **d** the cascade is initiated by removing node 2 as in Fig. 1b, **e** node 2 along with its links is removed, impacting nodes 5, 6, and 3, as depicted in Fig. 1c. Nodes 5 and 3 are the critical nodes and are protected, whereas node 6 is removed following the same procedure as in Fig. 1d. **f** No further failures occur, as the neighbors of impacted node 2 are either in the protected set or their fractional threshold $\frac{m}{k} > \theta$, causing the cascade to stop with a large fraction of the network remains intact.

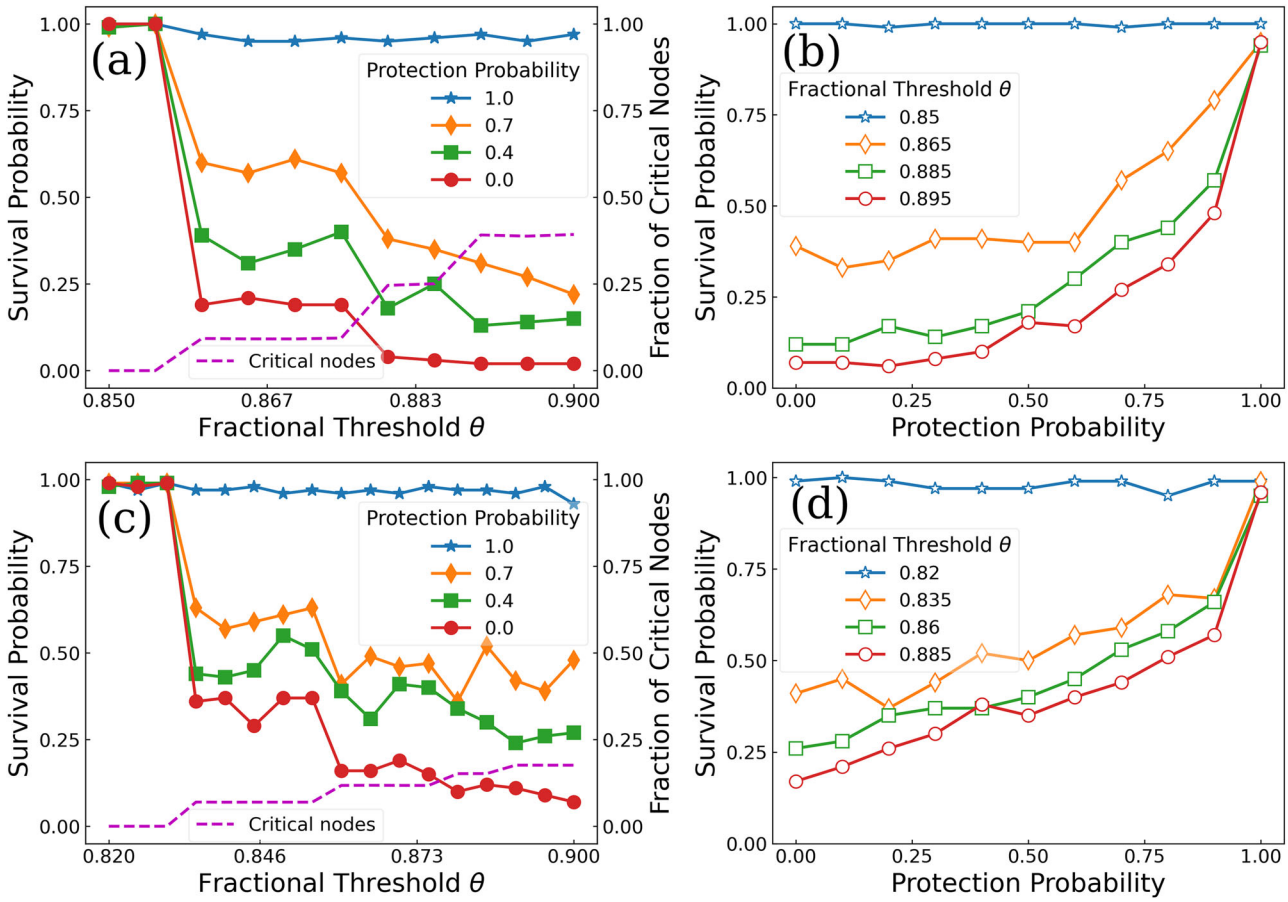

Fig. 5 | Application of the proposed mitigation framework of standard networks. Mitigation of cascading failure on the standard Erdős-Rényi (ER) (**a**, **b**) and Scale-free (SF) (**c**, **d**) networks. **a**, **c** Survival probabilities as a function of the predefined fractional threshold for distinct protection probabilities. **b**–**d** Survival probabilities as a function of protection probability for distinct predefined fractional thresholds. The pink dashed line corresponds to the fraction of critical nodes to be protected. We have fixed $N = 20{,}000$ and an average degree of $\langle k \rangle = 8$ for the ER network and $N = 20{,}000$, $\langle k \rangle = 6$ for the SF network. 150 realizations were performed for each network.

(critical set) of the network facilitating the maximal survival probability as a function of the fractional threshold θ. The lines connecting diamonds and squares correspond to the survival probability for 70% and 40% partial protection probabilities, respectively. Finally, the circles connected by the red line illustrate the network's surviving probability for the unprotected case. This is what we refer to as cascading failure (as we are not protecting any nodes).

The surviving probability is theoretically compared with the simulation results in the Supplementary Information in Fig. S1. The ER (SF) network always survives until the critical value of the predefined fractional threshold $\theta_c = 0.86$ (0.835), regardless of the degree of the protection probability. Near the critical threshold, the networks require a small fraction of critical nodes to be protected, as indicated by the pink dashed line, for the complete survival of the network (stars connected by the blue line) following the proposed mitigation strategy based on the graph coloring. In contrast, both ER and SF networks survival probability falls abruptly at θ_c and then continues its downfall more smoothly as the fractional threshold is increased for partial and zero protection probabilities. Note that the degree of the network's survival probability is larger for a larger fraction of the protection probability in the entire explored range of the fractional threshold θ. The theoretical estimate of the critical fractional threshold θ_c is depicted in a range of the average degree of the network in Fig. S2 of the Supplementary Information.

The survival probabilities of the ER and SF networks are depicted as a function of the protection probability in Fig. 5b, d, respectively, for four different predefined fractional thresholds. The unfilled stars connected by a blue line, correspond to the predefined fractional threshold $\theta = 0.85$ and $\theta = 0.82$, respectively, for ER and SF networks, elucidate the complete survival probability of both networks in the entire range of the protection probability, which is consistent with Fig. 5a, c. As the predefined fractional threshold θ increases, the survival probability decreases as indicated by lines connecting unfilled diamonds, unfilled squares, and unfilled circles for a given protection probability. Further, the survival probability increases with the protection probability for distinct predefined fractional thresholds and finally merges together for the full protection probability (see Fig. 5b, d). It also reveals that the network's complete survival probability is assured for any fractional threshold upon protecting the corresponding critical nodes with full protection probability. It is also to be noted that for a chosen partial protection (e.g., 0.7), 70% of the critical nodes are randomly selected from the pool of critical nodes. Further, the survival probabilities depicted in Fig. 4 are averaged over 150 realizations of the employed graphs. As a result, the specific subset of protected critical nodes varies across different realizations, leading to fluctuations in the increasing trend of the survival probability.

Now, to elucidate that the critical set identified by the proposed algorithm is the minimal number of fragile nodes to be protected from the pool of fragile set to ensure the maximum survival probability, we scale-up and scale-down the critical degree $\langle k \rangle_c$ and investigate the resulting survival probabilities as a function of the predefined fractional threshold as shown in Fig. 6a, b for the ER and the SF networks, respectively. The squares connected by the green solid line in Fig. 6 correspond to the network's survival probability for a fully protected critical set, obtained using the original critical degree $\langle k \rangle_c$, while the green dashed line represents the fraction of critical nodes for the given predefined fractional threshold. The diamonds

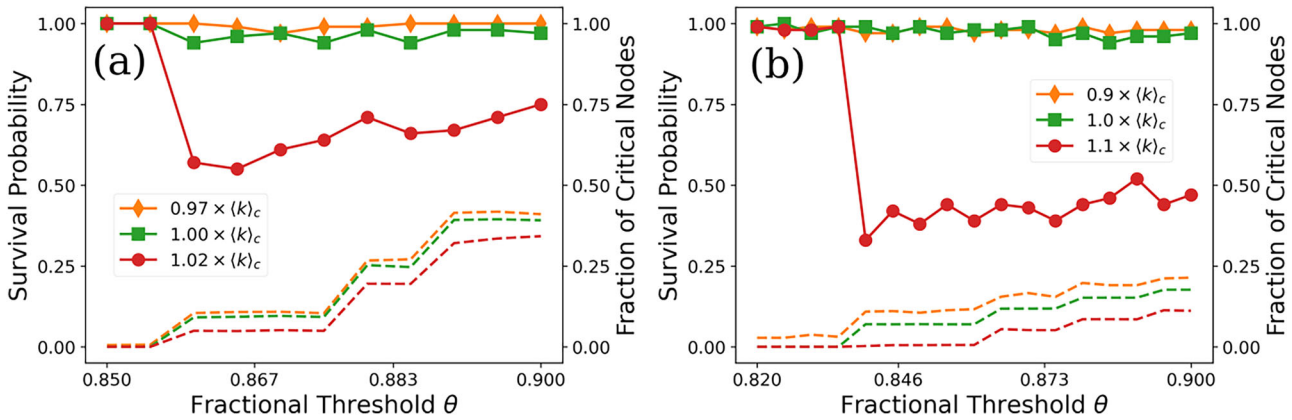

Fig. 6 | Scaling the critical degree. Survival probabilities as a function of the predefined fractional threshold for (**a**) Erdős-Rényi (ER) and **b** Scale-free (SF) networks are shown. The lines connecting squares, diamonds, and circles represent the full protection case, achieved by scaling down or scaling up the critical degree ($\langle k\rangle_c$). The corresponding critical nodes are indicated by dashed lines (same as in Fig. 5 on the right y-axis). The other parameters are the same as in Fig. 5.

and circles connected by the yellow and the red solid lines indicate the survival probabilities of ER (see Fig. 6(a)) and SF (see Fig. 6(b)) networks with the critical degree $\langle k\rangle_c$ scaled down to 97% and scaled up to 102% for ER and, scaled down to 90% and scaled up to 110% for SF. Evidently, the ER network is much more sensitive to the scaling of the critical degree $\langle k\rangle_c$ compared to the SF network. Note that lowering the critical degree allows the inclusion of more fragile nodes, as indicated by the dashed yellow line, in the critical set, resulting in improved survival probability. In contrast, increasing the critical degree leads to poor survivability, as shown by the line connecting red circles, due to the reduction in the number of fragile nodes in the critical set (see the dashed red line) compared to that of the critical nodes for $\langle k\rangle_c$. These results demonstrate that the proposed algorithm effectively identifies the minimal set of critical nodes to be protected from the fragile set by determining the least average critical degree $\langle k\rangle_c$ of the colored groups corresponding to the ER and the SF networks.

Comparison with the standard mitigation techniques. Figure 7 illustrates the effectiveness of the proposed framework over the standard intuitive (left column) and centrality based (right column) mitigation strategies widely employed in the literature. To begin with, we compare the proposed protection strategy for both ER (first row) and SF (second row) networks with simple intuitive strategies using the same size of the critical set, obtained for $\langle k\rangle_c$, for a fair comparison. We start by protecting the randomly selected nodes to illustrate that the proposed strategy is not just another random selection of fragile nodes. Pluses connected by the orange line correspond to the survival probability of the randomly selection nodes of the same size as that of the original critical set (see Fig. 7a, c). We have also chosen high-degree nodes (hubs), represented by hexagons connected by the green line in Fig. 7a, c), to further understand the role of hubs in SF networks under the discussed failure mechanism. In contrast to the intuitive understanding that protecting highly connected nodes leads to better network survivability, hubs do not turned out to be the potential candidates of the fragile set and consequently the critical nodes as shown under the Method Section. This is because the hubs remain robust until a very high threshold (θ) is reached under the removal of a single edge.

We have also considered the low-degree nodes (crosses connected by the red line) under the employed failure mechanism. However, removing low-degree nodes is very unlikely to propagate the cascade, as they are very likely to get isolated from the original network. It is evident from Fig. 7a, c that all three choices result in complete survival probability for $\theta < \theta_c$, similar to the survival probability for the original critical set obtained for $\langle k\rangle_c$ (stars connected by the blue line). Nevertheless, for $\theta = \theta_c$, the survival probabilities for all three choices drastically drop to ≈35% of the full survival probability and hover around it for $\theta > \theta_c$. In stark contrast, the survival probability specific to the original critical set remains near unity for $\theta > \theta_c$, elucidating the complete survival of both ER and SF networks throughout the entire explored range of the predefined fractional threshold.

Next, we compare our algorithm with standard centrality-based mitigation strategies, including closeness centrality[51] (triangles connected by the orange line), Katz centrality[52] (inverted triangles connected by the green line), and betweenness centrality[51] (pentagons connected by the red line). These comparisons are conducted for both ER (see Fig. 7b) and SF (see Fig. 7d) networks, ensuring the same number of critical nodes are protected in each case. Note that all three centrality-based strategies clearly underperform as their corresponding surviving probabilities drop abruptly to ≈25%(≈40%) of the full survival probability at $\theta = \theta_c$ for the ER (SF) network and hovers around it as a function of the predefined fractional threshold. Surprisingly, protecting the minimal critical set identified using the least average degree of the colored groups always facilitates the complete survival (stars connected by the blue line) of the networks (see Fig. 7b, d).

Next, we compare our mitigation algorithm with that proposed by Smolyak et al.[43], which served as a major inspiration for this work and provided an opportunity for an improvement. The primary distinction between our algorithm and that of Smolyak et al.[43] lies in the refinement/reduction step (i.e., steps 4–5). In their approach, they construct a connected subgraph of fragile nodes and protect only those fragile nodes whose degree exceeds the average degree of this subgraph. In contrast, our algorithm employs graph coloring to calculate the critical degree, defined as the lowest average degree among the colored groups (as described in the Mitigation Strategy section). We then protect only the fragile nodes whose degree exceeds this critical degree. Figure 8 compares the results of the proposed algorithm (blue stars connected by a solid line) with the Smolyak et al.[43] algorithm (yellow circles connected by a solid line).

In Fig. 8a, the survival probability for the ER network is plotted as a function of the predefined fractional threshold θ for the full protection case. Note that, as the fractional threshold increases beyond $\theta > 0.875$, the Smolyak et al.[43] algorithm struggles to maintain the full network survivability. This decline occurs because the reduction/refinement steps (steps 4–5) in their algorithm fail to incorporate enough fragile nodes into the protected (critical) set, which is critical for sustaining near-full survivability at higher fractional thresholds. To address this shortcoming, they resorted to manually lowering the critical degree, as detailed in the section on "Additional Model Parameters"[43]. This manual adjustment enabled them to include more fragile nodes in the protected set, ultimately restoring full survivability (as shown by the dashed blue line in Fig. 3[43]). In contrast, our graph coloring technique automatically and effectively determines the critical degree, ensuring that just enough nodes (critical set) are included in the protected set to achieve near-full survivability across the entire range of fractional threshold, as evidenced by the blue stars connected by solid lines in Fig. 8. Figure 8b shows the survival probability for the SF network as a

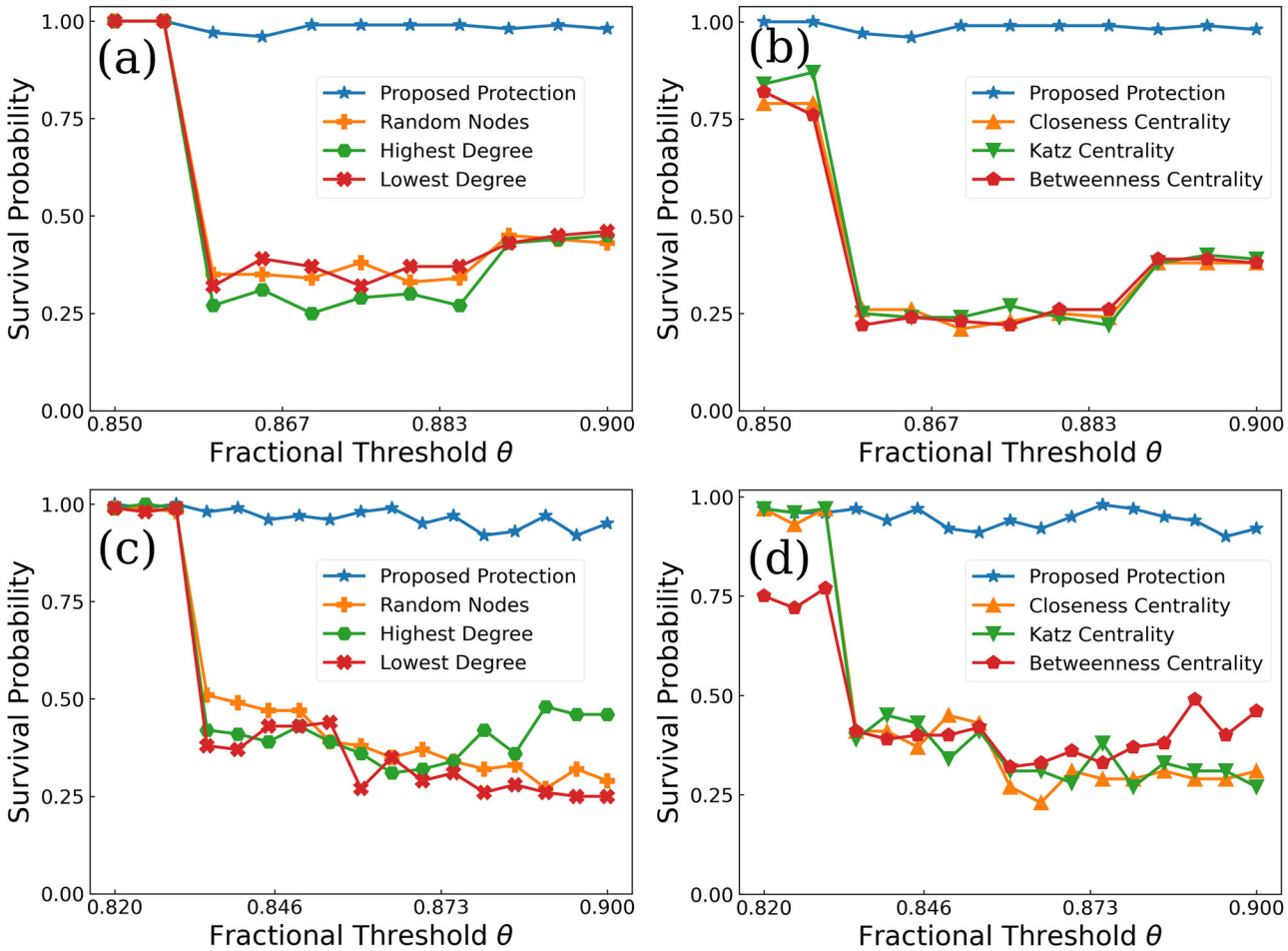

Fig. 7 | Comparison of the proposed and standard mitigation approaches. Survival probabilities as a function of the predefined fractional threshold for distinct mitigation strategies corresponding to the standard Erdős-Rényi (ER) (**a**, **b**) and Scale-free (SF) (**c**, **d**) networks. **a**, **c** Standard intuitive mitigation strategies. **b**, **d** Centrality-based mitigation strategies. We have fixed $N = 10,000$ and an average degree of $\langle k \rangle = 8$ for the ER network and $N = 10{,}000$, $\langle k \rangle = 6$ for the SF network. 150 realizations were performed for each network.

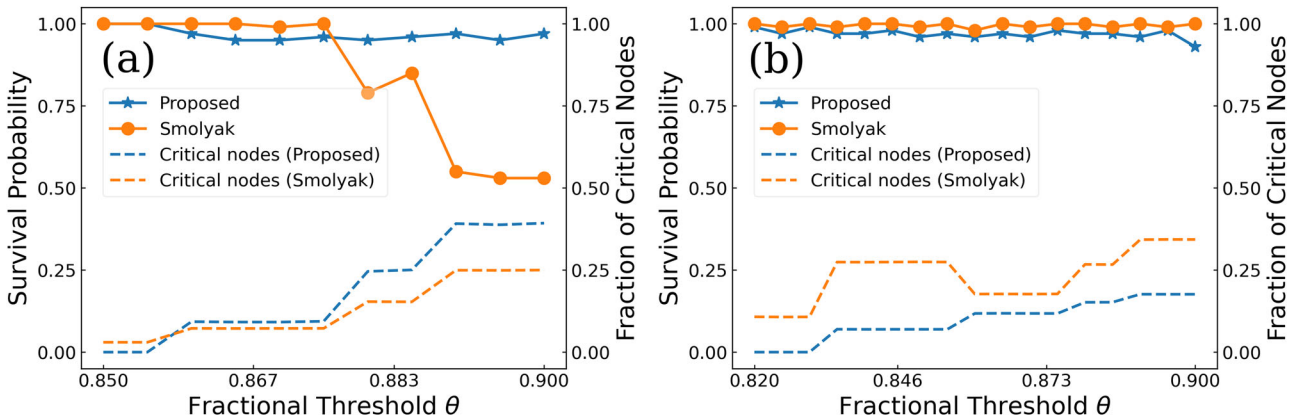

Fig. 8 | Comparison of the proposed and Smolyak's approaches. Survival probabilities as a function of the predefined fractional threshold for proposed and Smolyak's strategies corresponding to the standard Erdős-Rényi (ER) (**a**) and Scale-free (SF) (**b**) networks. The rest details are the same as in Fig. 5.

function of θ in the full protection case. While both strategies maintain full survival probability, the size of the fragile set (yellow dashed line in Fig. 8b) proposed by their algorithm is consistently an overestimate of the critical nodes estimated by our algorithm (blue dashed line in Fig. 8b), which makes it inefficient. Note that a comparison of the critical degree versus θ for both strategies is provided for synthetic and real-world networks in the Supplementary Material (see Fig. S10).

These results establish that the proposed mitigation technique adeptly identifies the minimal critical set to be protected from the pool of fragile nodes, thereby reducing the enormous resources deployed in protecting the entire fragile nodes as adopted by the conventional mitigation strategies[43,53]. Further, we have also confirmed the robustness of the observed results for a wide range of the network sizes and average degrees of both ER and SF networks.

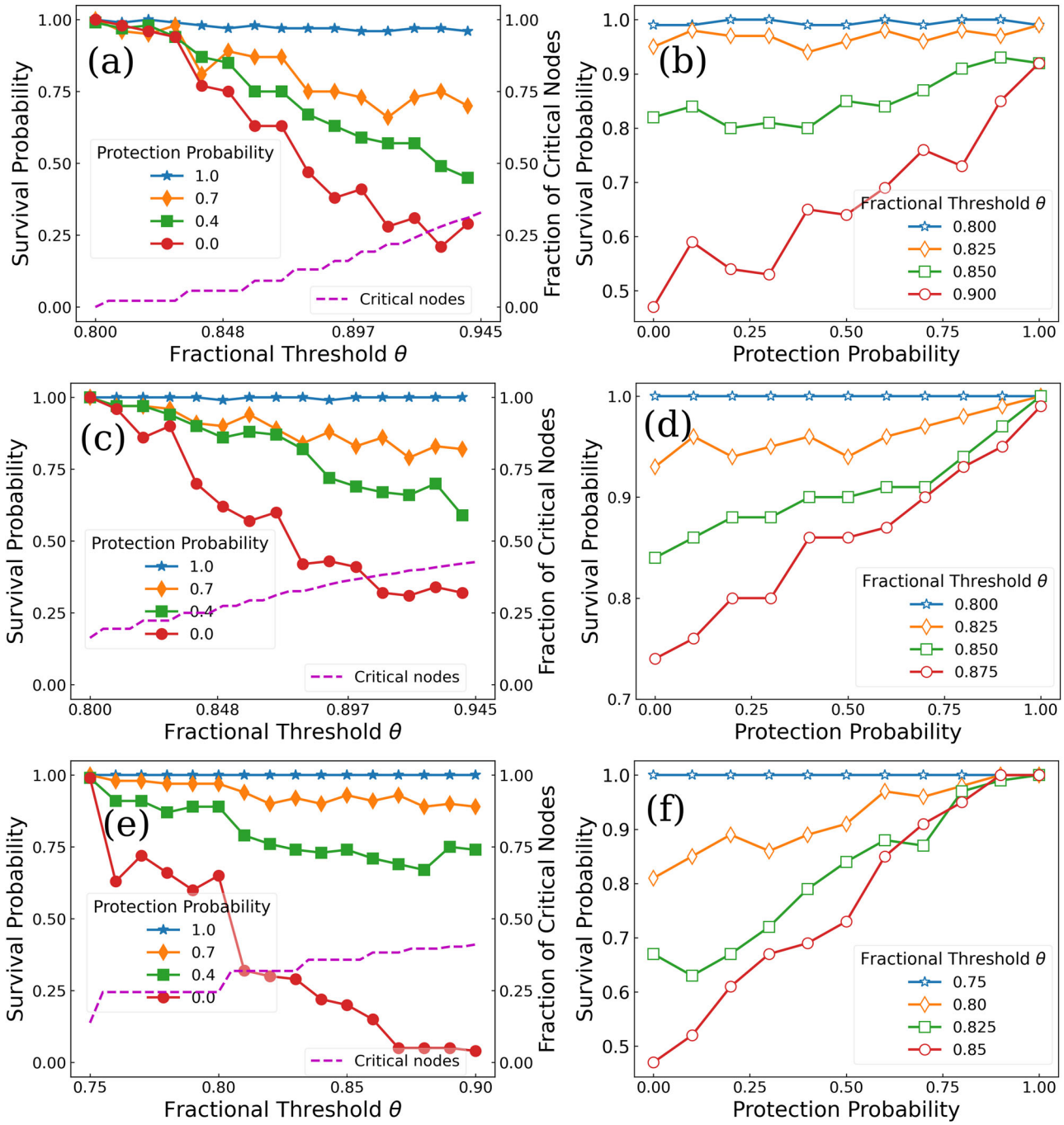

Fig. 9 | Application of the proposed mitigation framework to real-world networks. a, **b** LastFM Asia Social Network, **c**, **d** Condensed matter physics collaboration network, and **e**, **f** US Power Grid network. The other details are the same as in Fig. 5.

Application to the real-world networks

LastFM Asia social network. We proceed to apply our mitigation strategy to assess its efficacy in its application to real-world networks. First, we examine its application to the LastFM Asia Social Network, a collection of LastFM users sourced from the public API in March 2020[54]. In this network, nodes represent LastFM users hailing from Asian countries, while edges correspond to the mutual follower relationships between them. The number of users recorded is $N = 7626$, and their average degree turns out to be $\langle k \rangle = 7.29$. The first row in Fig. 9 illustrates the result of the application of our mitigation strategy on this real-world social network. It is to be noted that the survival probabilities in Fig. 9 are averaged over 150 realizations of random node removal to initiate the cascade. In particular, the survival probability for the LastFM Asia Social network is depicted in Fig. 9a as a function of the predefined fractional threshold for distinct protection probabilities and in Fig. 9b as a function of the protection probability for distinct predefined fractional thresholds. The fraction of the critical nodes to be protected is also represented as the pink dashed line in Fig. 9a. Note that only 2% of the total nodes qualify as critical nodes (which is 37% of the fragile nodes) that need to be protected for the fractional threshold $\theta = 0.805$. Recall that $\theta = 0.805$ refers to the fact that a node must have at least 80.5% of its immediate neighbors to be intact for its survivability. It is obvious that the size of the fragile set increases with the fractional threshold and consequently the critical nodes.

A more detailed analysis of the degree distribution of the critical nodes along the unprotected and fragile nodes is shown in Fig. S5 of the Supplementary Information. The markers and their protection probabilities in the

first column of Fig. 9 are the same as in Fig. 5. The survival probability is almost as large as 100% in the range of $\theta \in (0.8, 0.83)$ for all three distinct degrees of the protection probability including the unprotected case. A sudden drop in their survival probability is observed at $\theta_c = 0.83$ except for the fully protected case, which then decreases almost monotonically as a function of the predefined fraction threshold (see Fig. 9a). The survival probability decreases with an increase in the fractional threshold (see Fig. 9a) for a given partial protection probability. Further, the survival probability, for the distinct predefined fractional threshold, increases as a function of the protection probability (see Fig. 9b), which agrees with the trends observed in Fig. 5. Thus, it is evident that the proposed mitigation strategy, based on graph coloring technique, successfully determined the minimal critical nodes (pink dashed line), users, corresponding to the LastFM Asia Social Network, which needs to be protected for its complete survival probability (stars connected by the blue line).

Collaboration network. As an additional example of a social network, we present a collaboration network. Collaboration networks are primarily scale-free in nature. The proposed fractional threshold model could also be highly useful for identifying the critical nodes of an institution, industry, or researcher. Here, we use the condensed matter physics collaboration data[55] with nodes $N = 23, 133$ and average degree $\langle k \rangle = 8.08$, which is derived from the e-print arXiv and encompasses scientific collaborations among authors who have submitted papers to the condensed matter category. In this network, if the author i has co-authored a paper with the author j, an undirected edge is included between the nodes i and j. Moreover, when a paper is co-authored by k authors, this results in a fully connected subgraph comprising k nodes. Collaboration failure can occur due to various reasons such as severed ties, illness or death of a collaborator, non-compliance with mutual agreements, issues related to credit sharing, and much more. Again, it is evident from Fig. 9c that the collaboration network survives (line connecting stars) completely in the entire explored range of the predefined fractional threshold for full protection probability of its critical set (pink dashed line).

Nevertheless, the survival probabilities decrease as a function of the fractional threshold for the partial protection (lines connecting diamonds and squares) and zero protection (line connecting circles) probabilities. Further, the survival probability decreases with increase in the predefined fractional threshold for a given partial protection probability (see Fig. 9c), whereas the survival probabilities for the distinct predefined fractional thresholds increase as a function of the protection probability (see Fig. 9d). Note that only 16% of the total nodes qualify as critical nodes (which is 38% of the fragile nodes) that need to be protected for the fractional threshold $\theta = 0.80$. A more detailed analysis of the degree distribution of the critical nodes along the unprotected and fragile nodes is shown in Fig. S7 of the Supplementary Information. Thus, we have demonstrated that the collaboration network survives in a range of predefined fractional threshold by protecting the minimal critical nodes (collaborators).

US power grid network. The power grid network is mostly based on the redistribution of load[35,56]. Here, we model it using the basic assumptions of the fractional threshold model to analyze power grids. This implies that the grid fails if more than "m" out of its "k" connecting grids fail. We use the US grid network[57] with nodes $N = 4941$ and average connectivity $\langle k \rangle = 2.67$. Nodes within the network correspond to essential components such as generators, transformers, or substations, while edges symbolize the interconnected power supply lines. In the event of a transformer or substation malfunction, the repercussions extend to the connected transformers, as they correspond to the burden of redistributed loads. The results of the application of the proposed mitigation strategy on the US Grid network are depicted in the second row of Fig. 9. The survival probability decreases monotonically as a function of the predefined fractional threshold for the partial protection (lines connecting diamonds and squares) and the zero protection (line connecting circles) probabilities. However, the power grid network exhibits complete survivability (line connecting stars) upon protecting its critical nodes (pink dashed line) completely in the entire explored range of the predefined fractional threshold.

In addition, the survival probability decreases with an increase in the predefined fractional threshold (see Fig. 9e) for a given partial protection probability. Furthermore, the survival probabilities for the distinct predefined fractional threshold increases as a function of the protection probability (see Fig. 9f) as expected. Note that only 13% of the total nodes qualify as critical nodes (which is 50% of the fragile nodes) that need to be protected for the fractional threshold $\theta = 0.75$. A more detailed analysis of the degree distribution of the critical nodes along the unprotected and fragile nodes is shown in Fig. S6 of the Supplementary Information. Thus, the above results reveal that employing the proposed mitigation framework to gauge the vulnerability of a transformer based on the proportion of its neighboring components could be a pragmatic and efficient approach. By leveraging such a strategy, the proposed algorithm is able to proactively identify the susceptible transformers (critical set) for preemptive upgrades, mitigating the risk of future load fluctuations or overload failures. The degree distributions of fragile, critical, and non-fragile nodes of all paradigmatics and real-world networks are illustrated in Figs. S3–S7 of Supplementary Information to elucidate the efficacy of the graph coloring framework in perfectly identifying the minimal number of critical nodes from the fragile set.

Conclusion

We have introduced a framework to effectively mitigate cascading failures in complex networks. In addition, we have shown that this can be achieved by safeguarding the critical nodes that are most effective at propagating and intensifying failure. The existing mitigation techniques based on the fractional failure mechanism were successful in identifying the fragile nodes to be protected to mitigate the cascade[43], whose relative size is substantial to that of the network. We have identified the least average degree of the colored groups by employing the graph coloring concept, which has been used as a quantifier to refine the fragile set. The fragile nodes with degree greater than the least average degree of the colored groups are qualified as the critical nodes to be protected. The critical nodes are found to be the minimal possible set to retain the maximum survival probability of the networks, which we have established by scaling up and scaling down the least average degree of the colored groups, thereby substantially reducing the enormous computational cost vested in protecting the entire fragile nodes as adopted by the conventional mitigation strategies. Our framework requires only a minimal understanding of the local neighborhoods of the nodes to identify the critical nodes, while significantly enhancing the likelihood of network resilience, even without the precise knowledge of the initial source of impact.

We have validated the proposed framework using Erdős-Rényi and Scale-free networks, which emulate various real-world networks, and established their efficacy over the other failure mechanisms based on their degree and centrality measures. Furthermore, we have also assessed its applicability in practical scenarios by demonstrating its efficacy in various real-world networks, namely, social networks, collaboration networks, and the US power-grid network, including Texas power-grid network. We have also employed the proposed framework to analyze the Texas power grid's resilience against tropical cyclone-induced failures. Using the ACTIVSg2000 test case[58], we have identified the critical nodes whose protection significantly improves the grid's survival probability. This approach requires only network connectivity information, making it more efficient than a recent study focusing on specific line hardening[59]. Note that by protecting just 19% of total nodes (which is roughly half of the fragile nodes identified by our algorithm), the Texas power grid achieves complete survivability for a fractional threshold of 0.75 (see Fig. S8 of the Supplementary Information). A detailed analysis of the Texas power grid is provided in Fig. S9 of the Supplementary Information. By leveraging such a strategy, the proposed algorithm can proactively identify the susceptible transformers (critical set) for preemptive upgrades, mitigating the risk of future load fluctuations or overload failures.

It is to be noted that the proposed framework not only adeptly mitigates cascading failures in simple theoretical models but also establishes its robustness in intricate real-life networks. Understanding the underlying dynamics of failures in complex networks and devising effective mitigation strategies becomes increasingly imperative as we continue to rely on them and integrate complex networks into daily life. While our study has shed light on mitigation of cascading failure in static complex networks, some further open problems could be worked upon, presenting opportunities for future research. Our approach addresses node failure based on the fraction of neighboring nodes, which shows promise in failure mechanisms for social and collaboration networks.

However, in the case of power grid networks, where load redistribution occurs after the failure of a substation or transformer, our failure mechanism may not be as effective. Nonetheless, testing our approach with different failure mechanisms remains an open problem for future research. Another key area for further investigation is the extension of our methodology to coevolving networks[60,61]. As real-world networks are often dynamic, with nodes and edges changing over time, adapting our approach to account for temporal variations could yield valuable insights into its mitigation. Additionally, the emerging field of hypernetworks[62,63], which allows for higher-order interactions beyond pairwise connections, presents another promising avenue for exploration. Despite these unresolved issues, we contend that the methodology presented in this study offers a potentially valuable framework for examining and safeguarding actual networks against catastrophic cascading events. It is also to be noted that though the proposed mitigation technique is effective in providing a computationally efficient and practical solution across a wide range of networks, including synthetic ER and SF networks as well as the real-world networks considered in this study, it may not always guarantee the globally optimal set of critical nodes. This limitation is particularly notable in extremely complex or irregular network structures where achieving a globally optimal solution might require significantly higher computational resources, which might also be an open, challenging problem.

Data availability

The real-world network data (LastFM and Collaboration) that support the findings of this study are available in Stanford Large Network Dataset Collection https://snap.stanford.edu/data/. The US power grid network data is available in network repository https://networkrepository.com/opsahl-powergrid.php. The numerical source data for Figs. 5 to 9 are provided as Supplementary Data with this paper.

Code availability

The codes that were used for the findings of this study are openly available in the GitHub repository[64].

Received: 7 October 2024; Accepted: 1 April 2025;
Published online: 17 April 2025

References

1. Watts, D. J. & Strogatz, S. H. Collective dynamics of –small-world'networks. *Nature* **393**, 440–442 (1998).
2. Newman, M. Networks: an introduction: Oxford University Press, Inc. *Nielsen, M., Elmes, G. and Kipyatkov* 1999 (Elsevier Science, 2010).
3. Latora, V., Nicosia, V. & Russo, G. *Complex networks: principles, methods and applications* (Cambridge University Press, 2017).
4. Aral, S. & Nicolaides, C. Exercise contagion in a global social network. *Nat. Comm.* **8**, 14753 (2017).
5. Wunderling, N., Donges, J. F., Kurths, J. & Winkelmann, R. Interacting tipping elements increase risk of climate domino effects under global warming. *Earth Syst. Dyn.* **12**, 601–619 (2021).
6. Watts, D. J. A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. USA* **99**, 5766–5771 (2002).
7. Albert, R., Jeong, H. & Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
8. Jalili, M. & Perc, M. Information cascades in complex networks. *J. Complex Netw.* **5**, 665–693 (2017).
9. Dobson, I., Carreras, B. A., Lynch, V. E. & Newman, D. E. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science* **17** (2007).
10. Lawrence, J., Blackett, P. & Cradock-Henry, N. A. Cascading climate change impacts and implications. *Clim. Risk Manag.* **29**, 100234 (2020).
11. Gladwell, M. *The tipping point: How little things can make a big difference* (Little, Brown, 2006).
12. Shiller, R. Conversation, information, and herd behavior. *Am. Econ. Rev.* **85**, 181–85 (1995).
13. Lohmann, S. The dynamics of informational cascades: the Monday demonstrations in Leipzig, East Germany, 1989–91. *World Politics* **47**, 42–101 (1994).
14. Bikhchandani, S., Hirshleifer, D. & Welch, I. A theory of fads, fashion, custom, and cultural change in informational cascades. *J. Political Econ.* **100**, 992–1026 (1992).
15. Rogers, E. M. et al. Complex adaptive systems and the diffusion of innovations. *Innov. J. Public Sect. Innov. J.* **10**, 1–26 (2005).
16. Pastor-Satorras, R., Castellano, C., Van Mieghem, P. & Vespignani, A. Epidemic processes in complex networks. *Rev. Mod. Phys.* **87**, 925 (2015).
17. Dodds, P. S. & Watts, D. J. Universal behavior in a generalized model of contagion. *Phys. Rev. Lett.* **92**, 218701 (2004).
18. Šuvakov, M., Mitrović, M., Gligorijević, V. & Tadić, B. How the online social networks are used: dialogues-based structure of myspace. *J. R. Soc. Interface* **10**, 20120819 (2013).
19. Tadić, B., Gligorijević, V., Mitrović, M. & Šuvakov, M. Co-evolutionary mechanisms of emotional bursts in online social dynamics and networks. *Entropy* **15**, 5084–5120 (2013).
20. Smiljanić, J. & Mitrović Dankulov, M. Associative nature of event participation dynamics: a network theory approach. *PloS one* **12**, e0171565 (2017).
21. Holyst, J. A. (ed.) Cyberemotions: collective emotions in cyberspace. Chapter 11, 207–229 (Springer, 2016).
22. Ruan, Z., Iniguez, G., Karsai, M. & Kertész, J. Kinetics of social contagion. *Phys. Rev. Lett.* **115**, 218702 (2015).
23. Granovetter, M. Threshold models of collective behavior. *Am. J. Sociol.* **83**, 1420–1443 (1978).
24. Easley, D. et al. *Networks, crowds, and markets: reasoning about a highly connected world*, vol. 1 (Cambridge University Press, 2010).
25. Helbing, D. Globally networked risks and how to respond. *Nature* **497**, 51–59 (2013).
26. Wikipedia contributors. Iwiw — Wikipedia, the free encyclopedia (accessed 5 March 2024).
27. Török, J. & Kertész, J. Cascading collapse of online social networks. *Sci. Rep.* **7**, 16743 (2017).
28. Yuan, X., Dai, Y., Stanley, H. E. & Havlin, S. k-core percolation on complex networks: comparing random, localized, and targeted attacks. *Phys. Rev. E* **93**, 062302 (2016).
29. Chalupa, J., Leath, P. L. & Reich, G. R. Bootstrap percolation on a Bethe lattice. *J. Phys. C Solid State Phys.* **12**, L31 (1979).
30. Centola, D. & Macy, M. Complex contagions and the weakness of long ties. *Am. J. Sociol.* **113**, 702–734 (2007).
31. Huang, X., Vodenska, I., Havlin, S. & Stanley, H. E. Cascading failures in bi-partite graphs: model for systemic risk propagation. *Sci. Rep.* **3**, 1219 (2013).
32. Gai, P. & Kapadia, S. Contagion in financial networks. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **466**, 2401–2423 (2010).
33. Feng, L. et al. Competing for attention in social media under information overload conditions. *PloS one* **10**, e0126090 (2015).
34. Motter, A. E. & Lai, Y.-C. Cascade-based attacks on complex networks. *Phys. Rev. E* **66**, 065102 (2002).

35. Crucitti, P., Latora, V. & Marchiori, M. Model for cascading failures in complex networks. *Phys. Rev. E* **69**, 045104 (2004).
36. Kubale, M. *Graph colorings*, vol. 352 (American Mathematical Soc., 2004).
37. Matula, D. W. & Beck, L. L. Smallest-last ordering and clustering and graph coloring algorithms. *J. ACM* **30**, 417–427 (1983).
38. ERDdS, P. & Rwi, A. On random graphs I. *Publ. Math. Debr.* **6**, 18 (1959).
39. Albert, R. & Barabási, A.-L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 47 (2002).
40. Watts, D. J. & Dodds, P. S. Influentials, networks, and public opinion formation. *J. Consum. Res.* **34**, 441–458 (2007).
41. Duenas-Osorio, L. & Vemuru, S. M. Cascading failures in complex infrastructure systems. *Struct. Saf.* **31**, 157–167 (2009).
42. Elliott, M., Golub, B. & Jackson, M. O. Financial networks and contagion. *Am. Econ. Rev.* **104**, 3115–3153 (2014).
43. Smolyak, A., Levy, O., Vodenska, I., Buldyrev, S. & Havlin, S. Mitigation of cascading failures in complex networks. *Sci. Rep.* **10**, 16124 (2020).
44. Bondy, J. A. & Murty, U. S. R. *Graph theory* (Springer Publishing Company, Incorporated, 2008).
45. Dandashi, A. & Al-Mouhamed, M. Graph coloring for class scheduling. In *Proc. ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, 1–4, https://doi.org/10.1109/AICCSA.2010.5586963 (2010).
46. Welsh, D. J. & Powell, M. B. An upper bound for the chromatic number of a graph and its application to timetabling problems. *Comput. J.* **10**, 85–86 (1967).
47. Baggam, D. S. & Rani, S. Security for wireless sensor networks: bibliometric analysis. In *Proc. 2022 3rd International Conference on Computing, Analytics and Networks (ICAN)*, 1–5 (IEEE, 2022).
48. Chaitin, G. J. Register allocation & spilling via graph coloring. *ACM Sigplan Not.* **17**, 98–101 (1982).
49. Hale, W. K. Frequency assignment: theory and applications. *Proc. IEEE* **68**, 1497–1514 (1980).
50. Appel, K. I. & Haken, W. *Every planar map is four colorable*, vol. 98 (American Mathematical Soc, 1989).
51. Freeman, L. A set of measures of centrality based on betweenness. *Sociometry* **40**, 35–41 (1977).
52. Katz, L. A new status index derived from sociometric analysis. *Psychometrika* **18**, 39–43 (1953).
53. Ghanbari, R., Jalili, M. & Yu, X. Correlation of cascade failures and centrality measures in complex networks. *Future Gener. Comput. Syst.* **83**, 390–400 (2018).
54. SNAP: Network datasets: LastFM Asia Social Network — snap.stanford.edu. https://snap.stanford.edu/data/feather-lastfm-social.html (SNAP, accessed 11 August 2024).
55. Condense matter collaboration network. https://snap.stanford.edu/data/ca-CondMat.html (SNAP, accessed 11 August 2024).
56. Zhang, J., Dai, Y., Zou, K., Song, B. & Zhang, Z. Vulnerability analysis of the us power grid based on local load-redistribution. *Saf. Sci.* **80**, 156–162 (2015).
57. Rossi, R. A. & Ahmed, N. K. The network data repository with interactive graph analytics and visualization. In *AAAI* (2015).
58. ACTIVSg2000: 2000-bus synthetic grid on footprint of Texas — electricgrids.engr.tamu.edu. https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg2000/ (Latest Synthetic Electric Grid Cases, accessed 14 September 2024).
59. Stürmer, J. et al. Increasing the resilience of the Texas power grid against extreme storms by hardening critical lines. *Nature Energy* **9**, 526–535 (2024).
60. Gross, T. & Blasius, B. Adaptive coevolutionary networks: a review. *J. R. Soc. Interface* **5**, 259–271 (2008).
61. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D.-U. Complex networks: structure and dynamics. *Phys. Rep.* **424**, 175–308 (2006).
62. Ha, D., Dai, A. & Le, Q. V. Hypernetworks. *arXiv preprint arXiv:1609.09106* (2016).
63. Johnson, J. *Hypernetworks in the science of complex systems*, vol. 3 (World Scientific Imperial College Press, 2013).
64. Singh, K. Graph-coloring-mitigation. https://github.com/karanbisht684/Graph-coloring-mitigation/ (2024).

Acknowledgements

The work of V.K.C. is supported by DST-CRG Project under Grant No. CRG/2020/004353 and VKC wish to thank DST, New Delhi for computational facilities under the DST-FIST program (SR/FST/PS- 1/2020/135) to the Department of Physics. DVS is supported by the DST-SERB-CRG Project under Grant No. CRG/2021/000816. WZ is supported by the National Natural Science Foundation of China (Grant Nos. 12475035) and the Natural Science Foundation of Guangdong Province, China (Grant No. 2024A1515013238). I gratefully acknowledge Alex Smolyak for the fruitful discussions.

Author contributions

K.S. conceptualized, developed the methods, and carried out the numerical experiments. K.S. and D.V.S. analyzed the results and wrote the initial manuscript. K.S., D.V.S., W.Z., J.K., and V.K.C. interpreted the simulation results, revised the manuscript, and approved the final version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-025-02089-y.

Correspondence and requests for materials should be addressed to D. V. Senthilkumar.

Peer review information *Communications Physics* thanks Fenghua Wang and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at http://www.nature.com/reprints

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

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2025