Journal of Complex Networks (2023) **6**, Advance Access Publication on 6 December 2023
https://doi.org/10.1093/comnet/cnad047

Exploring the effectiveness of node attacks based on combined centrality measures in scale-free networks

P. B. DIVYA[1,†], T. P. JOHNSON[2], KANNAN BALAKRISHNAN[3], AND N. AZAD[4]
[1]*Department of Mathematics, Cochin University of Science and Technology, Kochi-682022, Kerala, India*
[2]*Applied Sciences and Humanities Division, School of Engineering, Cochin University of Science and Technology, Kochi-682022, Kerala, India*
[3]*Department of Computer Applications, Cochin University of Science and Technology, Kochi-682022, Kerala, India*
[4]*Software Architect, Telaverge Communication India Pvt Ltd, Bengaluru, Karnataka 560066, India*
[†]Corresponding author. Email: pbdivya@gmail.com

[Received on 7 May 2023; editorial decision on 10 November 2023; accepted on 16 November 2023]

This article introduces a novel method for targeting complex networks that involves using a hybrid centrality score to rank nodes and carry out attacks. Unlike previous studies that have focused on using individual centrality measures, this approach takes into consideration the varying significance of nodes across different centrality measures. The study utilizes simulations on scale-free networks to demonstrate that the proposed strategy can be highly effective in inducing network failure, and certain combinations of centrality measures can result in greater attack severity than using individual measures alone. Overall, the research offers valuable insights into improving node-attack strategies for complex networks, which are typically resilient to random failures but susceptible to targeted attacks.

Keywords: complex networks; node-attack strategy; central attacks; hybrid centrality; largest connected component; attack severity.

1. Introduction

Complex networks are ubiquitous in various fields, such as biology, social sciences and transportation systems [1–10]. These networks are characterized by their complex structures, high connectivity and resilience to random failures [11]. However, they are vulnerable to targeted attacks, such as node or link removal, which can cause significant damage or even collapse. Thus, understanding the nature of effective node-attack strategies is essential for maintaining the robustness and security of complex networks [12]. In recent years, many studies have investigated the importance of nodes in complex networks, and various centrality measures have been proposed to quantify a node's significance [13, 14]. However, most of these studies have focused on individual centrality measures, which may not accurately reflect a node's overall importance across different measures. Therefore, it is necessary to explore the idea of using a combination of centrality measures to rank nodes and perform attacks accordingly [15].

In this research article, we propose a novel node-attack strategy that utilizes a specific convex combination of three centrality measures, namely degree centrality, betweenness centrality and closeness centrality. We aim to investigate the effectiveness of our suggested strategy through simulations on scale-free networks. By modifying the coefficients in the convex combination, we examine the impact of our proposed node-attack strategy and compare it with attacks based on individual centrality measures.

Our findings suggest that certain combinations of centrality measures result in higher severity than individual centrality points, demonstrating the effectiveness of convex combination of centralities on scale-free networks. Our study provides insights into optimizing node-attack strategies in complex networks, which can aid in enhancing the robustness and security of various systems that rely on these networks.

2. Related literature

In recent years, the study of attacks in complex networks has gained significant attention due to its implications in various real-world scenarios [4–6, 8, 16, 17]. Researchers have investigated the robustness and vulnerability of complex networks under different types of attacks, including targeted attacks and central attacks [18–24]. Targeted attacks aim to exploit specific vulnerabilities within a network by targeting its most critical nodes or edges. Central attacks, a specific type of targeted attack, focus on compromising the network's most central nodes, potentially causing significant disruptions to the network's functionality and stability [12, 25].

One approach to identify the most central nodes in a network is through individual centrality measures [19, 20, 26–29]. These measures include degree centrality, betweenness centrality and eigenvector centrality, among others. Degree centrality considers the number of connections a node has, while betweenness centrality accounts for the number of shortest paths that pass through a node. Eigenvector centrality, on the other hand, considers the importance of the nodes that are connected to a particular node [14, 30].

However, a single centrality measure may not be enough to capture the complex structure and importance of nodes in a network. Therefore, researchers have proposed combined centrality measures that consider multiple centrality measures simultaneously [31]. For instance, Fei *et al.* [32] suggested combining different centrality measures by calculating the median of a node's maximum and minimum ranks induced by a given set of centrality measures. Meanwhile, Zhang *et al.* [33] used a combination of betweenness centrality and Katz centrality to evaluate node importance.

One more general approach is introduced by Keng *et al.* [15] by taking the convex combination of centralities, which combines different centrality measures with different weights. This approach can capture the importance of nodes based on different criteria, making it a more comprehensive measure of node importance.

Overall, these studies demonstrate the importance of considering different types of attacks and centrality measures when analysing the robustness and vulnerability of complex networks. The use of combined centrality measures, such as the convex combination of centralities, can provide a more accurate and comprehensive measure of node importance, which can aid in developing effective strategies for defending against attacks in complex networks [15].

In our work, we are trying to explore the significance of combined centrality attacks through attack simulations on scale free network.

3. Methodology

The major metrics that measure worth of a vertex are the various centrality measures. But, it is noticed that the role of nodes is different for different centrality measures. So ranking the nodes based on single centrality measure cannot be justified. For instance, consider the below example analysing the nodes in the highest positions based on various centralities

TABLE 1 *Rank values and corresponding nodes under DC, BC and CC*

Rank	DC	BC	CC
1	6	10	4, 10
2	7	1	6, 9
3	1, 4, 5, 8, 10	4	7, 9
4	2, 3, 9	6	1, 5, 8
5	-	7	-

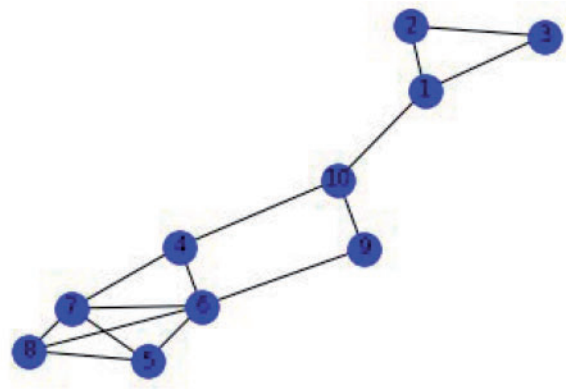

FIG. 1. An example graph

Table 1 shows the top 5 rank values and their corresponding nodes under degree centrality (DC), betweenness centrality (BC) and closeness centrality (CC) for the graph shown in Fig. 1.

The relative rankings of the nodes in each of the centrality measures indicate that the importance of nodes differs depending on the type of centrality measure used. Therefore, it is important to consider multiple measures of centrality when analysing the importance of nodes in a network.

Keng *et al.* [15] proposed a convex combination of the centrality measures. Here, we use this idea to perform attacks and assess its effectiveness. We call it as hybrid centrality index (HCI) which is defined as :

$$\text{HCI}_v = t_1 c_1(v) + t_2 c_2(v) + ... + t_n c_n(v), \tag{3.1}$$

where t_i is the weight assigned to the ith centrality measure c_i, and $c_i(v)$ is the normalized centrality score of vertex v for the ith measure c_i. The weights t_i satisfy the following conditions:

$$t_1 + t_2 + ... + t_n = 1, \tag{3.2}$$

and

$$0 \leq t_i \leq 1, \forall i \in \{1, 2, ..., n\} \tag{3.3}$$

where n represents the number of different centrality measures being considered in the HCI.

The normalization of centrality measures c_i are done with min–max criteria which re-scales the values in the range [0,1]. This ensures that the impact of a centrality measure on the final score is proportional to its relative importance.

The HCI is calculated using different convex combinations of weights t_i, where each weight corresponds to a different centrality measure. Once the HCI scores are calculated for all nodes in the graph, a node removal attack is performed to assess its efficiency. The attack's effectiveness is measured using the size of the largest connected component (LCC) after the attack. The results are compared to identify the weightage combination that provides highest attack severity. The weightage combination that results in the highest reduction in the size of the LCC is considered the most effective in terms of attack severity.

The HCI method provides a useful framework for evaluating node importance in a graph by combining multiple centrality measures and assessing the impact of node removal attacks. This study will provide insights into the effectiveness of the HCI method and the usefulness of combining multiple centrality measures for identifying critical nodes in complex networks.

4. Simulation study

The simulation study aims to compare the effectiveness of attacks based on combined centrality measure (using the HCI method) with those based on individual centrality measures.

For the study, we specifically use a set of three centrality measures: degree centrality, betweenness centrality and closeness centrality, to capture different aspects of node importance in the network including the number of direct connections (degree centrality), the degree to which a node lies on the shortest paths between other nodes (betweenness centrality), and the speed at which a node can reach other nodes in the network (closeness centrality) [34].

To evaluate the effectiveness of the HCI method, we perform node removal attack on a scale-free network, which is a common network structure found in many real-world systems. The analysis of the attack's effectiveness is based on the size of the LCC of the network after node removal [19, 35, 36].

We can summarise the major steps as follows.

4.1 *Network generation*

The choice of an appropriate network structure is crucial for any simulation study, as it can significantly impact the validity and relevance of the results. In our study, we chose to use scale-free networks as they are widely used to model real-world networks, including social networks, the internet and biological networks [37–39]. Scale-free networks are characterized by a power-law degree distribution, which means that the number of nodes with a certain degree follows a power-law distribution, rather than a normal distribution [37]. It means that a few nodes have a high degree, while most nodes have a low degree. This heterogeneity in node degrees is commonly observed in many real-world networks and makes scale-free networks an appropriate choice for simulating such networks. Previous studies have also used scale-free networks for similar simulation studies, further validating our choice of network structure [19, 40, 41]. Using a scale-free network as the underlying graph structure in our simulation study allows us to better capture the complex connectivity patterns and heterogeneity of real-world networks and evaluate the effectiveness of the HCI method in a realistic network setting.

A widely utilized algorithm for generating scale-free networks is the *Barabasi–Albert* algorithm [42]. The BA model operates by first initializing with a small set of nodes and then incrementally adding new

nodes to the network. The new nodes are preferentially attached to existing nodes that already have high degree. At every step, a new node is introduced into the network and is linked to a predetermined number of existing nodes (specified by parameter m), with the likelihood of linking to a particular node being proportional to its degree. That is that nodes with more connections are more probable to receive new links [42]. The study examined four scale-free networks of varying sizes, including 50, 100, 500 and 1000 nodes. The parameter value for each network was fixed at $m = 3$.

4.2 *Calculation of HCI*

The HCI score is calculated by computing the relevant centrality measures for each node in the network and combining them using a weighted sum formula [15]. The centrality measures used in our study are degree centrality, betweenness centrality and closeness centrality. Hence, we can calculate the HCI score for each node in the network using the following formula:

$$\mathrm{HCI}_v = t_1 \mathrm{BC}_v + t_2 \mathrm{CC}_v + t_3 \mathrm{DC}_v. \tag{4.1}$$

where

- $t_i, i = 1, 2, 3$ correspond to the weightage of the respective centrality measures.
- BC_v is the betweenness centrality of a node v, defined as [43, 44]:

$$\mathrm{BC}_v = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}, \tag{4.2}$$

  where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths that pass through v.
- CC_v is the closeness centrality of a of a node v, defined as [44]

$$\mathrm{CC}_v = \frac{1}{\sum_u d(u, v)}, \tag{4.3}$$

  where $d(u, v)$ is the shortest distance between u and v.
- DC_v is the degree centrality of node v which is the number of edges incident to v [20].

We choose t_i values in the range [0,1] with increments of 0.1, such that the sum of all three weightage values adds up to 1. Using this approach, we can obtain 66 different weightage combinations for the three centrality measures. Figure 2 shows the list of weightage combinations for the three centrality measures with S1 denoting degree centrality (DC), S11 denoting closeness centrality and S66 denoting betweenness centrality.

Once we have identified the weightage values for the three centrality measures, we can calculate the HCI score for each node in the network using Equation 4.1. Each combination corresponds to a unique set

Code	(t_1, t_2, t_3)	Code	(t_1, t_2, t_3)	Code	(t_1, t_2, t_3)
S1	(0.0, 0.0, 1.0)	S23	(0.2, 0.1, 0.7)	S45	(0.4, 0.6, 0.0)
S2	(0.0, 0.1, 0.9)	S24	(0.2, 0.2, 0.6)	S46	(0.5, 0.0, 0.5)
S3	(0.0, 0.2, 0.8)	S25	(0.2, 0.3, 0.5)	S47	(0.5, 0.1, 0.4)
S4	(0.0, 0.3, 0.7)	S26	(0.2, 0.4, 0.4)	S48	(0.5, 0.2, 0.3)
S5	(0.0, 0.4, 0.6)	S27	(0.2, 0.5, 0.3)	S49	(0.5, 0.3, 0.2)
S6	(0.0, 0.5, 0.5)	S28	(0.2, 0.6, 0.2)	S50	(0.5, 0.4, 0.1)
S7	(0.0, 0.6, 0.4)	S29	(0.2, 0.7, 0.1)	S51	(0.5, 0.5, 0.0)
S8	(0.0, 0.7, 0.3)	S30	(0.2, 0.8, 0.0)	S52	(0.6, 0.0, 0.4)
S9	(0.0, 0.8, 0.2)	S31	(0.3, 0.0, 0.7)	S53	(0.6, 0.1, 0.3)
S10	(0.0, 0.9, 0.1)	S32	(0.3, 0.1, 0.6)	S54	(0.6, 0.2, 0.2)
S11	(0.0, 1.0, 0.0)	S33	(0.3, 0.2, 0.5)	S55	(0.6, 0.3, 0.1)
S12	(0.1, 0.0, 0.9)	S34	(0.3, 0.3, 0.4)	S56	(0.6, 0.4, 0.0)
S13	(0.1, 0.1, 0.8)	S35	(0.3, 0.4, 0.3)	S57	(0.7, 0.0, 0.3)
S14	(0.1, 0.2, 0.7)	S36	(0.3, 0.5, 0.2)	S58	(0.7, 0.1, 0.2)
S15	(0.1, 0.3, 0.6)	S37	(0.3, 0.6, 0.1)	S59	(0.7, 0.2, 0.1)
S16	(0.1, 0.4, 0.5)	S38	(0.3, 0.7, 0.0)	S60	(0.7, 0.3, 0.0)
S17	(0.1, 0.5, 0.4)	S39	(0.4, 0.0, 0.6)	S61	(0.8, 0.0, 0.2)
S18	(0.1, 0.6, 0.3)	S40	(0.4, 0.1, 0.5)	S62	(0.8, 0.1, 0.1)
S19	(0.1, 0.7, 0.2)	S41	(0.4, 0.2, 0.4)	S63	(0.8, 0.2, 0.0)
S20	(0.1, 0.8, 0.1)	S42	(0.4, 0.3, 0.3)	S64	(0.9, 0.0, 0.1)
S21	(0.1, 0.9, 0.0)	S43	(0.4, 0.4, 0.2)	S65	(0.9, 0.1, 0.0)
S22	(0.2, 0.0, 0.8)	S44	(0.4, 0.5, 0.1)	S66	(1.0, 0.0, 0.0)

FIG. 2. List of weightage combinations for the three centrality measures

of weightage values that determines the relative importance of each centrality measure in the calculation of the overall HCI score.

4.3 *Attack Simulation*

We employ two types of attack strategies, namely the initial attack and the recalculated attack based on the HCI score for each weightage combination.

In the initial attack strategy, nodes are first sorted in descending order based on their centrality scores, and then removed one by one from the highest to the lowest score. The second attack strategy we used is the recalculated attack, in which the centrality values of the remaining nodes are recalculated after each node removal iteration. The node list is then sorted based on the updated centrality values, and the next node to be removed is selected from the top of the list [45].

To ensure the effectiveness of the attack, we considered the residual giant component of the network in each iteration of the attack [36]. We recorded the size of the LCC of the network after each round of node removal for each target fraction. To address the issue of ties in the selection of target nodes with similar HCI scores, we performed multiple attack trials for different network sizes and calculated the average size of the LCC from the obtained results.

4.4 *Severity checking*

To compare the severity of attacks using different weightage combinations, we use the severity measure V_{index}. The V_{index} is calculated for each weightage combination using the following formula [46]:

$$V_{\text{index}} = 0.5 - \frac{1}{N}\sum_{i=1}^{N}\frac{\text{LCC}_i}{N}, \tag{4.4}$$

where,

- N represents the size of the original network
- LCC_i represents the size of the LCC in the network after removing the ith node.

It is important to note that the vulnerability index V is derived as the complementary quantity to the robustness index R, where R is defined as [20]:

$$R = \frac{1}{N}\sum_{i=1}^{N}\frac{\text{LCC}_i}{N}. \tag{4.5}$$

The robustness index R, which quantifies the network's resilience to vertex removal, has a range between $1/N$ (minimum) and $\frac{1}{2}(1 - 1/N)$ (maximum) for any network and method of vertex removal. Therefore, the vulnerability index V inherits this fixed range and is bounded within the range of 0 to $\frac{1}{2}$ [20, 47].

We calculate the V_{index} value for each weightage combination and then compare them. The weightage combination with the highest V_{index} value is considered to be the most effective for the attack strategy.

4.5 *Result analysis and Discussion*

The result analysis process involves creating a scatter plot for each network to compare the severity of the initial attack and the recalculated attack using hybrid centrality approach with different weightage combinations. The x-axis represents the weightage of betweenness centrality (t_1), and the y-axis represents the weightage of closeness centrality (t_2). Since the weightage of degree centrality (t_3) depends on t_1 and t_2, its value is evident from the plot even though it is not explicitly represented. The point (0,0) on the plot represents the individual degree centrality measure, whereas (1,0) represents the betweenness centrality measure, and (0,1) represents the closeness centrality measure.

The severity of the attacks is indicated by the colour of the scatter points, with the colour bar indicating the severity levels. The plot provides an easy visualization of the severity of attacks under different centrality weightage combinations.

Using the plot, we can identify regions where the severity of attacks is high, indicating that the corresponding weightage combination is effective in maximizing the impact of network attacks. Additionally, we can analyse the distribution of severity values across the plot to identify any clusters or outliers, which could provide insights into potential vulnerabilities in the network.

Figures 3, 4, 5, 6 illustrates the comparison of severity levels for initial and recalculated attacks on a scale-free network of sizes 50, 100, 500 and 1000 (SF50, SF100, SF500 and SF1000) using the HCI scores calculated for 66 weightage combinations.

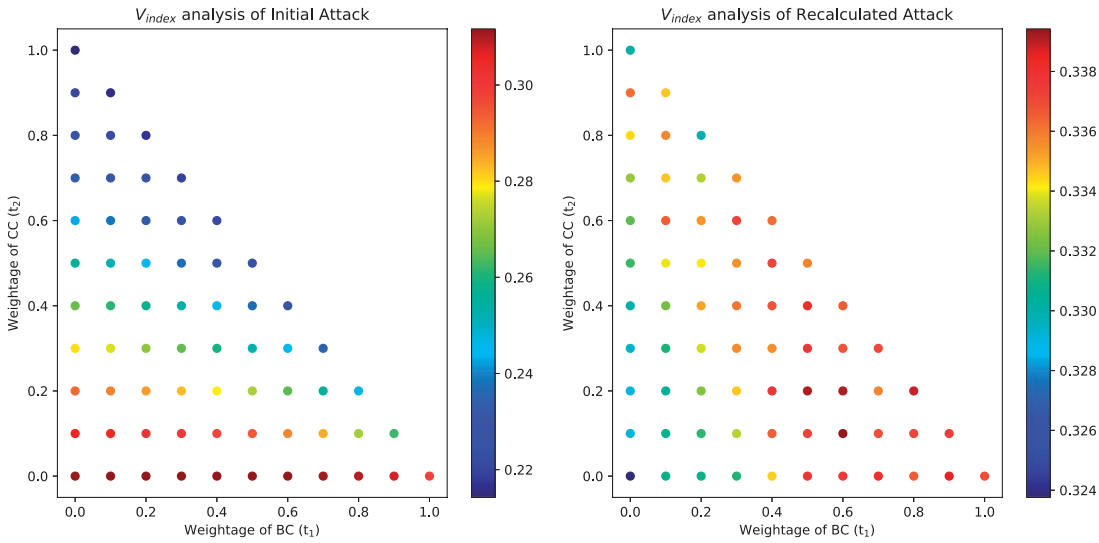

FIG. 3. Comparison of severity (V_{index}) of initial and recalculated attack on SF50 for different weightage combinations

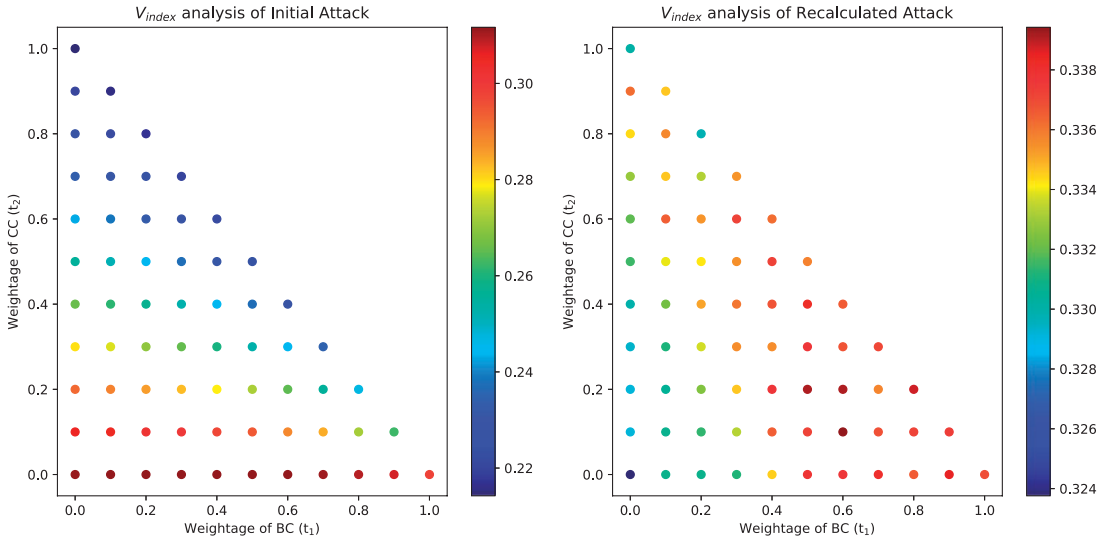

FIG. 4. Comparison of severity (V_{index}) of initial and recalculated attack on SF100 for different weightage combinations

Based on the severity plot in Fig. 3, we can observe that the severity level is high for the initial attack when the weightage is less for closeness centrality. The highest severity occurs at the weightage combination of (0.9, 0.0, 0.1), which implies that the network is highly vulnerable to attacks targeting the betweenness centrality while minimizing the closeness centrality. Specifically, this weightage combination emphasizes the importance of degree centrality, with a higher weightage given to the betweenness centrality over the closeness centrality. The results indicate that attackers can effectively break the SF50

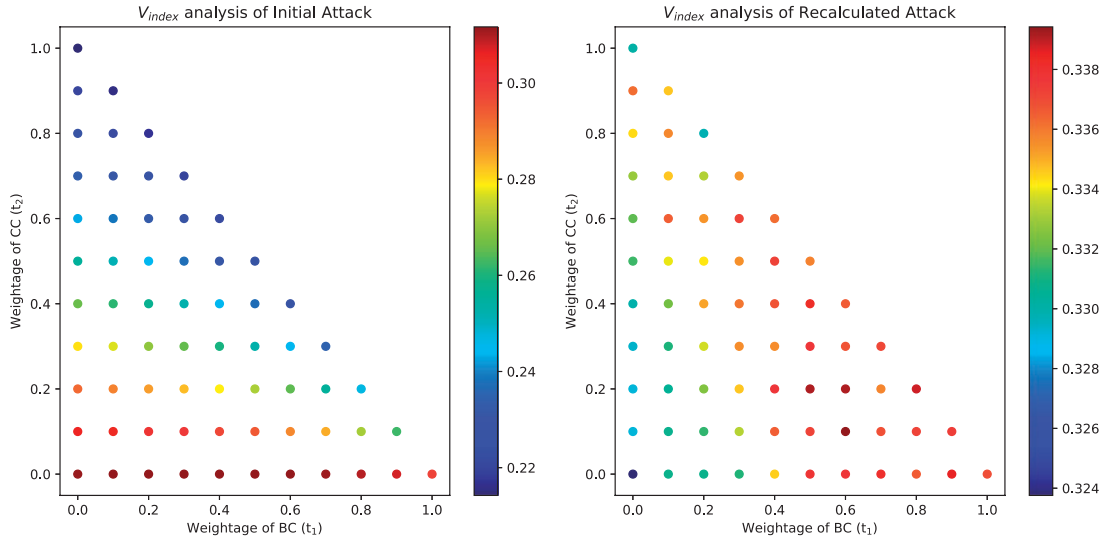

FIG. 5. Comparison of severity (V_{index}) of initial and recalculated attack on SF500 for different weightage combinations

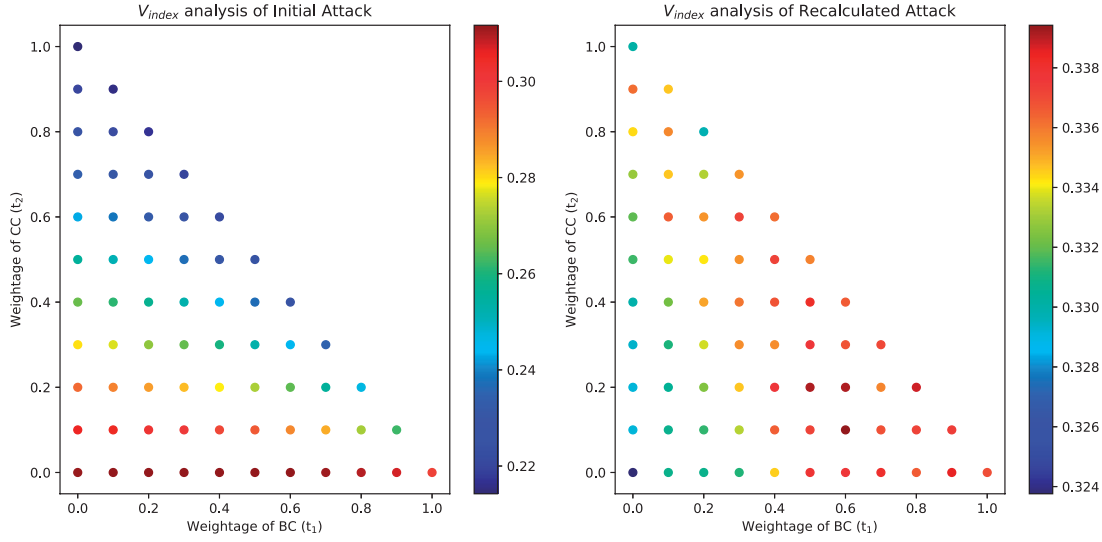

FIG. 6. Comparison of severity (V_{index}) of initial and recalculated attack on SF1000 for different weightage combinations

network by focusing on the most central nodes with high betweenness centrality while avoiding nodes with high closeness centrality.

Similar observations were made for the other studied networks as well regarding the severity of the initial attack. The plots showed that the severity level was high when the weightage for closeness centrality was low and the weightage for betweenness centrality was high.

TABLE 2 *Top 3 Weightage combinations with the highest severity values (V-index)*

Network	Initial attack		Recalculated attack	
	V-index	Weightage combination	*V*-index	Weightage combination
SF50	0.2376	(0.9, 0.0, 0.1)	0.2696	(0.1, 0.2, 0.7)
	0.2364	(0.0, 0.0, 1.0)	0.2696	(0.0, 0.3, 0.7)
	0.2348	(0.8, 0.0, 0.2)	0.2692	(0.1, 0.3, 0.6)
SF100	0.2763	(0.0, 0.0, 1.0)	0.3066	(0.3, 0.5, 0.2)
	0.2747	(0.7, 0.0, 0.3)	0.3058	(0.2, 0.4, 0.4)
	0.2742	(0.1, 0.0, 0.9)	0.3058	(0.2, 0.5, 0.3)
SF500	0.3110	(0.9, 0.0, 0.1)	0.3399	(0.7, 0.1, 0.2)
	0.3106	(0.1, 0.0, 0.9)	0.3388	(0.8, 0.0, 0.2)
	0.3106	(0.2, 0.0, 0.8)	0.3386	(0.7, 0.2, 0.1)
SF1000	0.311677	(0.1, 0.0, 0.9)	0.33942	(0.6, 0.1, 0.3)
	0.311677	(0.2, 0.0, 0.8)	0.33909	(0.6, 0.2, 0.2)
	0.311676	(0.3, 0.0, 0.7)	0.33908	(0.5, 0.2, 0.3)

The severity plot analysis shows that for the recalculated attack on the SF50 network, the combination of 0.1 weightage for degree centrality, 0.2 weightage for betweenness centrality and 0.7 weightage for closeness centrality leads to the highest severity. Interestingly, the severity values for this combination are also relatively high for a range of weightage values, specifically at a weightage of 0.1 for betweenness centrality and 0.3 for closeness centrality, up to 0.7. This implies that attacks on the SF50 network can be highly effective when the attacker prioritizes closeness and degree centrality while giving moderate weightage to betweenness centrality. The result of the recalculated attack in SF100 shows a similar pattern to SF50, while for SF500 and SF1000, the point of highest severity has shifted to a weightage combination where the betweenness centrality weightage is high and the closeness centrality weightage is low.

Table 2 outlines the top three weightage combinations associated with the highest severity values (*V*-index) for each network when initial and recalculated attacks are performed on it. This table provides valuable insights into the most effective weightage combinations for network attacks across the studied networks.

This study highlights the significance of utilizing a hybrid centrality approach to formulate an efficient attack strategy. The results show that the severity of attacks is high at weightage combinations that do not solely rely on individual centrality measures. However, further investigation is necessary to recognize the patterns in which the severity values change with different weightage values across diverse network topologies. In addition, the optimal weightage combination can be determined by using a grid search approach [48, 49].

5. Summary

This study investigated the effectiveness of different weightage combinations of degree, betweenness, and closeness centrality in breaking a network through initial and recalculated attacks on scale-free networks of various sizes. The results demonstrated that the severity of attacks was highest at points other than individual centrality measures, underscoring the importance of using a combined centrality approach in

designing effective attack strategies. Furthermore, the highest severity points varied depending on the network size and weightage combinations, indicating the need for further research to identify patterns in severity values across different networks. Overall, this study provides valuable insights into the use of centrality measures for breaking networks and can aid in the development of targeted attack strategies to weaken networks. We aim to extend this work to encompass a broader spectrum of empirical networks and real-world network scenarios.

References

1. Barabasi, A. L., & Oltvai, Z. N. (2004) Network biology: understanding the cell's functional organization. *Nat. Rev. Genetics*, **5**, 101–113.
2. Bellingeri, M., Bevacqua, D., Scotognella, F., Alfieri, R., Nguyen, Q., Montepietra, D., & Cassi, D. (2020) Link and node removal in real social networks: a review. *Front. Phys.*, **8**, 228.
3. Jin, E. M., Girvan, M., & Newman, M. E. (2001) Structure of growing social networks. *Phys. Rev. E*, **64**, 046132.
4. Latif, M. A., Naveed, M., & Zaidi, F. (2013) Resilience of social networks under different attack strategies. In Social Informatics: 5th International Conference, SocInfo 2013, Kyoto, Japan, November 25-27, 2013, *Proceedings 5*, Springer International Publishing, pp. 16–29.
5. Malik, H. A. M., Abid, F., Wahiddin, M. R., & Bhatti, Z. (2017) Robustness of dengue complex network under targeted versus random attack. *Complexity*, **2017**. DOI: 10.1155/2017/2515928.
6. Newman, M. E. (2001) Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. *Phys. Rev. E*, **64**, 016132.
7. Newman, M. E. (2002) Spread of epidemic disease on networks. *Phys. Rev. E*, **66**, 016128.
8. Zhang, D., Cetinkaya, E. K., & Sterbenz, J. P. (2013) Robustness of mobile ad hoc networks under centrality-based attacks. In *2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, pp. 229–235.
9. Zhou, Y., Wang, J., & Huang, G. Q. (2019) Efficiency and robustness of weighted air transport networks. *Transport. Res. E*, **122**, 14–26.
10. Zou, Z., Xiao, Y., & Gao, J. (2013) Robustness analysis of urban transit network based on complex networks theory. *Kybernetes*, **42**, 383–399.
11. Wandelt, S., Frahm, K. M., & Ghaffari, M. (2022) From random failures to targeted attacks in network dismantling. *Reliab. Eng. Syst. Saf.*, **218**, 108146.
12. Grubesic, T. H., Murray, A. T., & Pahwa, A. (2008) Comparative approaches for assessing network vulnerability. *Int. Reg. Sci. Rev.*, **31**, 88–112.
13. Gallos, L. K., Cohen, R., Liljeros, F., Argyrakis, P., Bunde, A., & Havlin, S. (2006) Attack strategies on complex networks. In Computational Science–ICCS 2006: 6th International Conference, Reading, UK, May 28–31, 2006. *Proceedings, Part III 6*, Berlin Heidelberg: Springer, pp. 1048–1055.
14. Rodrigues, F. A. (2019) Network centrality: an introduction. *A Mathematical Modeling Approach from Nonlinear Dynamics to Complex Systems* (Macau, E. eds). Nonlinear Systems and Complexity, Springer, vol **22**, pp. 177–196.
15. Keng, Y. Y., Kwa, K. H., & McClain, C. (2020) Convex combinations of centrality measures. *J. Math. Sociol.*, **45**, 195–222.
16. Bellingeri, M., Cassi, D., & Vincenzi, S. (2014) Efficiency of attack strategies on complex model and real-world networks. *Physica A*, **414**, 174–180.
17. Yazdani, A., & Jeffrey, P. (2011) Complex network analysis of water distribution systems. *Chaos*, **21**, 016111.
18. Freeman, L. C. (1978) Centrality in social networks conceptual clarification. Soc. Netw., **1**, 215–239.
19. Holme, P., Kim, B. J., Yoon, C. N., & Han, S. K. (2002) Attack vulnerability of complex networks. *Phys. Rev. E*, **65**, 056109.

20. Iyer, S., Killingback, T., Sundaram, B., & Wang, Z. (2013) Attack robustness and centrality of complex networks. *PLoS One*, **8**, e59613.

21. Nguyen, Q., Cassi, D., & Bellingeri, M. (2020) New nodes attack strategies for real complex weighted networks. arXiv preprint arXiv:2008.02139.

22. Nie, T., Guo, Z., Zhao, K., & Lu, Z. M. (2015) New attack strategies for complex networks. *Physica A*, **424**, 248–253.

23. Wan, N., Zhan, F., & Cai, Z. (2011) A spatially weighted degree model for network vulnerability analysis. *Geo-spatial Inform. Sci.*, **14**, 274–281.

24. Zhang, S., Si, W., Qiu, T., & Cao, Q. (2020) Toward more effective centrality-based attacks on network topologies. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, pp. 1–6.

25. Cetinay, H., Devriendt, K., & Van Mieghem, P. (2018) Nodal vulnerability to targeted attacks in power grids. *Appl. Netw. Sci.*, **3**, 34.

26. Albert, R., Jeong, H., & Barabási, A. L. (2000) Error and attack tolerance of complex networks. *Nature*, **406**, 378–382.

27. Broder, A., Kumar, R., Maghoul, F., Raghavan, P., Rajagopalan, S., Stata, R., & Wiener, J. (2000) Graph structure in the web. *Comput. Netw.*, **33**, 309–320.

28. Chen, P. Y., & Hero, A. O. (2013) Node removal vulnerability of the largest component of a network. In *2013 IEEE Global Conference on Signal and Information Processing*, IEEE, pp. 587–590.

29. Chen, P. Y., & Hero, A. O. (2014) Assessing and safeguarding network resilience to nodal attacks. *IEEE Commun. Mag.*, **52**, 138–143.

30. Ugurlu, O. (2022) Comparative analysis of centrality measures for identifying critical nodes in complex networks. *J. Comput. Sci.*, **62**, 101738.

31. Abbasi, A. & Hossain, L. (2013) Hybrid centrality measures for binary and weighted networks. *Complex Networks*. Studies in Computational Intelligence, Berlin, Heidelberg: Springer, vol. **424**, pp. 1–7.

32. Fei, L., Mo, H., and Deng, Y. (2017) A new method to identify influential nodes based on combining existing centrality measures. *Mod. Phys. Lett. B*, **31**, 1750243.

33. Zhang, Y., Bao, Y., Zhao, S., Chen, J., & Tang, J. (2015) Identifying node importance by combining betweenness centrality and katz centrality. In 2015 *International Conference on Cloud Computing and Big Data (CCBD)*, IEEE, pp. 354–357.

34. Goldenberg, D. (2021) Social network analysis: from graph theory to applications with Python. arXiv preprint arXiv:2102.10014.

35. Freitas, S., Yang, D., Kumar, S., Tong, H., & Chau, D. H. (2022) Graph vulnerability and robustness: a survey. *IEEE Trans. Knowl. Data Eng.*, **35**, 5915–5934.

36. Nguyen, Q., Pham, H. D., Cassi, D., & Bellingeri, M. (2019) Conditional attack strategy for real-world complex networks. *Physica A*, **530**, 121561.

37. Barabási, A. L., & Bonabeau, E. (2003) Scale-free networks. *Sci. Am.*, **288**, 60–69.

38. Crucitti, P., Latora, V., & Marchiori, M. (2003) Efficiency of scale-free networks: error and attack tolerance. *Physica A*, **320**, 622–642.

39. Wu, J., Tan, S. Y., Liu, Z., Tan, Y. J., & Lu, X. (2017) Enhancing structural robustness of scale-free networks by information disturbance. *Sci. Rep.*, **7**, 1–13.

40. Gallos, L. K., & Argyrakis, P. (2007) Scale-free networks resistant to intentional attacks. *EPL (Europhys. Lett.)*, **80**, 58002.

41. Newman, M. E. (2001) Clustering and preferential attachment in growing networks. *Phys. Rev. E*, **64**, 025102.

42. Albert, R., Jeong, H., & Barabási, A. L. (1999) Diameter of the world-wide web. *Nature*, **401**, 130–131.

43. Brandes, U. (2001) A faster algorithm for betweenness centrality. *J. Math. Sociol.*, **25**, 163–177.

44. Divya, P. B., Lekha, D. S., Johnson, T. P., & Balakrishnan, K. (2022) Vulnerability of link-weighted complex networks in central attacks and fallback strategy. *Physica A*, **590**, 126667.

45. Lekha, D. S., & Balakrishnan, K. (2020) Central attacks in complex networks: arevisit with new fallback strategy. *Physica A: Statistical Mechanics and its Applications*, **549**, 124347.

46. Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S., & Herrmann, H. J. (2011) Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci.* USA, **108**, 3838–3841.
47. Ventresca, M., & Aleman, D. (2015) Network robustness versus multi-strategy sequential attack. *J. Complex Netw.*, **3**, 126–146.
48. Liashchynskyi, P., & Liashchynskyi, P. (2019) Grid search, random search, genetic algorithm: a big comparison for NAS. arXiv preprint arXiv:1912.06059.
49. Liu, C., Wei, Z., Huang, Y., & Zhang, H. (2014) An improved grid search algorithm for parameters optimization on SVM. *Appl. Mech. Mater.*, **644**, 96–100.