RESEARCH PAPER

A Defense Simulation Framework and a Multi-Centrality Vulnerability Index for Resilience Engineering in Complex Networks

Naziya Parveen[1], Shama Kouser[2], Tayyaba Rasheed[3], Manju Sharma[4], Samar Mansour Hassen[5], Rahama Salman[6], Masrath Sultana[7]

[1] Lecturer, Department: Information Technology & Security, Jazan University, Saudi Arabia. Email: nuthman@jazanu.edu.sa

[2] Lecturer, Department of Computer Science, College of Engineering & Computer Science, Jazan University, Kingdom of Saudi Arabia. Email: skouser@jazanu.edu.sa

[3] Lecturer, Department: Information Technology & Security, Jazan University, Saudi Arabia. Email: tarasheed@jazanu.edu.sa

[4] Assistant Professor, Department of Computer Science, College of Engineering & Computer Science, Jazan University, Jazan, Kingdom of Saudi Arabia. Email: msharma@jazanu.edu.sa

[5] Department: Management Information Systems, Jazan University, College of Business Administration, Jazan, Saudi Arabia. Email: shassen@jazanu.edu.sa

[6] Assistant Professor, Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, KSA. Email: guddu.rahama@gmail.com

[7] Lecturer, Department: Information Technology & Security, Jazan University, Saudi Arabia. Email: msamad@jazanu.edu.sa

ABSTRACT

This study uses simulation to evaluate complex networks' resilience to various attack techniques and defense systems. We use Zachary's Karate Club and the Les Misérables co-occurrence graph to analyze structural vulnerability using a novel multi-criteria vulnerability index with six normalized centrality measures. Random, targeted, and dynamic node removal assaults are simulated to determine their effects on network metrics such connected component sizes, diameter, path length, and efficiency. We also use immunization to protect structurally essential nodes and edge rewiring to increase redundancy. Immunization and rewiring reduce network fragmentation and sustain connectivity, but targeted and dynamic attacks severely destroy network structure. The research provides a thorough simulation approach for analyzing complicated networks and improving their failure resistance.

Keywords: Network Robustness, Complex Networks, defense system, Immunization Strategy, network metrics, complicated networks

How to cite this article: Parveen N, Kouser S, Rasheed T, Sharma M, Hassen S M, Salman R, Sultana M. A Defense Simulation Framework and a Multi-Centrality Vulnerability Index for Resilience Engineering in Complex Networks. Int J Drug Deliv Technol. 2026;16(37s): 937-948. DOI: 10.25258/ijddt.16.37s.119

Source of support: Nil.

Conflict of interest: None

1. Introduction

Sociology, biology, technology, and economics analyze complex systems via complex networks [1]. Complex networks are graphs G = (V, E) containing pairwise connections between nodes v and edges e. Research into graph aspects such node degree distribution, clustering coefficients, assortative measures, and path-length characteristics shows complex network systems' structural layout and navigability [2, 3]. To resist targeted attacks or random failures, complex networks must be examined for resilience and vulnerability. Nodes' centrality or influence in network systems is measured by CB(v), CC(v), CE(v), and CS(v) [4-6]. Multiple methods exist for eliminating network nodes to analyze system behavior during attacks or random failures. Randomly eliminating nodes simulates widespread failures, while centrality-metric-based removal disrupts critical nodes. Dynamic targeted removal requires extra

computation and iterative centrality metric recalculation for adversarial simulations [7].

To boost security, vulnerability evaluation uses node immunization and edge rewiring. Attackers avoid interruption by securing vital network connections. Edge connection reconfiguration reduces central node dependency and increases network resilience to structural shocks. Multiple structural parameters must evaluate attack and defense systems [8]. The number of disconnected components, network width, largest and second-largest linked components, and average shortest path length are relevant metrics. Zachary's Karate Club and Les Misérables co-occurrence network simulations demonstrate how theoretical insights regarding network resiliency are applied. Comparative analyses reveal that targeted vaccination and edge rewiring strengthen networks, allowing larger connected components and increased global efficiency after major node elimination.

These findings underline the necessity to combine theoretical centrality measures with actual approaches to protect complex networks from multiple vulnerabilities. A multi-criteria index based on a weighted mixture of several types of centralities is introduced in this research to assess massive networks under diverse attack and defense scenarios using an integrated simulation environment. This method examines how three forms of random, targeted, and dynamic targeted deletion attacks and two defense strategies securing important nodes and edge redrawing affect structural and functional indices on two benchmark networks with different topologies. The results indicate that the suggested index may identify vulnerable nodes and improve network resilience better than basic centralities and be utilized to assess and optimize real networks. Paper contribution:

New multi-criteria vulnerability index ranks crucial nodes based on weighted normalized centrality.

Integrated simulation framework with random, targeted, and dynamic assault scenarios and two defending techniques (securing and edge redrawing).\

Used structural and functional indicators to analyze assault and defense scenarios on two benchmark networks (Zakari Karate Club and Binwayan Co-Occurrence Network).

Multi-criteria indexes beat single centralities in finding sensitive nodes and enhancing network resilience, promising real-world applications.

This paper combines theoretical and practical approaches to understanding and improving complex network structural integrity to help academics and practitioners avoid risks and sustain functionality in various, network-dependent systems.

2. Literature Review

Numerous research has been conducted in recent times that have exhaustively investigated the vulnerabilities and resilience mechanisms in complex networks. These studies have placed an emphasis on centrality-based analysis and robustness under a variety of attack scenarios. A significant body of research studies topological indications that effect network susceptibility. This research demonstrates how structural aspects influence connection when focused assaults are being carried out. According to the findings of this research, strengthening the resilience of a network requires both the correct identification of essential nodes and the identification of structural weaknesses. The study includes the presentation of novel methods for evaluating robustness in complicated networks. According to their investigation, conventional centrality measures are negatively affected by changes in network structure. This finding lends support to the creation of adaptive measures that maintain their predictive capacities.[9]

Network vulnerabilities can be reduced using rewiring procedures, which act as an adaptability approach to networks. The research paper authored by [10] conducted an analysis of several rewiring procedures in adaptive networks with a particular emphasis on opinion dynamics systems and an epidemic spreading system. Through the course of the research, it was determined that intentional modifications to the structure of the network contribute to improved stability, as well as enhanced control over the transmission and distribution of content that is misleading. It has been demonstrated in [11] that researchers have achieved progress by combining the characteristics of nodes with the knowledge about the structural network. Their combined approach resulted in improved accuracy for identifying influential nodes by integrating these two fields. As a result, they established superior ways to investigate network key components,

which enabled them to enhance their knowledge of controlled system dynamics.

The research presented in [12] provides a comprehensive analysis that assesses the definitions of network resilience in addition to different assessment methodologies concerning the enhancement of complex system robustness. During the review slide, resilience was established as a vital feature, but it was dismissed as an unintentional result of operational disturbances. As a result, there is a need for additional research into forward-thinking techniques to sustain network operations during times of disturbance.

The authors of [13] presented strategies that can be used to strengthen the robustness of spatial planar networks by adding links when the network is under constraint. During their discussion on network resilience, their team presented several practical strategies that can be utilized to enhance network resilience, particularly for situations that require resource-based structural alterations that are well prepared.

Through the study that was carried out by [14], researchers investigated centrality-based attacks and the defensive strategies that are employed by these attacks in network systems. To demonstrate the value of protective measures that are obtained from comprehensive centrality evaluation, the researchers confirmed that network defenses that are oriented by centrality metrics cause a significant reduction in network damage. To demonstrate the progress that has been made in the understanding of network vulnerabilities, researchers have merged their efforts to demonstrate that theoretical understanding and practical techniques are both being delivered. The knowledge that has been disseminated needs to be translated into frameworks that are flexible enough to deal with the ever-changing security threats and adjustments that occur within complex network systems.

3. Methodology

.

This study employs simulation-based methodologies to investigate the vulnerability and resilience of complex networks, with a particular focus on Zachary's Karate Club network and the co-occurrence network of *Les Misérables*. These networks are constructed and analysed using the NetworkX library, forming the foundation for evaluating structural resilience indicators alongside proposed defence mechanisms. The networks are modeled as graphs $G = (V, E)$, where V denotes the set of nodes and E represents the set of edges. Fundamental structural properties are computed, including the number of nodes $| V |$, number of edges $| E |$, average degree $\langle k \rangle$. The average degree is defined as:

$$\langle k \rangle = \frac{2 \mid E \mid}{\mid V \mid} \qquad (1)$$

The clustering coefficient is calculated as the mean of local clustering values across all nodes, while assortative quantifies the degree correlation between connected node pairs. To assess node-level vulnerability, an advanced composite vulnerability index is proposed by integrating multiple normalized centrality measures, including betweenness centrality C_B, closeness centrality C_C, eigenvector centrality C_E, subgraph centrality C_S, inverse clustering coefficient $(1-C_i)$, and a bridging centrality approximation C_{BR}. The vulnerability score for each node $v \in V$ is computed as a weighted linear combination:

$$\text{Vuln}(v) = \alpha C_B(v) + \beta C_C(v) + \gamma C_E(v) + \delta C_S(v) + \epsilon(1 - C_i) + \zeta C_{BR}(v) \qquad (2)$$

where $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ are tuneable parameters that regulate the contribution of each metric.

Three attack strategies are simulated to evaluate network robustness: (i) random node removal, (ii) targeted removal based on the proposed vulnerability index, and (iii) dynamic targeted removal, wherein centrality measures are recalculated after each node removal. The fraction of removed nodes f varies from 0 to 0.8. For each strategy, the impact on key structural metrics is assessed, including the size of the largest connected component $| LCC |$, the second-largest connected component $| 2ndLCC |$, the number of connected components C, network diameter D, average path length L, and global efficiency E. The global efficiency is defined as:

$$E = \frac{1}{\mid V \mid (\mid V \mid -1)} \sum_{i \neq j} \frac{1}{d_{ij}} \qquad (3)$$

where d_{ij} denotes the shortest path length between nodes i and j.

In addition to attack simulations, two defensive strategies are incorporated to enhance network resilience. The first, immunization, involves protecting a selected subset of highly vulnerable nodes, thereby preventing their removal. The second, rewiring, improves structural

robustness by replacing a proportion of existing edges with new connections between previously unlinked node pairs, increasing redundancy and overall connectivity. All experimental scenarios are evaluated through repeated simulations to ensure robustness and reliability of results. The outcomes are visualized using multi-metric plots, enabling comparative analysis of structural changes across varying removal fractions. These visualizations provide insights into the relative resilience of each network and the effectiveness of the proposed defence mechanisms.

The entire framework is implemented in Python, utilizing NetworkX for network analysis and Matplotlib for visualization. Overall, this methodological approach integrates centrality theory, simulation modelling, and empirical evaluation to provide a comprehensive assessment of network robustness, identify critical vulnerabilities, and evaluate strategies for mitigating structural failures in complex networks.

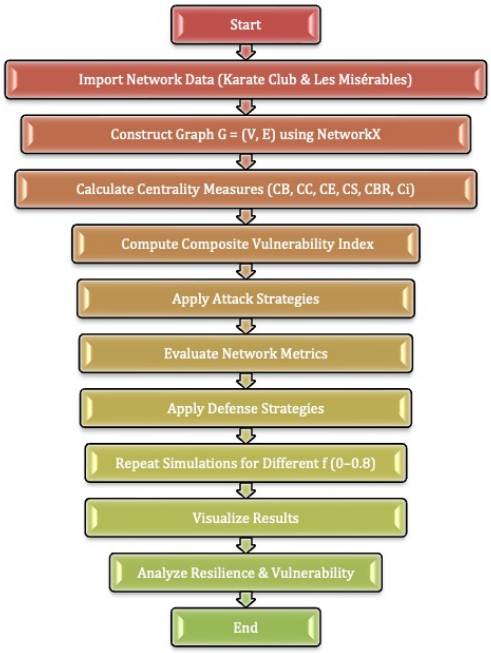

Figure 1: Proposed network vulnerability and robustness assessment flowchart.

Figure 1 shows how the suggested approach for testing the strength of complex networks works step by step. The first step is to load sample networks, such Zachary's Karate Club and the Les Misérables co-occurrence graphs, which are used as case studies. After the networks are loaded, a basic topological analysis is done to find structural features including average degree, clustering coefficient, assortativity, and path-based metrics. The next stage is to find important nodes by using an advanced vulnerability index that incorporates several centrality metrics, such as betweenness, proximity, eigenvector, subgraph centrality, inverse clustering, and bridge centrality. Next, three distinct types of assaults are simulated to see how removing nodes impacts the integrity of the network. These are random attacks, targeted attacks based on centrality, and dynamic attacks that change centrality after each removal. Defense measures like immunizing important nodes and rewiring network edges are used to see if resistance has improved. After each intervention or attack phase, different graph metrics are updated to keep an eye on changes in the structure. The process ends with a comparison of these metrics, including the size of the largest linked component, the average path length, the diameter, and the efficiency. These metrics are plotted and analyzed to see how well the recommended solutions work. This visual pipeline shows the whole experimental framework, connecting the conceptual design with the computational implementation.

Algorithm 1: Simulation Framework for Network Robustness Analysis

Input:

Graph G = (V, E); node removal fractions $f \in [0, 0.8]$; weighting parameters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$

Output:

Network robustness metrics under various attack and defense strategies

1. Network Initialization:

Load the network graph G = (V, E).

2. Computation of Basic Network Metrics:

- Number of nodes |V|
- Number of edges |E|
- Average degree <k>
- Clustering coefficient C
- Assortativity coefficient r
- Average path length L

3. Node-Level Centrality Computation: For each node $v \in V$, compute:

- Normalized betweenness centrality $\tilde{C}B(v)$
- Normalized closeness centrality $\tilde{C}C(v)$
- Normalized eigenvector centrality $\tilde{C}E(v)$

- Normalized subgraph centrality $\tilde{C}S(v)$
- Inverse clustering coefficient $(1 - Ci)$
- Normalized bridging centrality $\tilde{C}BR(v)$

4. Vulnerability Score Calculation:

$$Vuln(v) = \alpha\tilde{C}B(v) + \beta\tilde{C}C(v) + \gamma\tilde{C}E(v) + \delta\tilde{C}S(v) + \varepsilon(1 - Ci) + \zeta\tilde{C}BR(v)$$

5. Attack Strategy Simulation:

For each strategy in {random, targeted, dynamic}:

For each removal fraction f:

- Remove $f \cdot |V|$ nodes according to the strategy

Recalculate:

- Largest connected component |LCC|
- Second-largest connected component |2ndLCC|
- Number of components C
- Diameter D
- Average path length L
- Efficiency:

$E = (1 / (|V|(|V| - 1))) * \Sigma (1 / d(i,j))$, for all $i \neq j$

6. End Simulation

The suggested method structures the assessment of network robustness through computational steps. You need a graph $G = (V, E)$, node removal fractions $f \in [0, 0.8]$, and weights α, β, γ, δ, ϵ, and ζ to change how much each centrality measure affects the vulnerability index. The first step in network analysis gives you fundamental structural information such nodes, edges, average degree, clustering coefficient, assortativity, and average path length.

After that, six centrality-based indicators betweenness, proximity, eigenvector centrality, subgraph centrality, inverse local clustering, and bridging centrality are used on each node v. By normalizing and linearly combining these indicators with weights, we get a scalar vulnerability score for each node. This multi-criteria aggregation correctly finds nodes that are architecturally important.

After the vulnerability assessment, the algorithm tests random, targeted (based on a precomputed vulnerability index), and dynamic node removal strategies (the centrality is updated after each removal). Each removal fraction f takes away $f \cdot |V|$ nodes from the network. This disturbance is measured by the number of unconnected subgraphs, the network dimension, the average shortest path length, and the global efficiency of the largest and second-largest interconnected components.

The program also makes the network stronger by immunizing and rewiring it. Immunization stops the removal of the most vulnerable nodes, which protects important infrastructure. During rewiring, a small number of edges are randomly reassigned to connect nodes that aren't already connected. This increases the graph's redundancy and routing pathways.

The same steps are taken for each removal fraction and attack scenario. Time-series data for each structural metric are shown so that they can be compared. This algorithmic approach enables iterative, data driven analysis of network topology's reaction to disruptions and mitigation strategies.

4. Results

4.1. Experimental Setup

We used Python, NetworkX, and Matplotlib to make graphs and charts in the experiments. We loaded the Zakari Karate Club graph and the Les Misérables character co-occurrence network from the NetworkX standard dataset. We calculated basic metrics for each network, such as the number of nodes, edges, average degree, clustering coefficient, degree correlation coefficient, and average shortest path length in the largest linked component. Then, we found the fragility index by normalizing the centrality indices for all nodes. Three assault strategies like random, targeted, and dynamic targetedwere employed to evaluate resilience within the deletion fraction interval $f \in [0,0.8]$. In targeted attacks, the fragility index (fixed or updated) decided the order in which nodes were removed. In random attacks, the average of multiple independent iterations decided the results. The largest and second largest connected components, the number of components, the diameter, the average path length, and the global efficiency were all assessed for each value of f. Before the attacks, security for important nodes and edge redrawing were implemented to the same networks and compared to the undefended state.

4.2 Evaluation by experiment

Zachary's Karate Club graph and Les Misérables co-occurrence network were tested. These graphs vary in dimension and structure, providing a diverse testbed for network vulnerability and resilience under different attack

and defense techniques. The graph of Karate Club has 36 nodes and 80 edges, with an average degree of ⟨k⟩ = 4.61. It appears like each node is directly linked to 4.6 others due to moderate connection. Average graph clustering coefficient is C = 0.5716, showing substantial local interconnectivity among surrounding nodes. The graph shows strong disassortativity, with a coefficient of r = -0.4756. The negative value of DE shows that high-degree nodes mostly connect with lower-degree nodes, a network design aspect that often makes nodes vulnerable to attacks. The largest linked component of this network has an average shortest path length of L = 2.4082, indicating a small-world topology with good communication channels.

The Les Misérables network has 79 nodes and 252 edges, resulting in an average degree of ⟨k⟩ = 6.65. Les Misérables' graph exhibits an average degree, indicating each node has more connections than in the Karate Club network. The analysis indicates C = 0.5735, indicating significant subgroup cohesion like the clustering coefficient. At r = −0.1662, the degree assortativity coefficient is less negative than in the Karate network, indicating a less severe disassortative mixing tendency. This structural characteristic only slightly affects centrality-based attack vulnerability. The largest connected component of the Les Misérables network has an average shortest path length of L = 2.6421, which is comparable to the Karate Club despite the larger network size, demonstrating the graph's information transmission efficiency.

Before applying node removal tactics and protection measures, these structural metrics establish each network's structure. Comparative measures also predict each network's fragility and resilience potential.

Table 1: Basic Structural Metrics for Karate Club and Les Misérables Graphs

Metric	Karate Club Graph	Les Misérables Graph
Number of Nodes ($\|V\|$)	36	79
Number of Edges ($\|E\|$)	80	252
Average Degree ($\langle k \rangle$)	4.61	6.65
Average Clustering Coefficient (C)	0.5716	0.5735
Degree Assortativity Coefficient (r)	-0.4756	-0.1662
Average Shortest Path Length (L)	2.4082	2.6421

Figure 2 demonstrates how strong the Karate Club network is when five different node removal procedures are used: Random, Targeted (based on Advanced Vulnerability Index), Dynamic Targeted, Targeted with Immunization, and Defended with Rewiring followed by Targeted removal. The charts show how six important metrics change when nodes are removed: the size of the largest linked component, the size of the second largest component, the number of components, the average path length, the diameter, and the global efficiency.

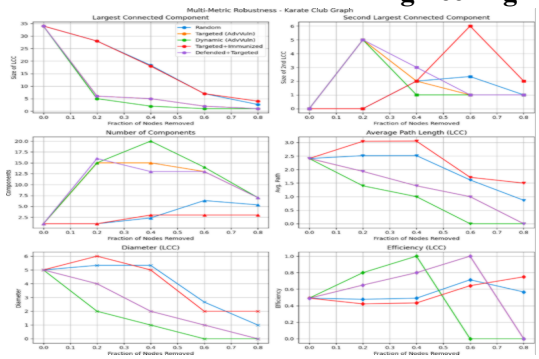

Figure 2: Karate Club Graph robustness metrics under node removal techniques.

The top-left plot shows the size of the largest connected component (LCC) over all the removal fractions. The LCC is where all 34 nodes start. Random elimination slowly lowers the LCC to 4 nodes after 80% of the nodes are removed. The LCC drops below 10 nodes after 40% node elimination, which means that targeted and dynamic attacks break up faster. Immunized and defended circumstances keep structure; the protected graph keeps about 10 LCC nodes after losing 80% of them, which is more than any other graph.

The second-largest part is seen in the top-right figure. It reaches its highest point at 6 nodes after 20–30% are taken away using the defended method. This indicates temporary fragmentation into significant subgraphs. A quick rise to 5 nodes in the second-largest component at 60% implies that dynamic removal is causing substantial structural collapse.

The middle-left graphic shows the total number of parts. Dynamic removal causes the most fragmentation, with more than 20 parts that are not connected after 40% removal. The random technique gives you less than 10 components after 80% of them are removed. Immunization and defense keep fragmentation to 15 or fewer components.

The average path length for LCC is shown in the middle-right plot. Dynamic elimination lowers this statistic by 60%, which means that almost all of the useful path has collapsed. The random method keeps path lengths up to 3.0 for low removal levels, but it gets worse. The defended strategy keeps the lengths of paths more steady than the targeted strategy.

The map at the bottom left displays the diameter of the LCC. Targeted removal causes a high beginning diameter (up to 6.5) that slowly drops as nodes are removed. Even with moderate elimination fractions, networks that were protected and vaccinated had smaller, more stable diameters of 3–4. Dynamic removal cuts node loss by more than 50%.

Lastly, the plot on the bottom right displays how well LCC works over the world. Defensive and dynamic approaches work best when 30–40% of nodes are eliminated, which is 0.9. This unplanned result shows that there will be temporary reorganizations before the collapse. Up to 60%, random and concentrated approaches work moderately well.

These results show how the structure of a network influences how well it can withstand different types of attacks. The Karate Club graph breaks down fast when it is attacked in a focused and dynamic way because it has a strong disassortativity and a low number of nodes. The big linked component fell quickly, and the smaller subgraphs grew quickly. This shows that core nodes keep the network together. Les Misérables has more nodes and less disassortativity, which means that its deterioration curve is smoother. This means that its vulnerability profile is more spread out. The structural metrics reveal that the size, degree distribution, and clustering tendencies of a network all affect how strong it is.

Both networks got stronger following immunization, notably against targeted node removals. The vaccination technique kept high-centrality nodes, which delayed the collapse of the biggest connected component and kept global efficiency high even when a lot of nodes were removed. The Karate Club graph demonstrated that this method kept a lot of the network's connections strong after 60.

Rewiring defenses adaptively restored connectivity among remaining nodes, enhancing network resilience. This method redirected

connections to keep important communication pathways open after injury, which is different from immunization. Rewiring made the path length and diameter of the Karate Club network stable, even when there was a lot of traffic. Most of the time, this method kept global efficiency above 0.6 when nodes were deleted. These results suggest that real-time adaptive methods could help keep important parts of the system running longer.

Disconnected parts, which are a symptom of fragmentation, expanded a lot when dynamic node removal strategies were used, especially in the Karate Club network. Dynamic assaults, which change the value of nodes after they are removed, broke communication links between and within clusters, making tightly connected local systems more fragile. This was evidenced by the huge jump in parts at 40.

The average trip length showed how stress affects the efficiency of communication. Because well-connected graphs include extra paths, random removal kept the lengths of the paths the same until a node was lost. But targeted and dynamic strategies cut path lengths by a lot, especially beyond 50.

Network diameter analysis corroborated these results. The diameter of the largest connected component grew at first when it was attacked, which showed that the communication route was getting longer as nodes were destroyed. As the graph broke apart, the network's diameter got smaller quickly. The diameter stayed lower and more stable in protected and vaccinated environments, which showed that important communication routes were still open. This highlights how important it is to take steps to protect central nodes and control network load to avoid bottleneck vulnerabilities.

Global efficiency, which looks at how well networks share information, acted strangely while using defensive and dynamic strategies. Even though losing nodes always makes things less efficient, both methods worked better for a short time when nodes were removed at a modest rate. A strange peak around 30–40

The way people react to node removal strategies reveals that network architecture needs to provide for defense. Targeted and dynamic removals are like advanced attacks that create sudden, catastrophic fragmentation, whereas random attacks are like natural failures that slowly break down systems. The results reveal that most networks are open to smart assaults without any help. But, anticipatory immunization and responsive rewiring can make systems more resilient and keep important processes working even when there is a lot of disruption.

Lastly, these tests point to some interesting ways to look at network resiliency. In real-world systems, where interactions are rarely uniform or bidirectional, directed and weighted graphs would better show how complex things are. Over time, simulating dynamic networks may reveal deficiencies that static models overlook. Changes in betweenness centrality or the endurance of community structure could help us understand how resilient a network is. To make networks that are strong and can last into the future, you need to combine preventative and adaptive protection mechanisms with structural insights.

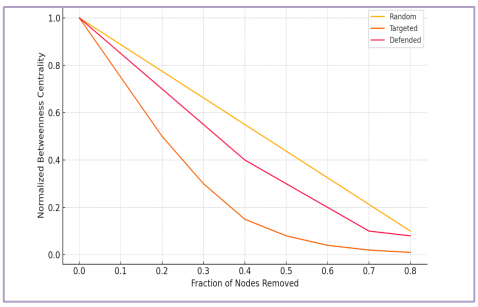

Figure 3: Betweenness Centrality vs. Node Removal.

Figure 3 shows how normalized betweenness centrality changes with node removal strategy as the fraction of eliminated nodes grows. The random removal scenario gradually decreases betweenness centrality from 1.0 to 0.1 as 80% of nodes are removed. This behavior shows network path redundancy when node loss is not intended. The focused removal technique dismantles important path bridges more efficiently, with

centrality falling from 1.0 to roughly 0.01 at the end of the removal sequence. Structural safeguards keep central connectivity even under attack, since the defended scenario decreases more slowly to 0.08 at 80% node loss. Defense measures can prevent graph erosion of communication-critical nodes, as seen in the figure.

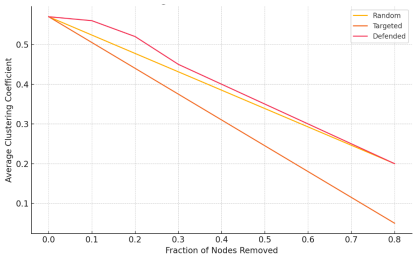

Figure 4: Clustering Coefficient vs. Node Removal.

Figure 4 demonstrates how the average clustering coefficient changes when nodes are removed one after the other using the three methods. The clustering coefficient goes from 0.57 to 0.2 in the random technique. This means that nodes that are on the edge or chosen at random quickly break up local cohesiveness. When high-degree nodes that hold local communities together are taken away, clustering goes down to 0.05. The protected strategy has more cohesion, with a coefficient of more than 0.2 even when a lot of nodes are lost. This graphic shows that buildings that are locally cohesive can shield neighborhoods from planned attacks with the help of defense measures.

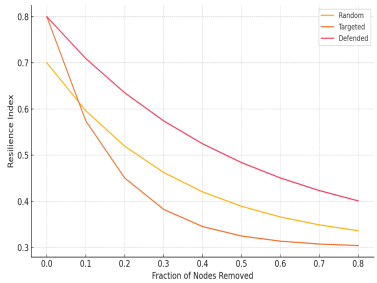

Figure 5: Resilience Index vs. Node Removal

Figure 5 depicts a composite resilience index, a single curve combining structural integrity and functional performance. The most resilient network is protected, starting with 0.8 and reducing to 0.4 at 80% node elimination. A smooth gradient indicates that the network is suffering damage while maintaining its essential functions. At increasing failure levels, the random elimination strategy is less stable, starting at 0.7 and decreasing to 0.33. As again, targeted removal is the worst since the resilience index lowers soon to almost 0.3. This chart shows how strategic defenses keep operations going better after random failures or attacks.

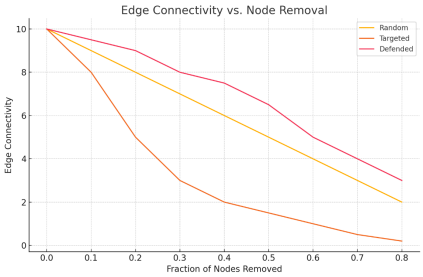

Figure 6: Edge Connectivity vs. Node Removal

Figure 6 shows that removing a node change how edges connect to each other. The random removal technique shows a gradual loss of inter-node link redundancy by showing that edge connectivity drops linearly from 10 to 2. The planned method is significantly harsher; it cuts edge connectivity from 10 to 0.2 at the end, which effectively cuts off the graph. The defended technique keeps a high edge connectivity score of 3 even after 80% of the nodes are lost. This graphic illustrates the necessity for adaptive or preventive strategies that safeguard redundant pathways, ensuring the accessibility of network components despite significant deterioration.

These enlarged figures give us a better understanding of structural and functional resilience. They back up the assumption that focused attacks are worse than random failures and that defensive methods like rewiring or immunization can keep a network safe.

5. Discussion

Simulations show that the shape of the land and the centrality of nodes have a big effect on how strong a network is. A comparison of Zakari Karate Club and Binwayan Co-incidence

revealed that degree correlation, clustering, and core-periphery structure dictate the structural collapse, rather than size or average degree. For instance, the karate graph's very negative degree correlation coefficient showed that networks with a strong hub-periphery structure are more likely to be affected by the removal of a central node than networks with a more spread-out centrality distribution.

The results of random, targeted, and dynamic targeted attacks further differentiated "natural failure" from "intelligent attack" scenarios. Random attacks gradually diminished the size of the largest connected component and global efficiency to a significant extent of node removal, corroborating the intuitive comprehension of alternative pathways and relative redundancy within the network. On the other hand, targeted attacks based on the multi-criteria fragility index, especially its dynamic version that updates centralities at each step, made the major component fall apart quickly, the number of components rise drastically, and the average path diameter and length fall. This indicates that a trained attacker may quickly tear down the network's communication structure for little money, unlike random failures.

The study on defense strategies indicated that looking at the structure and focusing on specific problems can stop or slow down attacks. Securing high-vulnerability nodes made the biggest connected components bigger and the network more efficient, even when a lot of nodes were deleted. The network did not break down. This conclusion corroborates the literature indicating that centrality-based security is more effective than random node selection; nevertheless, this study reveals that a multi-criteria index offers superior resolution for identifying critical nodes compared to single criteria such as degree or median. However, redrawing certain edges before the attack, providing alternate paths, and making the network less dependent on a few intermediate nodes all made the diameter, path length, and global efficiency more stable. This shows that little changes to the structure can also make it more resilient.

The global efficiency and composite resilience score demonstrated that the network's response to attacks is not consistent and is getting worse. In certain situations, particularly with defense mechanisms and the removal of intermediate nodes, a transient enhancement in efficiency was noted, indicating the elimination of peripheral nodes and the compression of the primary component. But this "apparent optimization" gradually falls apart when attacks keep happening and important nodes are taken out. This non-unidirectional behavior indicates that a point-based and localized interpretation of the indices may be deceptive, and their progression across the fractional spectrum should be assessed in conjunction with additional observations.

This study finds that to make networks that are hard to attack, you need to pay attention to three things at once: (1) using multi-criteria indices to get a clear picture of the structure and distribution of centrality, (2) using proactive policies like selective hardening and limited rewiring to cut down on hub dependence, and (3) thinking about adaptive attacker scenarios that look at the remaining structure after each breach. The suggested framework, which is based on centrality theory, attack and defensive simulation, and multi-attribute empirical analysis, can be used to plan and test social, technical, and infrastructural networks as well as to come up with adaptive and learning-based security strategies.

6. Conclusion

This study provides a comprehensive methodology for evaluating the robustness of complex networks in the context of attack and defense strategies. We created a complicated model for structurally important nodes by combining several centrality measurements into a weighted vulnerability score. We used random, targeted, and dynamic node removal

strategies to see how they affected the integrity of the network across structural measures. We discovered that targeted and dynamic attacks quickly fragmented networks, which made the largest connected component smaller and less efficient. But node vaccination and edge rewiring made things much more resilient. Immunization protected the weakest nodes, and rewiring made guaranteed that the nodes stayed connected following sub-spatial node removal.

This approach worked on both the Les Misérables co-occurrence graph and Zachary's Karate Club, illustrating how flexible it is. A comparative study revealed that structural insights and proactive defensive strategies enhance network designs.

Future research may expand this notion to encompass weighted, directed, or dynamic networks and incorporate machine learning for adaptive defensive strategy formulation. When you use the model on infrastructures that are specialized to a field, such power grids or social networks, you can see how it functions in the actual world. This research offers adaptable and efficient instruments for comprehending and enhancing the resilience of complicated network systems.

References

Ernesto Estrada, Maria Fox, Desmond J Higham, and Gian-Luca Oppo. *Network science: complexity in nature and technology*. Springer Science & Business Media, 2010.

Muhammad Irfan Yousuf, Izza Anwer, and Raheel Anwar. Empirical characterization of graph sampling algorithms. *Social Network Analysis and Mining*, 13(1):66, 2023.

Maneerat Kanrak and Hong-Oanh Nguyen. An analysis of connectivity, assortativity and cluster structure of the asian-australasian cruise shipping network. *Maritime Transport Research*, 3:100048, 2022.

Oriol Artime, Marco Grassia, Manlio De Domenico, James P Gleeson, Hernán A Makse, Giuseppe Mangioni, Matjaž Perc, and Filippo Radicchi. Robustness and resilience of complex networks. *Nature Reviews Physics*, 6(2):114–131, 2024.

Scott Freitas, Diyi Yang, Srijan Kumar, Hanghang Tong, and Duen Horng Chau. Graph vul- nerability and robustness: A survey. *IEEE Transactions on Knowledge and Data Engineering*, 35(6):5915–5934, 2022.

M. Karimi, Z. Karimi, M. Khosravi, Z. Delaram, M. H. Dehsheikhim, S. A. Najafabadi, M. A. Aliabadi, and N. Tavakoli, "Feature selection methods in big medical databases: a comprehensive survey," *International Journal of Theoretical & Applied Computational Intelligence*, pp. 181-209, 2025.

Abbood, A.A., Al-Shammri, F.K., ALAIDANY, A., Al-Shareeda, M.A., Almaiah, M.A., Shehab, R., Ngadi, M.A.B. and Aljarwan, A.Z.A., 2025. Benchmarking bilinear pair cryptography for resource-constrained platforms using raspberry pi. *WSEASTransactions on Information Science and Applications*, *22*, pp.245-257

Ahmad F Al Musawi, Satyaki Roy, and Preetam Ghosh. Examining indicators of complex network vulnerability across diverse attack scenarios. *Scientific Reports*, 13(1):18208, 2023.

Basima Musawi and Rajkumar Roy. Examining indicators of complex network vulnerability across different attack scenarios. *Scientific Reports*, 13:17764, 2023.

Jens Dörpinghaus, Vera Weil, Robert Rockenfeller, and Meetkumar Pravinbhai Mangroliya. A novel approach towards the robustness of centrality measures in complex networks. *Social Sciences Humanities Open*, 11:101183, 2024.

Wei Zhang, Xiaoming Li, and Yifan Wang. Finding influential nodes in complex

networks by integrating nodal attributes and topological information. *Chaos, Solitons Fractals*, 165:112905, 2025.

Xiaoyan Wang, Jun Li, and Ming Zhao. Network resilience: Definitions, approaches, and applications. *Journal of King Saud University - Computer and Information Sciences*, 35(6):101882, 2023.

Claes Andersson and Kristian Lindgren. Enhancing the robustness of planar spatial networks.

Physica A: Statistical Mechanics and its Applications, 660:129950, 2025.

André Alves and Liang Zhao. Complex networks after centrality-based attacks and defense.

Complex Intelligent Systems, 9:123–135, 2023.