Assignment 3: Network robustness

Network Analysis

Delaram Doroudgarian
5881909

Seyedeh Aida Atarzade Hosseini
6936800

Academic Year 2024/2025

Introduction

This report presents a three-part analysis on the robustness of complex networks under various node removal strategies. The aim is to study how the removal of critical nodes affects the connectivity of the network, focusing on the size of the largest connected component (Giant Component).

1 Attacks on a Synthetic Graph

Graph Description

We generate a synthetic scale-free network using the Barabási–Albert (BA) model with 1000 nodes, where each new node connects to 3 existing nodes.

Attack Strategies

The following node removal strategies are implemented:

- **Random Attack**: Nodes are removed randomly.
- **Target Attack**: Nodes with highest degrees are removed first.
- **Betweenness Attack**: Nodes with highest betweenness centrality are removed first.
- **Closeness Attack**: Nodes with highest closeness centrality are removed first.
- **PageRank Attack**: Nodes with highest PageRank are removed first.

Results

The size of the giant component is measured after each step of node removal. The X-axis represents the fraction of nodes removed, while the Y-axis shows the size of the largest component.

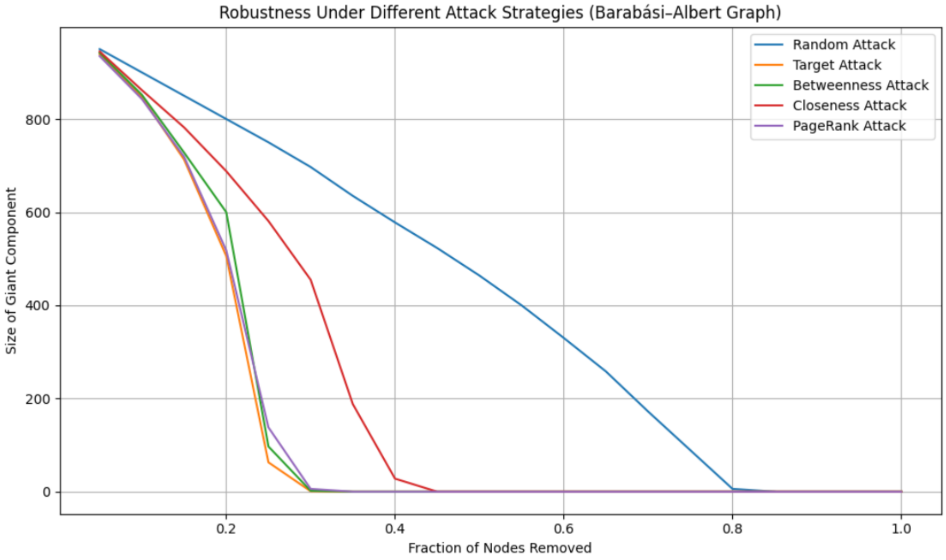


Figure 1: Robustness under different attack strategies on Barabási–Albert graph

2 Attacks on a Real-World Network

Graph Description

We use the Email-Eu-core network dataset, which consists of 1005 nodes. The largest connected component includes 986 nodes and is extracted for the analysis.

Results

The same attack strategies are applied to the real-world graph. The results on Figure2 and Table1 show that targeted attacks, especially based on betweenness, rapidly reduce the size of the giant component compared to random failures.

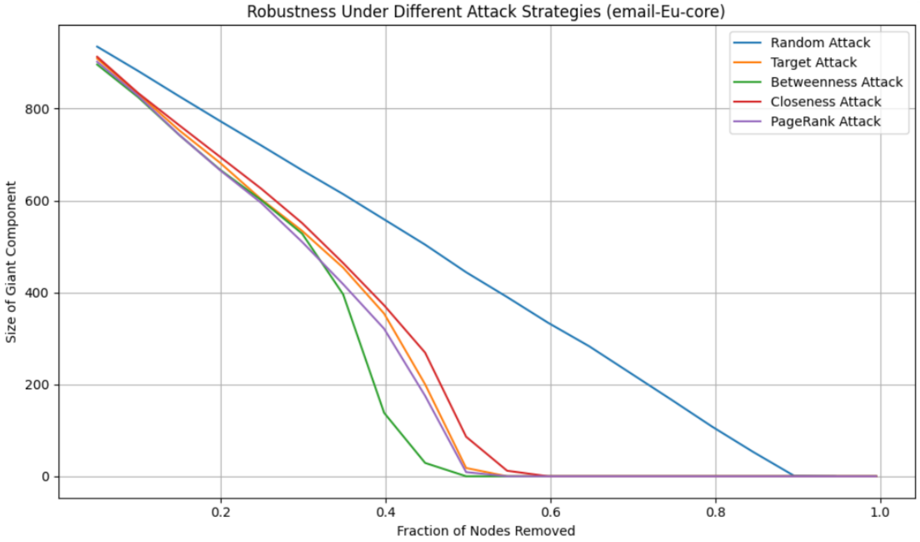


Figure 2: Robustness under different attack strategies on Email-Eu-core graph

Attack Strategy	**Nodes for Breakdown**
Random Attack	931
Target Attack	539
Betweenness Attack	490
Closeness Attack	588
PageRank Attack	539

Table 1: Nodes Required for Complete Network Breakdown under Each Attack Strategy

3 Building Robustness

Once the most damaging attack strategies were identified, we aimed to improve the robustness of the Email-Eu-core network by adding new edges.

Robustness Enhancement Strategies

- **Hubs:** Adding edges between neighbors of three high-degree nodes (hub triadic closure).
- **High-Betweenness:** Adding edges between neighbors of two nodes with the highest betweenness centrality.
- **Low-Degree:** Connecting low-degree nodes to high-closeness nodes to reinforce weak areas of the network.
- **Low-Degree Long-Distance:** Connecting low-degree nodes that are far from each other to shorten paths and increase redundancy.

These approaches increase local connectivity and provides alternative paths in case of node failures.

Critical Threshold f_c

For each strategy, we applied the modification and computed key topological metrics after each step: the number of nodes (N), number of edges (L), average degree ($\langle k \rangle$), second moment ($\langle k^2 \rangle$), and the critical threshold f_c computed as:

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1}$$

Results

Table 2 summarizes the evolution of these metrics. While all strategies maintained the node count ($N = 986$), they varied significantly in cost and impact:

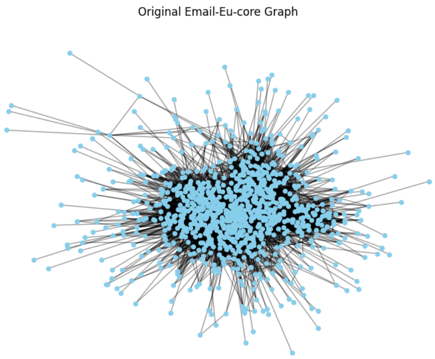
Strategy	**Improvement** (f_c)	**Edge Cost**	**Observation**
Original Graph	Baseline ($f_c = 0.9864$)	None (no added edges)	Base graph for comparison; used as the starting point for all improvement strategies.
Hubs	Very High ($f_c \uparrow$ to 0.9977)	Very High (Over 88K new edges)	Maximum robustness achieved, but extremely expensive in terms of added links.
High-Betweenness	High ($f_c \uparrow$ to 0.9972)	High (≈ 67K edges added)	Excellent improvement with slightly lower cost than Hubs; efficient up to step 1.
Low-Degree	Moderate ($f_c \uparrow$ to 0.9881)	Low (≈ 600 new edges)	Cost-effective strategy; no noticeable enhancement in network robustness.
Low-Degree Long-Distance	Negligible (No real change in f_c=0.9864)	Very Low (≈ 15 edges total)	Minimal impact; edge additions do not significantly enhance network robustness.

Table 2: Comparison of Edge-Addition Strategies Based on Robustness Gain and Edge Cost

Overall, **High-Betweenness** provided a strong balance between improvement and cost at step 1, raising f_c to 0.9972 with significantly fewer edges than Hubs.

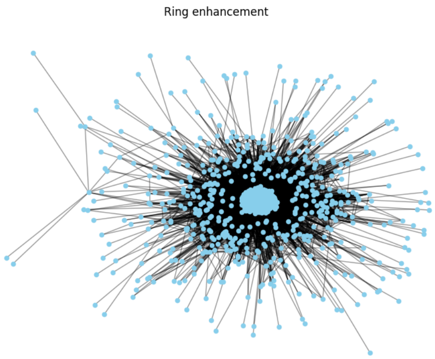
Graph Visualizations

The original network (Figure 3) exhibits a relatively sparse structure with hubs not directly connected. Figure 4 applies the ring enhancement strategy, where triangles are added among neighbors of high-degree hubs. This results in a significant increase in connectivity and the robustness threshold ($f_c = 0.99773$), but at a very high edge cost. Figure 5 applies the high-betweenness bridge strategy, connecting neighbors of central nodes with high betweenness. The structure becomes more robust and cohesive, while slightly reducing edge overhead compared to ring enhancement. The strategy connecting low-degree nodes (Figure 6) with long distances yields minimal structural change and negligible robustness improvement (f_c remains ≈ 0.9864). Although it incurs very low edge cost, it does not provide meaningful resilience gain, making it ineffective for robustness enhancement.



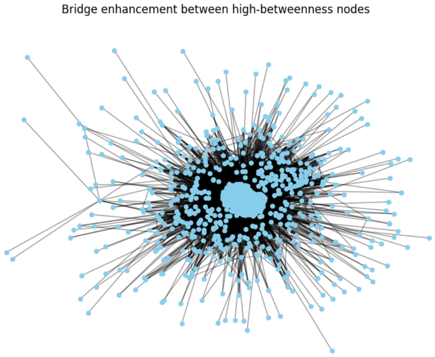
Original Email-Eu-core Graph

Figure 3: ($f_c = 0.98652$)



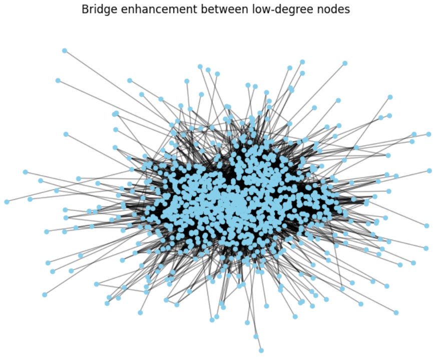
Ring enhancement

Figure 4: ($f_c = 0.99773$)



Bridge enhancement between high-betweenness nodes

Figure 5: ($f_c = 0.99722$)



Bridge enhancement between low-degree nodes

Figure 6: ($f_c = 0.98808$)

Robustness Comparison

Figure 7 and Figure 8 compares the robustness curves (size of giant component vs fraction of nodes removed) before and after improvement by high-betweenness bridge strategy. The post-improvement graph (Figure 8) shows a clear shift toward higher robustness, especially against targeted attacks (degree-based, betweenness, PageRank), where the giant component remains significantly larger for most of the removal process. This indicates a notable increase in fault tolerance due to the edge additions involving high-betweenness nodes. Random attacks still cause similar degradation, but strategic attacks are much less effective after reinforcement.

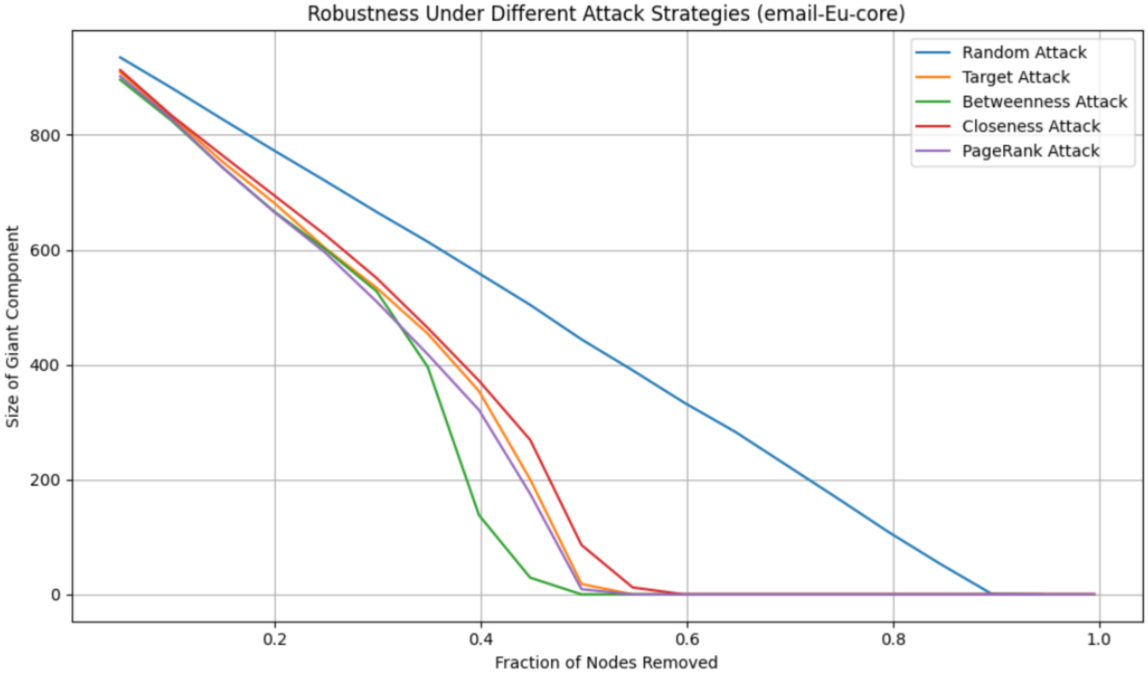


Figure 7: Before Improvement

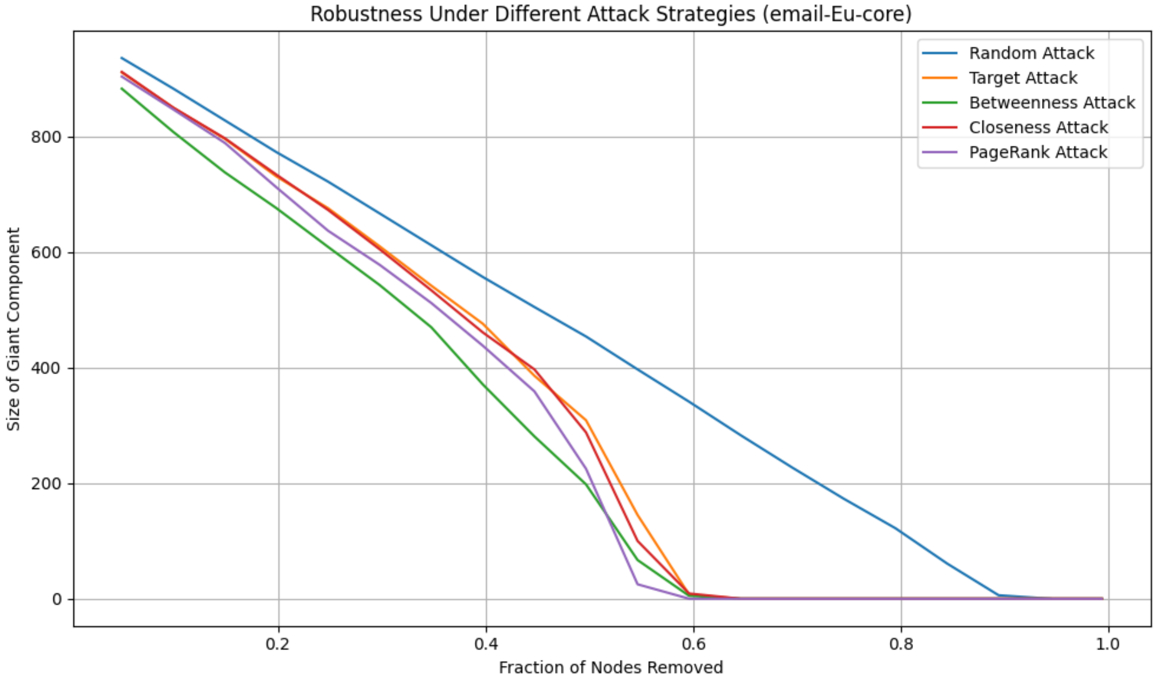


Figure 8: After Improvement

1 Conclusion

In this study, we evaluated the robustness of the Email-Eu-core network under various targeted and random attack strategies. The initial analysis revealed the network's vulnerability to centrality-based attacks, especially those targeting high-degree and high-betweenness nodes.

To improve resilience, we tested and compared four edge-addition strategies:

- **Ring (triangle) connections among hub neighbors**
- **Bridging high-betweenness nodes**
- **Connecting low-degree nodes to central nodes**
- **Linking distant low-degree nodes**

Among these, the **ring enhancement (hubs)** strategy showed the highest robustness improvement, with f_c increasing from 0.9864 to 0.9977. However, this came at the cost of over 88K new edges, making it the most expensive approach in terms of edge cost.

The **high-betweenness bridging** strategy also demonstrated excellent improvement in robustness ($f_c \approx 0.9972$), but with a significantly lower edge cost ($\approx$ 67K new edges), offering a more cost-effective alternative to the hubs strategy.

The **low-degree node strategies** resulted in marginal to moderate improvements in f_c, with minimal edge additions (as low as 15 and 600 edges), making them suitable for scenarios with strict resource constraints.

The robustness curves before and after high-betweenness enhancement clearly demonstrated that the improved networks better preserve connectivity under targeted attacks, confirming the effectiveness of structural reinforcement.

In summary, intelligently adding a small number of edges based on node centrality measures can significantly enhance network robustness. Among the tested methods, the high-betweenness strategy provides the best trade-off between resilience gain and edge cost.