

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

Imam Qasim Mousa¹, Kheirolah Rahsepar Fard¹

¹Department of Computer Engineering and Information Technology, University of Qom, Ghadir boulevard, Qom, Iran

Abstract

This study proposes a simulation model to investigate the resilience of complex networks against different types of attacks and evaluate the effectiveness of related defense strategies. For this purpose, two reference networks, including the social network of Zachary Karate Club and the co-occurrence network of characters in the novel "Les Misérables", were selected as evaluation platforms. For the evaluation of the structural fragility of the network, a new multidimensional index is proposed, which is defined by the combination of six normalized centrality values. Afterward, the impact of various attacks, including random node removal, structural importance-based attacks, and dynamic attacks, is simulated, and the effects of these attacks on the basic properties of the network, including the size of the largest connected component, the diameter of the network, the average path length, and the efficiency of the network, are evaluated. Moreover, the effectiveness of two defensive strategies, including the protection strategy and the edge reconfiguration strategy, is also evaluated for the preservation of the network from the effects of the attack and the maintenance of the level of connectivity at an optimal state. It is observed from the results obtained through the simulation of the attacks that the impact of the targeted attack and the dynamic attack is more detrimental to the integrity and coherence of the network compared to the impact of the other attacks. Moreover, the application of the defensive strategies can save the network from the effects of the attack and can maintain the level of connectivity at an optimal state.

Keywords: Edge Rewiring, Network Robustness, Vulnerability Index, Complex Networks, Node Removal, Immunization Strategy, Centrality Measures, NetworkX, Graph Theory
Keywords.

1. Introduction

It is recognized that complex networks are one of the important tools used in the analysis of complex systems. As discussed in references [1,2], complex networks have been widely used in the study of various social networks in the field of sociology, biological networks in the field of biology, technology networks, and economic networks. It is general knowledge that the networks are usually described by a graph $G=(V,E)$, where the nodes $v \in V$ represent the system components and the edges $e \in E$ represent the relationship between the system components. The analysis of the structural properties of the graph is used to obtain useful information about the system networks in terms of the system accessibility and the system structure itself.[3,4]

Moreover, due to the nature of complex networks that can be attacked, a comprehensive analysis of the robustness of the complex networks is necessary. Four centralization measures $C_B(v)$, $C_C(v)$, $C_E(v)$ and $C_S(v)$ help identify the centrality or influential potential of nodes within network systems [5].

Multiple methods exist for removing network nodes to understand how the system behaves when subject to attacks or random failure situations. The process of randomly removing nodes models widespread node failures whereas targeted removal strategies built from centrality metrics aims at disrupting the most central nodes. The dynamic targeted removal process integrates iterative centrality metric

recalculation for adversarial simulations while demanding additional processing resources [6].

Advancing security through vulnerability assessment utilizes two defensive strategies referred to as node immunization and edge rewiring. The identification and protection of vital network connection nodes constitute immunization through which attackers seek defense against disruption during attacks. Alternative defense strategies through rewiring modify edge connections to reduce the dependency on few central nodes which enhances network resilience to structural disruptions. To precisely evaluate the function of attacking and defensive plans in networks, it is important to measure a number of structural elements [7-9].

These set of indicators are often assessed through metrics such as the size of the biggest and second linked components and the series of some isolated clusters. The presumable parameters of the assigned should be determined by the network and the length of the nodes. Conversely, the simulation-inclined research particularly, on studies on networks like the Zachary's Karate Club and the occurrence of the individuals relating to the number Les Misérables, can create room for conceptual models in relation to the network steadiness which can be translated into tangible and well observable findings. Comparisons of various occurrences indicate that network that can strengthened utilizing methods like the targeted protection of the projected key nodes and edge rearrangement to maintain structural degradation and show maximum steadiness. These set of networks can maintain higher fractions of linked components and a maximum efficacy, even when the node deletion can occur on a very high scale. Generally, the findings show that depending on a single metric is insufficient. Instead, integrating centrality-inclined metrics with structural reinforcing plans can assist in the improvement of the resilience of difficult networks to threats and vulnerabilities [10].

In this study, a multi-criteria index based on a weighted combination of several types of centralities is introduced and the behavior of complex networks under different attack and defense scenarios is analyzed in the form of an integrated simulation framework.

This framework combines three different types of attack scenarios, including random deletion, targeted attack, and dynamic attack, with two defense strategies, namely, protecting critical nodes and reconfiguring the edge structure. Then, the impact of these combinations on a set of structural and performance indices in two reference networks with different topologies is analyzed. The results indicate that the proposed index for designing attacks and defenses is more effective than using only simple centrality measures in more accurate identification of sensitive nodes and increasing network resilience. Therefore, it can be used as a practical tool for analyzing and optimizing real networks. The contribution of the paper is:

- Introducing a multi-criteria vulnerability index based on a weighted combination of several normalized centrality criteria for ranking critical nodes.
- Providing an integrated simulation framework that combines three random, targeted, and dynamic targeted attack scenarios with two defense strategies of securing and edge redrawing.
- Systematically evaluating attack and defense scenarios on two benchmark networks with different topologies (Zakari Karate Club and Binwayan Co-Occurrence Network) using several structural and functional indicators.

- Demonstrating that the use of a multi-criteria index performs better than single centralities in identifying sensitive nodes and enhancing the structural resilience of the network and has the potential to be applied to real networks.

Thus, the present research provides a relatively complete framework for the study and improvement of the structural integrity of complex networks. At the same time, the present framework brings the theoretical discussions closer to the practical aspects, allowing researchers and practitioners to use a set of efficient tools for the reduction of risks and the maintenance of efficiency in various kinds of complex networks.

2. Related Work

In recent years, there has been considerable interest among researchers to address these issues more seriously and to provide solutions to improve resilience within complex networks. Most of these studies have concentrated on the role played by centrality measures and have analyzed how these networks respond to different types of attacks. For example, it has been recommended that by [13] that the topological features of a network serve as a critical function to determine its links under targeted assaults. In this context, it has been emphasized that to improve resilience within a network, it is not sufficient to simply “make the overall structure stronger,” but it is also necessary to identify nodes more accurately and to uncover hidden weaknesses within the network structure. In this context, some studies, like the one presented by [14], have aimed to provide new ways to measure resilience within these networks. In addition to this, the findings provided by this group of studies reveal that although centrality measures can be highly efficient under steady-state conditions where there are no changes to the network structure, these measures tend to be highly ineffective under conditions where there are changes to the network.

From another point of view, the concept of network reconfiguration or reconfiguration has been introduced as a powerful technique to deal with the problem of vulnerabilities. In the paper [15], the performance of a set of edge reconfiguration strategies for adaptive networks is examined. According to the results of the paper, along with the improvement of stability, the desired degree of control over processes such as the spread of disease or the spread of misinformation is achieved. The results of the paper again highlight the importance of “informed intervention” for the development of the structure of the network. Moreover, the combination of the information obtained from the analysis of the feature data of the nodes with the information obtained from the analysis of the general network structure has led to important achievements over the last few years. According to the paper [16], the combination of these two approaches has enabled the more accurate determination of the influential nodes of the network and the better understanding of the behavior of the critical part of the network. The above-mentioned combination of approaches has opened new avenues for the study of the behavior of the complex system.

The paper [17] presents different perspectives on the concept of resilience. In the paper, different methods of evaluating the robustness of the complex system are compared. However, the most important part of the paper is that the resilience is considered not only as a random phenomenon but also as a feature that is subject to the planning process. In addition, [18] has also proposed practical solutions to improve the resilience of a spatial network, especially by introducing new links under certain conditions. The above research indicates that even under resource constraints, it is possible to improve network stability to a great extent by introducing changes that have been computed. Finally, the research [19] also discusses attacks that occur based on criteria related to centrality, as well as defense strategies, and indicates that when

decisions for defense strategies are made based on criteria related to centrality, damage to the network is reduced to a great extent. This again emphasizes the importance of a detailed understanding of network structure while making decisions related to defense strategies. Overall, it is indicated by this research that understanding the vulnerability of complex networks is not just limited to theoretical discussions, but it is also possible to develop approaches that can easily translate theoretical knowledge into practical solutions to make these networks efficient and effective under changing conditions.

3. Methodology

In this study, simulation-based approaches are used to investigate the vulnerability of complex networks. For this purpose, two co-occurrence networks, Zachary's Karate Club and Les Misérables, are used. These networks are loaded using the NetworkX library and used as a platform for running experiments, in which both structural resilience indices are measured and resilience enhancement strategies are evaluated and compared. The networks exist as graphs named $G = (V, E)$ which show V as nodes and E as edges within the structure.

The computation of fundamental structural network features includes measuring $|V|$ and $|E|$ together with $\langle k \rangle$, C , r and L . The definition of average degree states:

$$\langle k \rangle = \frac{2|E|}{|V|} \quad (1)$$

The clustering coefficient is derived as the average of local clustering values, while assortative measures the correlation between degrees of connected nodes.

To assess the vulnerability of nodes, an advanced vulnerability index is proposed by combining multiple normalized centrality measures: betweenness C_B , closeness C_C , eigenvector centrality C_E , subgraph centrality C_S , inverse clustering coefficient $1 - C_i$, and a bridging centrality approximation C_{BR} . The combined vulnerability score for each node $v \in V$ is calculated using a weighted sum:

$$\text{Vuln}(v) = \alpha \tilde{C}_B(v) + \beta \tilde{C}_C(v) + \gamma \tilde{C}_E(v) + \delta \tilde{C}_S(v) + \epsilon(1 - C_i) + \zeta \tilde{C}_{BR}(v)$$

(2)

where $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ are tunable weights controlling the contribution of each metric. Three attack strategies are simulated: random removal, targeted removal using the advanced vulnerability index, and dynamic targeted removal where centrality scores are updated after each node removal. The fraction of removed nodes f varies from 0 to 0.8. In each of the strategies examined, the traces of changes can be clearly seen in the main network indicators; indicators such as the size of the largest connected component $|LCC|$, the size of the second largest component $|2ndLCC|$, the total number of components C , the network diameter D , the average path length L and finally the overall network efficiency E . In this framework, network efficiency is defined as follows:

$$E = \frac{1}{|V|(|V| - 1)} \sum_{i \neq j} \frac{1}{d_{ij}} \quad (2)$$

In this definition, d_{ij} represents the shortest path between two nodes i and j in the network. In addition to simulating different attack scenarios, two defensive

approaches are also considered: hardening and rewiring. In the hardening method, a number of nodes that are most vulnerable are selected and protected in such a way that they remain outside the deletion cycle. In contrast, rewiring seeks to strengthen the network structure by removing some of the existing edges and creating new links between nodes that were not previously connected; an approach that improves the level of connectivity and stability of the network by increasing redundancy.

In order to analyze each scenario, simulation happens through a series of steps and iterations for each scenario to be evaluated. This analysis happens through a series of multi-indicator graphs, which show changes to structural indices within the network during the simulation process. This makes it easier to compare the resilience of each network and assess the efficacy of each proposed defense strategy. This model has been written totally in Python and uses the network library to examine and Matplotlib to show the results. this model serves a detailed method to network robustness by combining methods in relation to the centrality, analysis and simulation. This not only identifies weaknesses and areas where vulnerability exists but simulates the effects of destructive behavior within the network and ultimately identifies which strategies are most effective to improve resilience within complex networks.

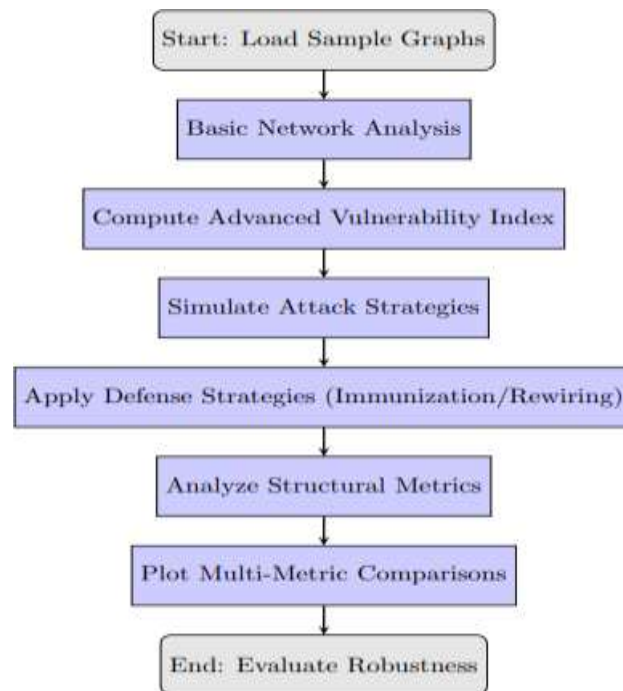


Figure 1. overview of the steps of the proposed method for assessing the vulnerability and stability of complex networks

The procedure starts by choosing and loading a number of sample networks; in this case, two co-occurrence networks, including the famous Zachary Karate Club and the novel *Les Misérables*, are selected as examples. The next step involves an initial topological analysis performed in the first step to obtain basic features of the network structure. The second step involves the computation of an advanced vulnerability measure, which incorporates different centrality measures such as betweenness, closeness, eigenvector, subgraph, reverse clustering, and bridging centrality. This step allows for the more accurate detection and identification of sensitive and influential nodes within the network. The third stage includes the simulation of three distinct attack scenario with the computation and updating the centrality of the basic

measures and their core values after each deletion stage. The defensive plans are then performed to enhance the resilience and the choice and safeguarding of the key nodes and the reconfiguration of edges to enhance the network connection and the structural idleness. The last step includes the addition and plotting of network metrics to observe the changes and efficiency of the projected plans and the related flexibility of the networks. The final step involves the comparative analysis and plotting of the relative effectiveness and the relative resilience of the networks using indicators such as the size of the largest connected component, average path length, network diameter, and efficiency. The connection between the conceptual idea and the computational implementation is thus clearly established.

Algorithm 1 Simulation Framework for Network Robustness Analysis

```

1: Input: Graph  $G = (V, E)$ , removal fractions  $f \in [0, 0.8]$ , weights  $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ 
2: Output: Metrics after attack and defense simulation
3: Load network  $G$ 
4: Compute basic metrics:  $|V|, |E|, \langle k \rangle, C, r, L$ 
5: for each node  $v \in V$  do
6:   Compute normalized:
     • Betweenness  $\tilde{C}_B(v)$ 
     • Closeness  $\tilde{C}_C(v)$ 
     • Eigenvector centrality  $\tilde{C}_E(v)$ 
     • Subgraph centrality  $\tilde{C}_S(v)$ 
     • Inverse clustering  $1 - C_i$ 
     • Bridging centrality  $\tilde{C}_{BR}(v)$ 
7:   Compute vulnerability score:
     
$$\text{Vuln}(v) = \alpha \tilde{C}_B(v) + \beta \tilde{C}_C(v) + \gamma \tilde{C}_E(v) + \delta \tilde{C}_S(v) + \epsilon(1 - C_i) + \zeta \tilde{C}_{BR}(v)$$

8: end for
9: for each strategy in {random, targeted, dynamic} do
10:  for each removal fraction  $f$  do
11:    Remove  $f \cdot |V|$  nodes according to strategy
12:    Recalculate:
     • Largest component  $|LCC|$ 
     • Second-largest component  $|2ndLCC|$ 
     • Number of components  $C$ 
     • Diameter  $D$ 
     • Average path length  $L$ 
     • Efficiency:  $E = \frac{1}{|V|(|V|-1)} \sum_{i \neq j} \frac{1}{d_{ij}}$ 
13:  end for
14: end for

```

- 15: Apply immunization by protecting top vulnerable nodes
 - 16: Apply rewiring by replacing selected edges with new random links
 - 17: Repeat simulation and metric analysis
 - 18: Plot multi-metric comparison results
-

The proposed algorithm is designed to assess the robustness of the network in a systematic and step-by-step manner. The work starts from receiving the graph $G=(V,E)$ and at the same time, an interval for the node removal fraction in the range $f \in [0,0.8]$ and weighting coefficients $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ are defined; coefficients that determine what contribution each centrality criterion will have in calculating the final vulnerability index.

In the first step, a general survey of the network structure is performed to obtain an initial picture of its state; in this step, items such as the number of nodes and edges, average degree, clustering coefficient, community structure and average path length are extracted, and this basic picture helps to better interpret the network behavior in the following steps. Then, each node is evaluated separately with six different centrality criteria.

The criteria, each of which looks at the importance of the node from a specific angle, range from its role in the traffic paths to its impact on the entire network. Next, the values obtained are first normalized to be comparable. Then, they are linearly combined using the specified weighting coefficients. The output of this step is a single score for the vulnerability of each node, which indicates how much the removal of that node can harm the network structure. The advantage of this method is that the identification of critical nodes is not limited to a specific criterion and ultimately a more realistic and complete picture of the importance of the nodes is provided.

After the vulnerability level of the nodes is determined, the algorithm enters the attack simulation stage. In this section, three different scenarios are considered: in the first case, nodes are removed from the network randomly; in the second case, the removal is done purposefully and based on the vulnerability ranking; And in the third case, a dynamic approach is used in which, after each elimination step, the centrality criteria are recalculated and the decisions are updated. For each value of the elimination fraction f , a corresponding number of nodes, equal to $f \cdot |V|$, are eliminated from the network so that the gradual process of structural degradation is visible.

The implications of the above-mentioned disturbances are measured based on a series of structural parameters; the size of the largest and second-largest connected components, the number of disconnected subgraphs, the diameter of the network, the average length of the shortest paths, and the overall efficiency. These parameters enable the precise monitoring of the changes in the network and the measurement of the stability of the network based on various types of attacks.

Apart from the various types of attack scenarios that the algorithm takes into account, there are two defense mechanisms that the algorithm takes into consideration to evaluate the effectiveness of the networks in enhancing the overall resilience of the networks. In the protection mechanism, the nodes that are most vulnerable according to the calculated parameters are not removed from the network. This means that the nodes are maintained in the network as part of the overall structure of the network. On the other hand, the redrawing mechanism is based on the incorporation of a certain number of edges between the nodes that were not initially connected to one another. This is done to enhance the redundancy of

the overall structure of the network. All the above steps are carried out over a range of removal values and all the attack scenarios. The final results of the algorithm will be the temporal data that will be used to plot the trend of the changes that occur in the networks. Overall, the above algorithm is a useful tool that helps understand the implications of various types of disturbances that occur in complex networks and the effectiveness of the defense mechanisms in mitigating the overall impact of the above-mentioned disturbances.

4. Results

4.1. Experimental Setup

The experiments were carried out using the Python language with the NetworkX library used for the analysis of the networks and Matplotlib used for the plotting. Two benchmark networks were used; one is the graph of the Zakari Karate Club, and the other is the character co-occurrence network from the novel "Les Misérables." The networks were loaded from the NetworkX standard dataset. For the networks, the basic features were calculated, including the number of nodes and edges, average degree, clustering coefficient, degree correlation coefficient, and average shortest path length in the largest connected component.

Then, the proposed fragility index was obtained based on the normalized combination of several centrality measures for all nodes. To evaluate the resilience, three attack strategies of random deletion, targeted deletion, and dynamic targeted deletion were applied in the deletion fraction interval $f \in [0, 0.8]$. In the random attack, the results were reported based on the average of several independent iterations, while in the targeted attacks the order of node removal was determined based on the fragility index (fixed or updated). For each value of f , the size of the largest and second connected components, the number of components, the diameter, the average path length, and the global efficiency were recorded. The defense strategies of securing critical nodes and redrawing part of the edges were also applied to the same networks before executing the attacks and compared with the undefended condition.

4.2. Experimental evaluation

The empirical evaluation of this research is conducted on two widely used benchmark networks: the Zachary Karate Club graph and the Les Misérables character co-occurrence network. These two networks have distinct differences in terms of size, density, and connectivity patterns, and are therefore good candidates to better measure the network behavior against different attack and defense scenarios, from the perspective of vulnerability and resilience.

The Karate Club network comprises of 34 nodes and 78 edges, and its average degree is $\langle k \rangle = 4.59$; that is, each node is linked to around four to five other nodes on normal. The average clustering coefficient of the network is also $C = 0.5706$, representing that local links in this network are potent and neighbors are often linked to each other. Conversely, the network is not totally the same in terms of extent. The value of $r = -0.4756$ for the degree relationship to indicate that the nodes with maximum degrees tend to be linked to nodes with low degrees. This sort of structure can make communication more effective, but often makes the network more susceptible to projected attacks, and it can remove a huge part of the links. In terms of distance, the total length of the shortest path in the largest link component is around $L = 2.4082$; meaning that most of the nodes are linked in a few short steps, and the network shows the small universal property to a good degree.

Contrastively, the Les Misérables network is greater and denser. It contains 77 nodes as well as 254 edges, and its normal extent is $\langle k \rangle = 6.60$; This means that each of the nodes is linked to a larger number of the other nodes and broadly has more intense interactions than the known Karate network. Its cluster coefficient is $C = 0.5731$. However, the degree relationship in this network is around $r = -0.1652$; it is still negative. This means that the possibility of high-degree to low-degree association is weaker in but its heterogeneousness is much less severe than in the Karate Club. The usual shortest track length in the main connected component of this network is similarly $L = 2.6411$; though the network is broader, this value is also acceptable to indicate that information distribution through the network is still effective.

In general, this initial review of structural indicators may assist to have a clear image of the topological state of the networks and to implement the node removal scenarios and resistance approaches. This major comparison indicates how flexible each network maybe to the fragmentation of its inherent features, and conversely, what capacity and possibility it has to add to the structural disruptions.

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

Metric	Karate Club Graph	Les Misérables Graph
Number of Nodes ($ V $)	34	77
Number of Edges ($ E $)	78	254
Average Degree ($\langle k \rangle$)	4.59	6.60
Average Clustering Coefficient (C)	0.5706	0.5731
Degree Assortativity Coefficient (r)	-0.4756	-0.1652
Average Shortest Path Length (L)	2.4082	2.6411

Figure 2 displays how the Karate Club network seeks to respond to five distinct node elimination plans to include random elimination and dynamic programmed removal, and a rewiring-inclined defense strategy. In the above figure, the modifications in six main structural indicators, viz: the size of the largest and second linked components, the normal path length, the total efficacy, and the network are shown as a role of the fraction of eliminated nodes, in a clear sense, comparing the potency and resilience of the network under each strategy.

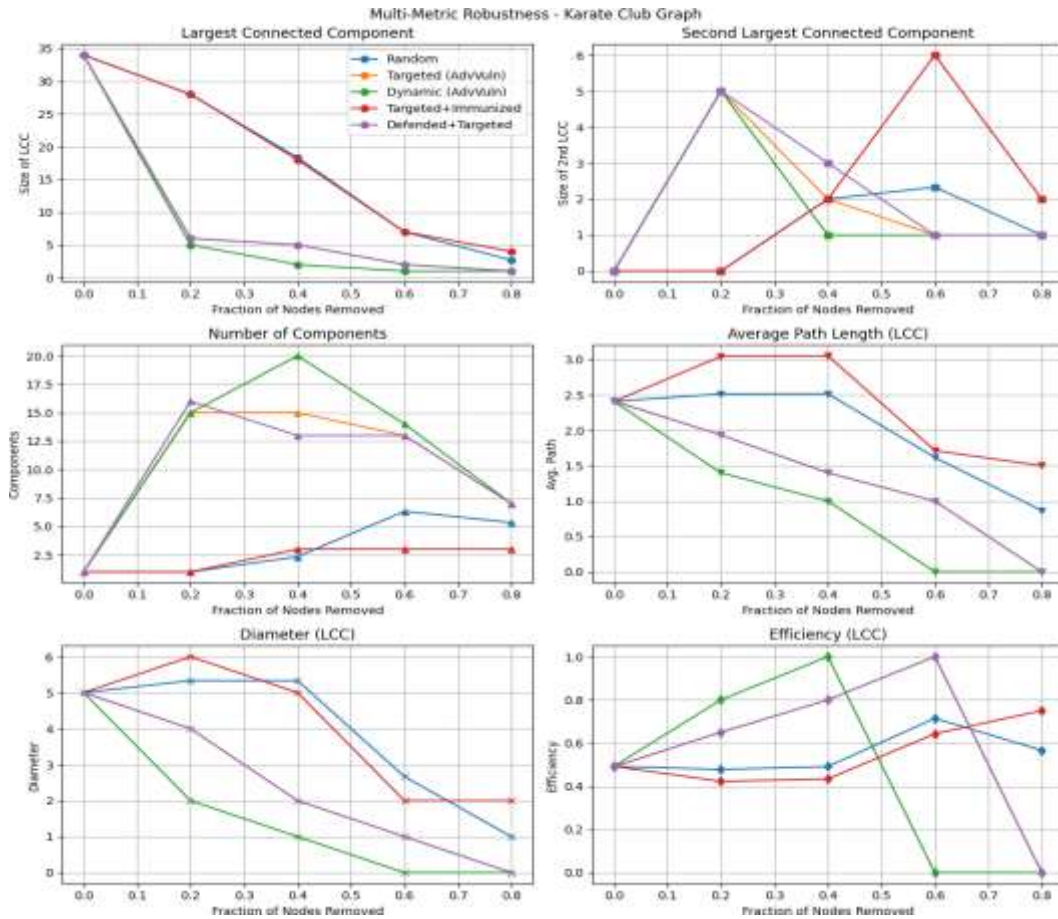


Figure 2: Sturdiness metrics under different node elimination approaches for the Karate Club Graph.

The graphs in Figure 2 display in detail how the Karate Club network responds to dissimilar node elimination scenarios. The top-left graph shows the size of the largest connected component (LCC); in the initial state, all 34 nodes are inside the LCC. When random deletions occur, this component gradually shrinks, reaching about 4 nodes after 80% of the nodes are removed. However, in targeted attacks—and especially dynamic attacks—the network collapse occurs much faster, with the LCC size falling to less than 10 nodes after only 40% of the nodes are removed. In contrast, the security/defense approaches fare better, and the defended scenario can still maintain about 10 nodes in the largest connected component even after 80% of the nodes are removed.

The top-right graph examines the behavior of the second largest component. In the defended case, between about 20 and 30% node removal, the size of this component increases to about 6 nodes, which could be indicative of a transient phase, where the network is divided into a few relatively important subgraphs for a while. On the other hand, dynamic removal produces a more abrupt jump in the second component, and around 60% removal, its size reaches about 5 nodes, a pattern that suggests a more aggressive and severe decomposition of the structure. The middle-left graph also shows the total number of

components: dynamic removal produces the most fragmentation, with more than 20 separate components formed by removing 40% of the nodes. Random removal is milder, and even at 80% removal, the number of components remains below 10. In security and defense scenarios, the network is less fragmented and the number of components is controlled even at high deletion percentages, usually below 15.

The middle-right graph shows the average path length within the largest connected component. In dynamic removal, this indicator virtually reaches zero as 60% node deletion is approached; meaning, in random removal, the path length is still considerably high in the early levels to almost 3, but it can decrease as removals continue. In these potential intervals, the defended scenario indicates greater steadiness and maintains a more unified communication approach that potential attacks. The bottom-left graph affirms similar difference: in targeted removal which reaches around 6.5, however, it can decrease as node removals continue. In a safe and defended network, the diameter is often smaller and steadier, and it eventually remains around 3-4 even at modest removal units. Flexible deletion is also the most destructive and after passing around 50% removal, the diameter practically heads to zero.

Finally, the bottom-right graph indicates the total efficacy modifications of the largest linked component. Interestingly in dynamic removal, the network efficacy may reach high values close to 0.9 for some time which is within the range of around 30-40% node removal. This addition is perhaps connected to some sort of temporary rearrangement of the other paths before the last collapse. But in along the path, about 60% removal a sharp and remarkable drop takes place.

Generally, the findings show that the resilience of any network is dependent more on its structure. The Karate Club network, is the smaller and highly heterogeneous and faster when attacks are eminent, which highlights the fact that the network relies on a few central nodes; the largest connected component (LCC) and the addition in the number of the subgraphs displays this reliance. Conversely, the, the results show that the Les Misérables network, because of its greater and more unified distribution of connections, it experiences a smoother and slowly collapse, which seems that the vulnerabilities are distributed evenly. From this assertion, the robustness of a particular network can be determined by the size and other factors such as clustering patterns, degree distribution, and the location of central nodes. When the central nodes are protected, the LCC collapse will take place later and the network will maintain an acceptable stage of function, but in the Karate Club network, this impact seems noticeable and a significant portion of links is kept after around 60% of the node deletion. In addition, the rewiring-inclined defense with some adaptive reconfiguration of links often takes resilience a step forward, as a result of the complete function and to remain replicable such as the path length as well as the diameter in a steadier play a major performance and can maintain above about 0.6 for a large part of the deletion procedure. This general picture indicates that flexible and adaptive defenses can be genuinely decisive, especially for such sensitive instance in the networks and prevent swift degradation of network throughout.

The average pathway length assists to perceive more exactly how a network keeps the losses its links under huge stress.

However, in beset attacks and especially in the dynamic removal, these options may disappear swiftly and perhaps after 50% of the node removals, the average length may drop

dramatically and as well, all meaningful and consistent communication paths and the potential communication format will collapse.

The results with regards to the diameter of the network may also reinforce this assertion. However, it occurs as if the network is attempting to maintain the links with the fewer items and the links because it becomes more stretched. But as the removal keeps on decreasing rapidly, the network may become disjointed into a tiny and more isolated parts, and there will be no more single network with a meaningful diameter. In other related defended scenarios, the diameter often remains at a lower and more steady values, to indicate that the major communication paths are kept safely and that the defensive intervention will have a safeguarded communications ways and load from communicating on a much constraint points and forming crucial blockages.

The overall network routine behaviour may be interesting. In a natural form, it would be expected that the performance may reduce as the nodes are removed, but in the defended scenarios and even in dynamic deletion, a partial increase in the routine is noted at different levels of removal of about 10-40%). This often happens through the removal of some ineffective links; the network may become more compacted for a short time and the data flow on the other paths is more aligned and effective. If the deletion continues, the network will finally enter a serious decline stage.

These behavioural variations show that defensive strategies are critical issues in the design of proposed network and management which can be seen as marginal issues. Random removals can be similar to the natural faults and often cause slow degradation whereas the flexible attacks may replicate intelligent threats that can cause failures. However, the use of proactive defensive plans like the protection of crucial nodes and modification of network structure can assist in the increment of network resilience to maintain crucial roles and stop structural collapse.

The result of this study similarly outlines new space for additional research in the entity of network resilience. This can provide a better perception of the actual systems, because the connections remain constant and the association are not always two-way. It is also of special concern to study dynamic networks that can modify over time. When the network is developing or and are not well-detected in static models. Additionally, the use of complementary indicators is central to social structures that can increase the precision of resilience examination.

Lastly, if practical and adaptive protection devices are intended based on an accurate perception of network structure, we can move to attain stable and resilient option that is not against specific threats but again with different sorts of threats.

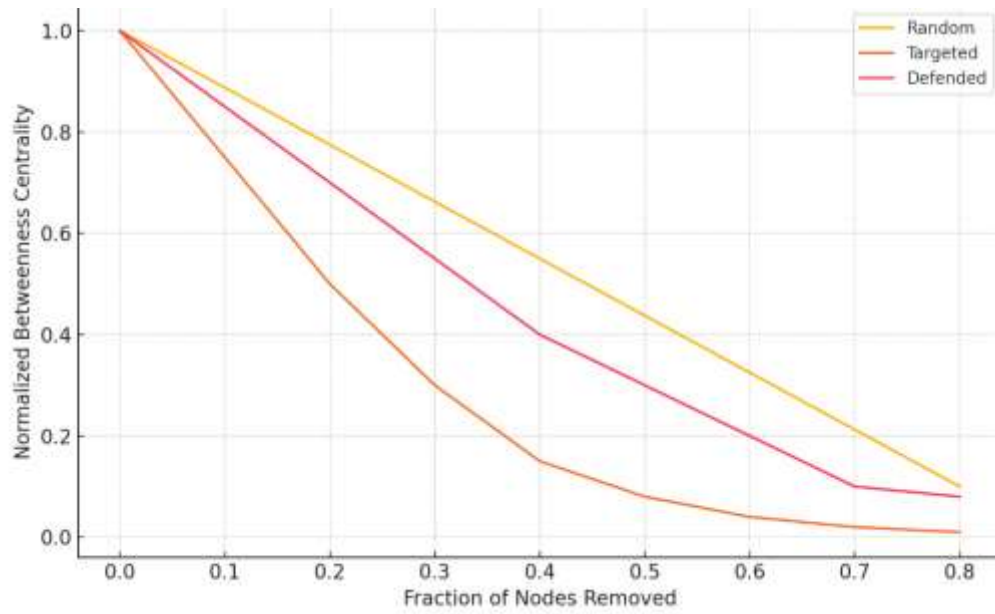


Figure 3: Betweenness Centrality vs. Node Removal.

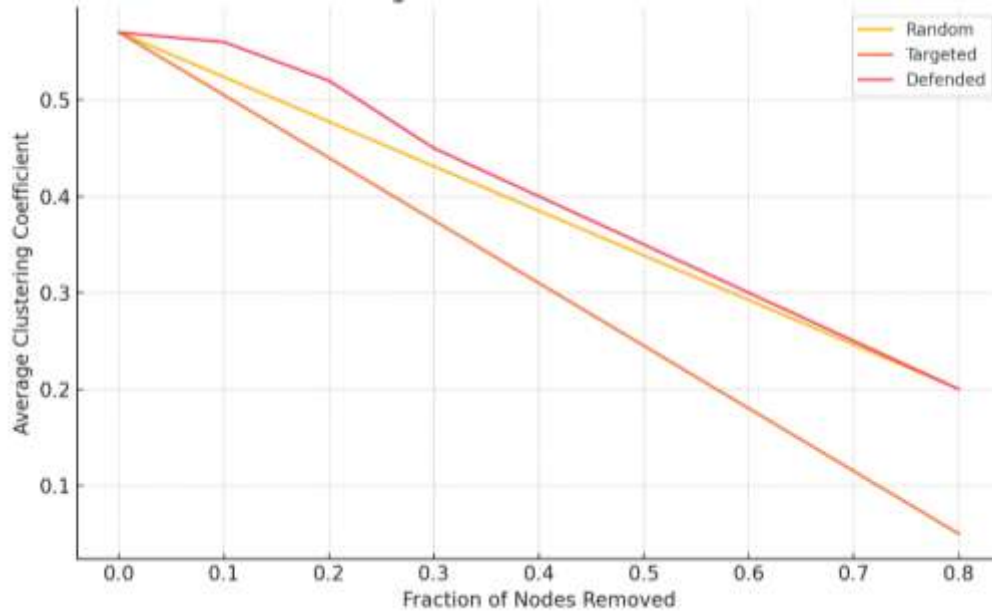


Figure 4: Clustering Coefficient vs. Node Removal.

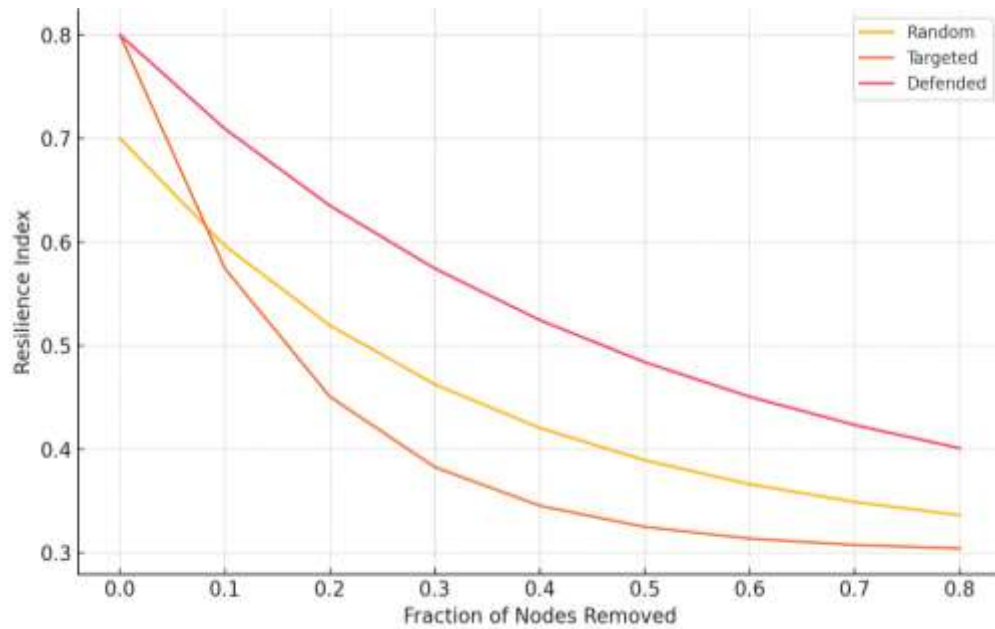


Figure 5: Resilience Index vs. Node Removal

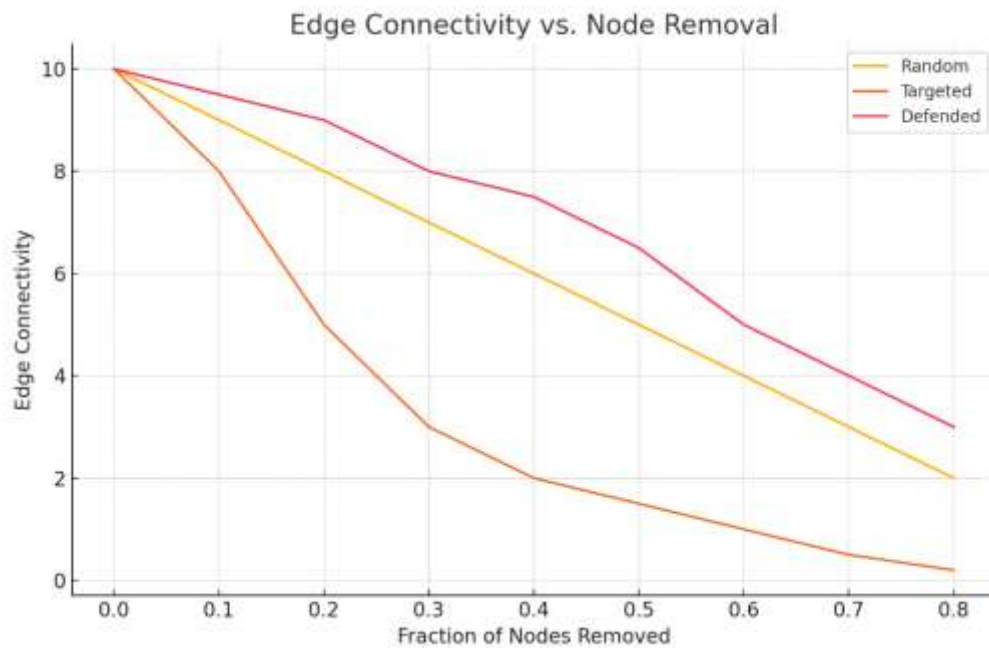


Figure 6: Edge Connectivity vs. Node Removal

Figure 3 shows the possible modifications in normalized betweenness centrality under three distinct scenarios of random elimination, defended state and targeted elimination and to

indicate the variations in network behaviour in every scenario. In random removal, the reduction in betweenness centrality is belated and nearly the same; with around 80% of nodes eliminated, the value of this index possible drop from 1.0 to about 0.1. occurs when the nodes are eliminated without any priority, but the information will be maintained by reliance on some options path for a while and the restraint of communication ways may happen slowly.

In contrast, beset removal contains stern effect on the network. Here betweenness centrality may drop to quickly approach around 0.01 at the end of the whole process. In this sense the behaviour can make sense owing to this plan that can remove the exact nodes that seems to act as essential bridge and the key intermediate points in the communication arena. This shows that defensive measures can affect the function of the failure rate of some sensitive nodes and hold a minimal communication flow in the network.

Figure 4 demonstrates how the normal cluster coefficient acts as nodes are slowly removed. In the other random removal scenario, this value brings drop from 0.57 to around 0.2 that shows the node are eliminated elliptically, the local unity of the network slowly weakens. The possible reduction can be seen as something very fast and destructive and it may result to coefficient drops to around 0.05; due to exactly the highly linked nodes and in contrast a protected network experiences can decline and despite the broad deletion of nodes, to maintain a cluster coefficient above 0.2. this means that defensive options can preserve the consistency of the network's neighbourhoods and even during purposeful deletions.

In Figure 5, a compound measure is assigned that concurrently represents the functional and structural aspects of the projected network to show the network resilience. The findings display that the defensive stage performs best around 0.8 and reduces to around 0.4 even with the deletion of nearly 80% of the nodes. This little reduction indicates that the network is susceptible to damage. The case of targeted deletion has the sternest impact on the network, to reduce the value of the resilience index to 0.3 from the onset. Figure 6 indicates the modifications in the edge connectivity as the ratio of node removal increases. The case of random deletion increases. The case of similar deletion almost near in linear from 10 to around 2. However, the removal of targeted deletion indicates the edge connectivity is reduced much more sternly to about 0.2.

In the protected scenario, the circumstances are favourable to the extensive node deletion, the edge connectivity remains about 3. This finding shows that the defensive and adaptive intercessions, to maintain the optional paths, and can better serve the network and continuity in crucial circumstances. Generally, these graphs clearly indicate the clear show how the network resilience can change from a functional and structural perspective and affirm the major conclusion of the study.

5. Discussion

Replication results show that the resilience of networks is dependent broadly on their topological structure and how vital (centrality is divided among nodes. A comparison of the two popular networks of Binwayan Co-incidence and Zakari Karate Club exhibited that designs of clustering, degree correlation, clustering, and core-periphery structure play a firm role in how the major structure slowly failed. Specifically, the strongly negative value of the extent relationship coefficient in the Karate graph indicated that networks with such structure

hub-periphery to the targeted deletion of central nodes than networks with centrality dispersal.

The results of arbitrary, targeted and flexible targeted attacks also exposed a clear variation between the natural failure and the intelligent attack situations. In the potential random attack, the global efficacy slowly reduced to a relatively maximum fraction of node removal, which is reliable in the perception of the existence of options and relative redundancy in the potential network. In contrast, beset attacks reliant on the multi-criteria fragility index. This will update the centralities of each stage that led to the swift collapse of the basic part and a sudden decrease in the number of diameter and length of the paths.

The study of defense approaches indicated that the integration of structural evaluation of the targeted intercession can essentially reduce the impact of the attacks. Saving the nodes with maximum susceptibility scores resulted in higher connected part sizes and universal efficacy being maintained at high levels of removal to the defenseless state and the procedure of network decomposition was reduced. This finding is in consonance with the prior literature that suggests centrality-inclined security is more efficient than the random node choice; but, in this work, it was indicated that the usage of a multi-criteria index offers higher resolution for the identification of critical nodes than a single criterion. Conversely, redrawing some edges before the attack through the addition of alternative paths and reduce the reliance of network on a limited number of intermediate nodes to a dedicative diameter, global efficacy, and path length to indicate the lightweight structural changes in improving resilience.

The behavior of indicators like the universal efficacy and the composite resilience index indicated that the networks response to attacks is not uniform. In some situations, the presence of the defense at intermediate levels of the node removal and the compression of the major component provides way to total collapse as attacks continue and the key nodes are removed. This nonlinear behavior suggests that if we examine the metrics only at a few points and locally, we may get a wrong impression; because a metric may show a large drop in part of the path but become more stable later, or vice versa. For this reason, it is better to analyze the changes in the metrics over the entire interval of the deletion fraction and along with other structural and functional metrics to obtain a more accurate picture of the network state. Overall, the findings of this study emphasize that to design attack-resistant networks, we must simultaneously consider several points: first, to understand the network structure and distribution of centralities well with a set of complementary metrics, second, to use preventive strategies such as selective hardening and limited rewiring to avoid the network becoming overly dependent on a few vulnerable hubs, and third, to take adaptive attacker scenarios seriously; An attacker who, after each elimination step, re-examines the remaining network and intelligently selects new targets. Consequently, the proposed model that combines the centrality theory and the defense simulation as well as empirical analysis of different features can be applied to design and assess infrastructure, technological and social networks for the growth of adptive and even learning-inclined defense approaches in future research.

6. Conclusion

This study offers a relatively detailed model for the assessment of the robustness of difficult networks against different defense and attack approaches. By applying the precisely accurate measures to structurally identify critical nodes, and through the simulation of node

elimination in three distinct ways viz; dynamic, random and targeted, the impact of disruption on network integrity was evaluated with different measures. The result demonstrated that the dynamic and targeted attacks have the highest possibility to break the network function to degrade swiftly. Conversely, the process can increase the network's resilience; and harden provided there is better safeguard of sensitive nodes and rewiring with additional protection for sensitive nodes. Execution of this approach on two genuine networks, the Zachary Karate Club network and Pessimistic Personality Co-occurrence Network, demonstrated that this model works well on various sorts of networks and the utilization of structural analysis and proactive defense methods typically results in the potent network design. The model can be extended to weighted, and dynamic networks with the use of machine learning procedures for better protection planning. It can also be tried for practical networks like the power grids or social networks to clearly understand the real applicability of this approach. The projected model has the possibility to be extended to directed and dynamic network. Machine learning methods can be used to design and schedule adaptive defenses. If this approach is tested on real infrastructures such as power grids or social networks, a clearer and more accurate picture of its effectiveness and practical application will be obtained.

References

- [1] Ernesto Estrada, Maria Fox, Desmond J Higham, and Gian-Luca Oppo. Network science: complexity in nature and technology. Springer Science & Business Media, 2010.
- [2] Muhammad Irfan Yousuf, Izza Anwer, and Raheel Anwar. Empirical characterization of graph sampling algorithms. *Social Network Analysis and Mining*, 13(1):66, 2023.
- [3] 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.
- [4] M. Aliabadi, M. Karimi, Z. Karimi, and M. Fard, (2025), "The Effect of Photoplethysmography Signal Denoising on Compression Quality," *Iranian Journal of Electrical & Electronic Engineering*, vol. 21, no. 1.
- [5] M. Emadi, M. Karimi, and F. Davoudi, (2023), "A Review on Examination Methods of Types of Working Memory and Cerebral Cortex in EEG Signals," *Majlesi Journal of Telecommunication Devices*, vol. 12, no. 3.
- [6] S. S. Seyed Abolghasemi, M. Emadi, and M. Karimi, (2024), "Accuracy Improvement of Breast Tumor Detection based on Dimension Reduction in the Spatial and Edge Features and Edge Structure in the Image," *Majlesi Journal of Electrical Engineering*, vol. 18, no. 1, pp. 33-44.
- [7] 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.
- [8] A. Rehman, M. Harouni, F. Zogh, T. Saba, M. Karimi, and G. Jeon, (2023), "Detection of Lung Tumors in CT Scan Images using Convolutional Neural Networks," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, pp.769-777.
- [9] Scott Freitas, Diyi Yang, Srijan Kumar, Hanghang Tong, and Duen Horng Chau. Graph vulnerability and robustness: A survey. *IEEE Transactions on Knowledge and Data*

- Engineering, 35(6):5915–5934, 2022.
- [10] 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.
 - [11] 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
 - [12] 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.
 - [13] Basima Musawi and Rajkumar Roy. Examining indicators of complex network vulnerability across different attack scenarios. *Scientific Reports*, 13:17764, 2023.
 - [14] 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.
 - [15] 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.
 - [16] 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.
 - [17] Claes Andersson and Kristian Lindgren. Enhancing the robustness of planar spatial networks. *Physica A: Statistical Mechanics and its Applications*, 660:129950, 2025.
 - [18] 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.
 - [19] Alaidany, A.A. and Lakizadeh, A., 2025. Improving the Accuracy of Cancer Driver Gene Identification based on Dimensionality Reduction Using Deep AutoEncoders. *International Journal of Intelligent Engineering & Systems*, 18(9).rks after centrality-based attacks and defense.