Stockholms universitet

Stochastic Modeling of Dynamic Networks with Growth and Removal

Alvina Lindqvist

Kandidatuppsats i matematisk statistik
Bachelor Thesis in Mathematical Statistics

Kandidatuppsats 2025:19
Matematisk statistik
Juni 2025

www.math.su.se

Matematisk statistik
Matematiska institutionen
Stockholms universitet
106 91 Stockholm

Matematiska institutionen

Mathematical Statistics
Stockholm University
Bachelor Thesis **2025:19**
http://www.math.su.se

Stochastic Modeling of Dynamic Networks with Growth and Removal

Alvina Lindqvist*

June 2025

Abstract

In this report, we simulate a dynamic network based on preferential attachment, where the network evolves over discrete time steps by either growing or shrinking. That is, by adding or removing a node. We study how different factors, such as the probability of adding a node, the number of interactions per new node, and the removal strategy (random vs. targeted), affect the overall robustness of the network. The main focus is on how these changes influence the size of the *largest connected component*, a common measure of structural cohesion. The results provide insight into how seemingly small changes in network dynamics can significantly affect resilience.

The simulations show that the network's robustness is strongly influenced by the number of edges per new node (m) and the probability of node addition (p_{add}). When m is small, the network is sparse and quickly fragments under both random and targeted removal. As m increases, the network becomes significantly more connected and robust.

For $p_{add} > 0.5$, the network grows, and the largest connected component (LCC) remains stable under random attacks. However, targeted removal of high-degree nodes leads to rapid fragmentation. The degree distribution approximately follows a power law under random removal, but simulations have confirmed that the pattern breaks down under targeted strategies or when the growth rate is too slow. The robustness curves and estimated power law exponents γ support the theoretical prediction that scale-free networks are resilient to random failures but vulnerable to targeted attacks.

*Postal address: Mathematical Statistics, Stockholm University, SE-106 91, Sweden. E-mail: alvina@telia.com. Supervisor: Maria Deijfen, Daniel Ahlberg.

Acknowledgements

I would like to express my sincere gratitude to my supervisors, Maria Deijfen and Daniel Ahlberg, for their guidance and support throughout this project.

I have done the overall work of my code, but I have occasionally used OpenAI's ChatGPT as a support tool to resolve specific programming issues and to improve the structure of my code during the development of the simulations.

To assist with grammar and English phrasing, I have made use of LaTeX's integrated LanguageTool, where I have been writing my report.

Contents

1 Introduction

Many critical infrastructures, such as power grids, the internet, and communication systems can be represented as networks. These networks often look similar to the ones studied in theory, with a few nodes that have many connections. This makes the network efficient, but also more vulnerable if those high degree nodes are removed.

The connection points, such as routers, printers, or switches that can receive and send data from one endpoint to another are called network *nodes*. In networks constructed according to preferential attachment some nodes tend to attract more connections than others. An interesting question is: What happens to the network's cohesion when these central nodes are removed?

1.1 Real life network data

One clear example of a network structure when the whole system was affected because of the disruption of a few key nodes is the cyberattack on Ukraine's power grid in 2015. Hackers managed to cut power for a large part of the country by targeting just a few key parts of the network. In 2016, a new and more advanced attack used special malware to attack the grid in Kyiv. [4]

In Sweden, the power grid became a hot topic during the winter of 2002, when electricity prices rose sharply and there were warnings about possible power shortages. At the same time, Svenska Kraftnät reported increased threats from foreign actors, including espionage and sabotage. [7]

The internet is also vulnerable. In 2024, several submarine cables in the Baltic Sea were damaged, which affected the internet access in parts of Northern Europe. Events like this show how real-world networks can be sensitive to the removal of important nodes. That is why it is useful to study how networks change when nodes are removed, either randomly or in a target way, which is what this report explores through simulations.

1.2 Preferential Attachment and Scale-Free Networks

Scale-free networks refer to all networks whose degree distribution follows a power law, at least asymptotically. According to the mechanism, each new node connects to m existing nodes, with a probability proportional to their current degree

$$\pi_i = \frac{k_i}{\sum_j k_j}$$

where k_i is the degree of node i.

This results in a power-law degree distribution:

$$P(k) \sim k^{-\gamma}$$

where the probability of a node having k connections decreases as k increases. However, at a relatively slow rate compared to exponential or Poisson distributions. The power-law distribution, implies that there is a non-negligible probability of finding nodes with a very large number of connections. This property differs scale-free networks from many other types of networks where high-degree nodes are extremely rare. This model was first introduced by Barabási and Albert in 1999 [1], and is now a foundational concept in network science.

One well-known generative model for producing scale-free networks is the *preferential attachment model*. In this model, the network grows over time by sequentially adding nodes. Each new node connects to m existing nodes with the probability π_i (introduced above), meaning that nodes with higher degree are more likely to receive new connections. The mechanism leads to a power law degree distribution with exponent $\gamma = 3$, under idealized assumptions. It is important to note that not all scale-free networks are generated via preferential attachment, and not all networks generated by preferential attachment remain scale-free under various modifications. Scale-freeness is a structural property of the network, while preferential attachment is a model that can give rise to such a structure.

1.3 The largest connected component

The largest connected component (LCC) is a commonly used measure of a network's coherence. We let $G = (V, E)$ be an undirected graph, where V denotes the vertices (nodes), and E denotes the edges (links). The LCC is defined as the component $C \subseteq V$ such that

$$|C| = \max\{|C_i| : C_i \text{ is a connected component of } G\}$$

and the LCC fraction is

$$f_{\text{LCC}} = \frac{|C|}{|V|}$$

A value of $f_{\text{LCC}} \approx 1$ implies that the network is mostly connected, and low values indicate fragmentation.

To investigate the network's resilience to node removal, we analyze the LCC and how it changes under successive node removals. Both random removal and targeted removal (based on high-degree nodes) are considered. After each node is removed, the size of the LCC is calculated as a percentage of the original network. This generates a robustness curve that illustrates how the network fragments over time.

The robustness is also summed up in a single value, defined as the arithmetic mean of the LCC proportion over the entire removal process:

$$R = \frac{1}{Q}\sum_{i=1}^{Q} S(i), \quad \text{where } S(i) = \frac{LCC(i)}{N}$$

and N is the total nodes in the network at the end of the growth process, Q is the number of removal steps and $S(i)$ is the size of the LCC after i nodes have been removed. [5]

1.4 Other network models

Not all networks are generated by the preferential attachment principle. One example is the Erdős–Rényi model, introduced by Paul Erdős and Alfréd Rényi. In the model, a graph is generated by connecting each possible pair of nodes with a fixed probability, independently of all other pairs. This results in a random network without any preference for central or highly connected nodes.

The model is often used to represent systems without a central structure, such as certain communication or fault-prone systems. It produces a degree distribution similar to a Poisson process, where most nodes have approximately the same number of connections.

Unlike preferential attachment models, which typically produce a few highly connected nodes and a power-law degree distribution, the Erdős–Rényi model does not capture scale-free behavior. However, it is useful for studying randomness and serves as a baseline model in network theory.

2 Definition of the model

2.1 Simulation model

In this study, we simulate a dynamic network model based on the preferential attachment principle by the removal of nodes. This allows the network both to grow and to shrink over time. The stochastic model can be described as a discrete-time process $\{G_t\}_{t\geq 0}$, where $G_t = (V_t, E_t)$ denotes the network at time t. Initially at $t = 0$, there is an initial network G_0, usually a small complete graph with $|V_0| = S$ nodes.

At each discrete time step $t \to t+1$ in the simulation, exactly one of the following two events occurs:

- Growth with a probability p_{add}. A new node is added to the network and connects to m existing nodes. These m target nodes are selected without replacement, meaning that each existing node can be chosen at most once per step. This ensures that multiple edges between the same pair of nodes do not occur.

  The selection is based on preferential attachment, where the probability of choosing a node is proportional to its degree at time t. For the first

attachment, this is exactly

$$\mathbb{P}(\text{New node connects to node } i) = \frac{k_i(t)}{\sum_{j \in V_t} k_j(t)}$$

For subsequent edges, the remaining nodes are rescaled accordingly, so the probabilities are only approximately proportional to degree but the principle of preferential attachment still holds.

- Removal with probability $1 - p_{\text{add}}$. An existing node is removed from the network along with its edges. The removal is either *random* (uniform over all nodes) or *targeted*, where the node with the highest degree is selected:

$$k_{\max}(t) = \max_{i \in V_t} k_i(t)$$

The process is repeated for a total of n time steps, resulting in the final network G_n. We then analyze the resulting structure, focusing on the size of the largest connected component (LCC) and the degree distribution.

By varying the parameters m and p_{add} in the range $(0.5, 1]$, we investigate how the balance between growth and shrinkage affects the formation and resilience of highly connected nodes.

For each value of p_{add}, we simulate a dynamic network with n time steps. Afterwards, we extract the degrees k of all the remaining nodes and examine whether the degree distribution follows a power law of the form

$$P(k) \sim k^{-\gamma},$$

using the Python package `powerlaw`, which performs a statistical fit of a power law distribution to empirical data.

The function `powerlaw.Fit()` estimates two key parameters:

- γ: the power-law exponent, describing how quickly the probability decreases for higher node degrees.
- $x_{\min}$: the minimum degree from which the power-law behavior is assumed to hold. Degrees below $x_{\min}$ are excluded from the fit, as they may not follow power-law scaling.

These parameters are estimated using maximum likelihood methods by fitting a discrete power-law model to the observed degree distribution.

The estimated values of γ and $x_{\min}$ for each p_{add} are presented in the tables below, alongside the final number of nodes in the network.

It is important to note that the model does not exhibit a power law for all combinations of m and p_{add}, particularly under targeted node removal and low values of p_{add}. This will become evident in section 3.1 where we analyze the distributions observed in the simulations.

2.2 Analytical derivation of expected number of nodes

The stochastic process that describes the network development can be seen as a discrete "birth-death process", where at every time step the number of nodes decreases with 1 node (birth) or increases with 1 node (death). As mentioned earlier, we have

- Probability that one node is added is p_{add}.
- Probability that one node is removed is $1 - p_{\text{add}}$.

Let X_t be the stochastic number of nodes at time t. Then the change at every time step can be described as

$$X_{t+1} = \begin{cases} X_t + 1 & \text{with probability } p_{\text{add}}, \\ X_t - 1 & \text{with probability } 1 - p_{\text{add}}. \end{cases}$$

The number of nodes after n steps can be described as

$$X_n = X_0 + \sum_{i=1}^{n} Y_i,$$

where every Y_i is an independent and identically distributed random variable that takes on values according to

$$Y_i = \begin{cases} +1 & \text{with probability } p_{\text{add}}, \\ -1 & \text{with probability } 1 - p_{\text{add}}. \end{cases}$$

Since each step is independent and identically distributed, the expected value is

$$\mathbb{E}[Y_i] = \sum_{y} y \cdot \mathbb{P}(Y_i = y)$$

and we obtain

$$\mathbb{E}[Y_i] = (+1) \cdot p_{\text{add}} + (-1) \cdot (1 - p_{\text{add}}) = 2p_{\text{add}} - 1.$$

Because of the linearity of expectation value, we can determine the expected number of nodes after n steps

$$\mathbb{E}[X_n] = \mathbb{E}[X_0] + \sum_{i=1}^{n} \mathbb{E}[Y_i] = X_0 + n(2p_{\text{add}} - 1),$$

where X_0 is the initial number of nodes.

This describes a random walk with a step variable $Y_i \in \{-1, +1\}$, representing either the removal or addition of a node. The parameter p_{add} thus controls the drift of the process.

- If $p_{\text{add}} > 0.5$, the process has a positive drift and the expected number of nodes increases linearly with time. The network grows.
- If $p_{\text{add}} = 0.5$, the network becomes a symmetric random walk with no drift. In probability theory, it is well known that such a process will almost surely be absorbed to 0. In this context, it means that the network will eventually lose all its nodes. Because of this extinction behavior, we exclude simulations with $p_{\text{add}} = 0.5$ in this study.
- If $p_{\text{add}} < 0.5$, the process has a negative drift, and the number of nodes decreases with time. The network shrinks over time and eventually collapses.

To quantify the variation, we can also calculate the variance for each step

$$\text{Var}(Y_i) = \mathbb{E}[Y_i^2] - \mathbb{E}[Y_i]^2 = 1 - (2p_{\text{add}} - 1)^2 = 4p_{\text{add}}(1 - p_{\text{add}}).$$

Since the steps are independent, the total variance after n steps is

$$\text{Var}(X_n) = 4np_{\text{add}}(1 - p_{\text{add}}).$$

This provides a measure of the spread we can expect around the expected value after n steps.

3 Theoretical analysis of network robustness

3.1 Degree distribution and power-law behavior

In the simulations we investigate whether the degree distribution of the network follows a power law of the form

$$P(k) \sim k^{-\gamma},$$

where the exponent γ determines how quickly the probability of large node degrees decreases. It is known from the Barabási-Albert model (BA model) that network with pure preferential growth (without removal) asymptotically have a power-law distribution with exponent $\gamma \approx 3$.

More precisely, the theoretical form of the discrete power-law distribution is given by

$$P(K = k) = \frac{k^{-\gamma}}{\zeta(\gamma, x_{\min})},$$

where $\zeta(\gamma, x_{\min})$ is the Hurwitz zeta function. [10]. This function acts as a normalization constant to ensure that the probabilities sum to 1 over all degrees

$k \geq x_{\min}$. The Hurwitz zeta function is defined as

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s},$$

and is used to model the long-tail behavior of scale-free networks.

To estimate the exponent γ and the lower bound $x_{\min}$, we use the Python package *powerlaw*, which applies a maximum likelihood method (MLE), under the assumption that the degree distribution follows a power-law behavior for $k \geq x_{\min}$. The package also supports statistical goodness-of-fit tests, such as Kolmogorov-Smirnov (KS) test, to asses how well the fitted power law matches the observed data.

However, in this study, no such formal tests were performed. This means that while we provide fitted values of γ and $x_{\min}$, we do not verify whether the power law is the best fit compared to other heavy-tailed distributions (e.g., exponential or log-normal). Still, the estimated parameters serve as useful indicators of whether the scale-free behavior emerges in the simulations.

It is also known from theory that under targeted removal of highly-connected nodes, especially when $m = 1$ and p_{add} is small, that the network does not maintain a power-law degree distribution. This is because the most connected nodes are repeatedly removed, preventing the development of a heavy-tailed structure. These theoretical expectations are confirmed in the simulations: under random removal, the estimated γ typically remains within the range expected for scale-free networks, whereas under targeted removal, γ becomes unstable or undefined when the network fragments severely.

In particular, Deijfen (2010) shows that for $m = 1$, a power-law degree distribution cannot be maintained under target removal when p_{add} is too low. However, under random removal, the network still tends to follow a power-law distribution, albeit with modified parameters.

3.2 Percolation threshold and network fragmentation

The percolation threshold marks the critical point at which the network undergoes a structural phase transition, from being largely connected to breaking apart into many smaller components. This transition is typically characterized by the removal of the giant component, defined as a connected subgraph containing a positive fraction of all nodes in the network. A giant component is one whose size grows linearly with the total number of nodes n, i.e., it is of order $\Theta(n)$.

In classical random networks, such as the Erdős-Rényi model, the percolation threshold is well defined and can be analyzed mathematically using classical percolation theory. Above the threshold, a giant component forms; below it, only small components exist. In contrast, scale-free networks with degree distribution $P(k) \sim k^{-\gamma}$ are known to be remarkably robust to random failure. Albert

et al. (2000) showed that this resilience arises from the network's heterogeneity: most nodes have low degrees, while a few nodes have very high degrees and maintain the overall connectivity. Under random removal, the giant component can persist even when a large fraction of nodes are removed.

4 Simulations and results

4.1 Robustness Curve

In the simulation conducted in this study, we initialized the network with a small initial graph of three nodes. A connected starting network ensures that growth is always possible, while keeping the initial structure minimal reduces its influence on the evolving network properties. In the dynamic network, at each time step, either one node is added with probability p_{add} (between 0.6 and 1), or one node is removed with probability $1 - p_{\text{add}}$.

The number of time steps (n) was set to 5000. We aimed for a network large enough for meaningful statistical analysis, while keeping the simulations computationally manageable.

To illustrate how two different types of attacks affect the network structure when the network has reached its full size, we perform two types of attacks: a targeted attack, where highly connected nodes are removed first, and a random attack, where nodes are removed uniformly at random. The figure below shows the size of the Largest Connected Component (LCC) as a function of the fraction of removed nodes, for both attack types. We have chosen a node addition probability of $p_{\text{add}} = 1$ to prevent the network from already being fragmented for $m = 1$, but the qualitative behavior of the robustness curve remains the same for other values.

We settle on 10 iterations in this simulation, calculating the R scores and LCC before the attack. This means that the mean values are represented in Table 1 below.

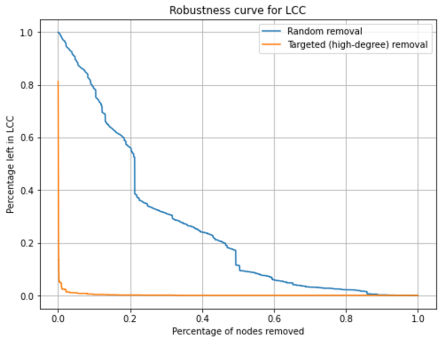

Figure 1: Robustness Curve for random and central targeted removal of nodes ($m = 1$)

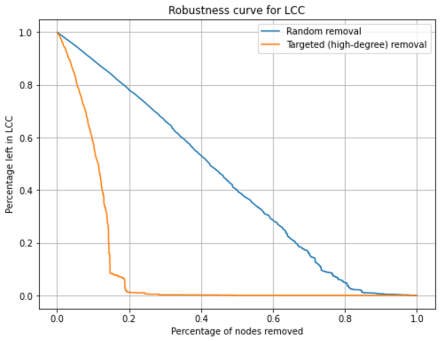

Figure 2: Robustness Curve for random and central targeted removal of nodes ($m = 2$)

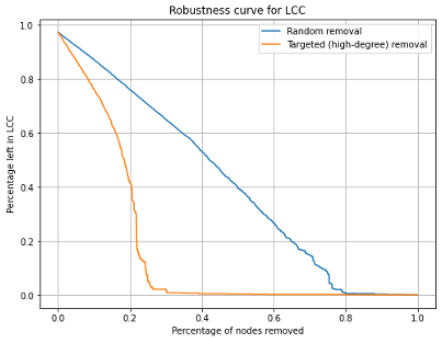

Figure 3: Robustness Curve for random and central targeted removal of nodes ($m = 3$)

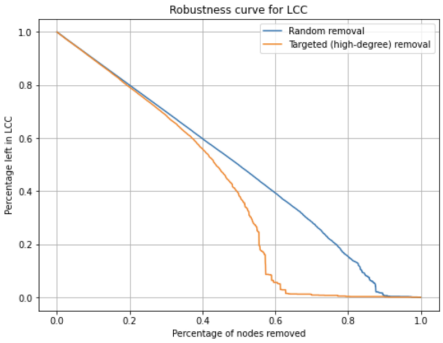

Figure 4: Robustness Curve for random and central targeted removal of nodes ($m = 8$)

Figure	m	LCC before attack (% of network)	R_{targeted}	R_{random}
Figure 1	1	100 %	0.0025	0.1940
Figure 2	2	100 %	0.1033	0.4126
Figure 3	3	100 %	0.1918	0.4562
Figure 4	8	100 %	0.3860	0.4910

Table 1: LCC before node removal and robustness scores R (average LCC size during removal) for both targeted and random strategies

As expected, we can see that for all m, the LCC covers the entire network, before the simulated attack begins. This makes it easier to interpret the robustness

results, because it shows how a well-connected network reacts to different types of attacks.

The simulation results show that for small values of m the random removal curve gradually declines, and the targeted removal leads to an abrupt collapse of the network structure. This shows that the network is *robust to random failures but vulnerable to targeted attacks*, a characteristic feature of scale-free networks.

In addition to the robustness curves, we also calculated a number called the robustness score R for each simulation. This score shows, on average, how much of the network remained connected when nodes were being removed. It gives a simple way to compare how well the network handled attacks. As shown in Table 1, the robustness score increases as m increases, meaning that networks with more initial connections are better able to withstand attacks.

4.2 Connectivity: $m = 1$ (Tree-like structure)

We now investigate how the parameter p_{add} affects the components, particularly the LCC, when nodes are added with exactly one link ($m = 1$), which means that the network grows in a tree-like structure and no new cycles can be created. Here $\bar{s}_{\text{comp}}$ denotes the mean size of the components, excluding the LCC. We performed 10 iterations, and calculated the mean values, which are shown in the tables below.

The results show that the choice of removal strategy has a large effect on the network's growth and structure.

Table 2: Removal strategy: Random removal, $m = 1$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	967.3 (19.33%)	391.0	2.31	65.6	6.39%	3.37	3.6
0.7	2009.0 (40.16%)	600.1	3.09	155.2	7.73%	2.97	3.6
0.8	2999.2 (59.95%)	580.7	4.34	484.4	16.15%	2.86	3.8
0.9	3997.8 (79.91%)	397.3	6.56	1396.9	34.94%	2.73	3.7
1.0	5003 (100%)	1	NaN	5003	100%	2.70	4.1

Table 3: Removal strategy: Targeted (high degree) removal, $m = 1$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)
0.6	1002.0 (20.03%)	1000.8	1.00	2.1	(0.21%)
0.7	1891.6 (37.81%)	1978.6	0.95	4.0	(0.21%)
0.8	2983.9 (59.64%)	2778.7	1.07	9.9	(0.33%)
0.9	4006.2 (80.08%)	2231.6	1.79	24.4	(0.61%)
1.0	5003 (100%)	1	NaN	5003	(100%)

The results in Table 2 and Table 3 show clear structural differences in the network depending on both the probability parameter p_{add} and the removal strategy.

We observe that the number of components is lower for random removal than for targeted removal. This is likely because targeted removal isolates nodes more effectively by removing the most connected nodes first, which leads to rapid fragmentation of the network.

The mean component size (excluding the LCC), denoted by $\bar{s}_{\text{comp}}$, is generally larger for random removal and appears to increase as p_{add} grows. In contrast, for targeted removal, the mean component size remains close to 1, with its highest value reaching only 1.79.

As expected, the size of the LCC is significantly larger under random removal than under targeted removal, and increases rapidly with higher values of p_{add}. While the LCC gives an idea of global connectivity, the mean component size reveals how the rest of the network is structured after fragmentation.

Under random removal, γ remains in a typical scale-free range between 2.60 and 3.37. For targeted removal, these values are unstable or undefined when the LCC becomes too small, as expected for $m = 1$ networks at low p_{add}, where targeted attacks are known to destroy the power-law degree distribution.

Size of the largest component, $m = 1$

To deepen the analysis, we plot the mean size of the largest connected component (LCC) as a function of p_{add} and expand the parameter space by simulating more values of p_{add} in steps of 0.05. As before, we run 10 iterations and report the average results.

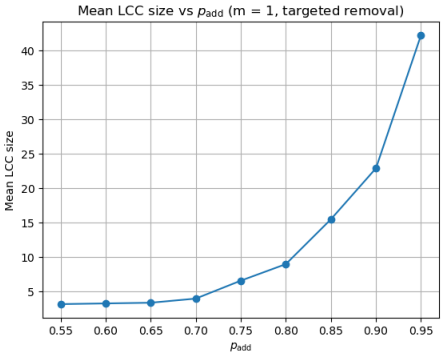

Figure 5: m = 1, removal strategy: targeted (high degree)

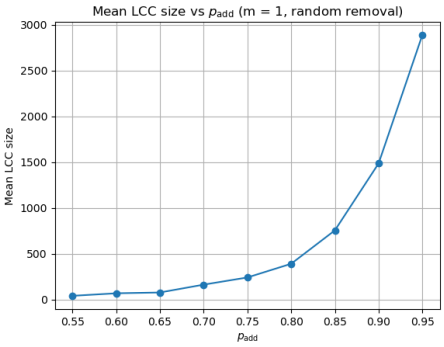

Figure 6: m = 1, removal strategy: random

For $m = 1$, the results reveal a sharp contrast in robustness between targeted and

random node removal. In Figure 5 (targeted removal), the growth of the largest connected component (LCC) remains severely limited even for relatively high values of p_{add}. For example, the LCC size is only about 4 nodes at $p_{\text{add}} = 0.7$, meaning that the network contains almost entirely isolated nodes. As p_{add} increases, it reaches around 42 nodes at $p_{\text{add}} = 0.95$. This indicates that although the network is growing, the continuous removal of high-degree nodes effectively prevents any substantial structure from forming.

In contrast, Figure 6 (random removal) shows a faster-than-linear increase in LCC size under random node removal. At $p_{\text{add}} = 0.95$, the LCC reaches nearly 2900 nodes on average-more than half of the network. This suggests that the network is significantly more robust to random failures than to targeted attacks. Even at $p_{\text{add}} = 0.8$, the LCC already exceeds 750 nodes, showing that a connected core can survive as long as new nodes are added faster than they are removed at random.

4.3 Connectivity: $m > 1$

In this section, we analyze the behavior of the dynamic network when each new node connects to $m = 2$, 3 and 8 existing nodes. As in the previous section, we vary the growth parameter p_{add} and compare both random and targeted node removal strategies. The results are presented in the tables below.

Table 4: Removal strategy: Random removal, $m = 2$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1029.4 (20.58%)	147.4	1.07	872.9	84.79%	3.16	3.6
0.7	2004.8 (40.07%)	176.9	0.82	1860.0	92.78%	3.06	4.1
0.8	3015.8 (60.28%)	93.2	1.03	2921.0	96.86%	2.90	4.2
0.9	4005.6 (80.06%)	30.0	1.01	3976.2	99.27%	2.73	4.3
1.0	5003 (100.00%)	1	NaN	5003	100%	2.74	5

Table 5: Removal strategy: High degree, $m = 2$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1024.6 (20.48%)	1017.70	1.00	6.40	0.62%	2.99	2.00
0.7	2032.8 (40.63%)	1682.0	1.06	247.90	12.20%	4.60	2.8
0.8	2971.9 (59.40%)	1140.6	1.09	1727.30	58.12%	4.356	3
0.9	4001.8 (79.99%)	528.7	1.06	3440.5	85.97%	9.57	6.6
1.0	5003 (100.00%)	1	NaN	5003	100%	2.68	4

Table 6: Removal strategy: Random removal, $m = 3$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1001.2 (20.01%)	64.50	1.03	936.0	93.49%	3.32	4.6
0.7	2019.2 (40.36%)	48	1.02	1971.25	97.63%	3.23	5.4
0.8	2994.0 (59.84%)	21.1	1.00	2973.9	99.33%	2.99	4.9
0.9	3984.2 (79.64%)	4.6	1.00	3980.6	99.91%	2.84	5.1
1.0	5003 (100.00%)	1	NaN	5003	100%	2.67	4

Table 7: Removal strategy: High degree, $m = 3$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1010.9 (20.21%)	980.10	1.00	29.40	2.90%	4.55	3
0.7	1997.0 (39.91%)	824.70	1.04	1139.5	57.06%	5.25	3.60
0.8	2992.0 (59.80%)	448.60	1.03	2528.80	84.52%	3.71	3.30
0.9	4030.6 (80.56%)	155.4	1.02	3873.3	96.10%	6.92	5.9
1.0	5003 (100.00%)	1	NaN	5003	100%	2.74	5

Table 8: Removal strategy: Random removal, $m = 8$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1011.8 (20.22%)	4.7	1.00	1008.1	99.63%	4.15	10.1
0.7	2011.6 (40.21%)	1.6	1.00	2011.0	99.97%	3.62	10.2
0.8	2993.2 (59.83%)	1.0	NaN	2993.2	100%	3.22	9.50
0.9	4016.6 (80.28%)	1.0	NaN	4016.6	100%	3.01	9.5
1.0	5003 (100%)	1.0	NaN	5003	100%	2.83	8

Table 9: Removal strategy: High degree, $m = 8$

p_{add}	Nodes (n)	Components	$\bar{s}_{\text{comp}}$	LCC	LCC (%)	γ	$x_{\min}$
0.6	1026.9 (20.53%)	129.0	1.47	838.9	71.69%	11.213	8.8
0.7	2003.0 (40.03%)	45.3	1.02	1958.0	97.75%	10.58	10.9
0.8	3000.4 (59.97%)	10.5	1	2990.9	99.68%	5.57	9.7
0.9	3994.8 (79.85%)	2.1	1	3993.7	99.97%	3.38	8
1.0	5003 (100.00%)	1	NaN	5003	100%	2.88	12

Compared to the sensitive network structures observed when $m = 1$, the introduction of fixed connectivity $m > 1$ leads to a significant change in the network behavior. Both the number of connected components and the size of the

largest connected component (LCC) show systematic improvements as m increases.

The simulation results in Tables 3 – 6 show significant variation in f_{LCC} (the fraction of nodes belonging to the LCC) depending on the parameters p_{add} and m. Specifically:

- For $m = 2$, under *random removal*, the number of components decreases and f_{LCC} remains high across all the tested values of p_{add}.
- Under *targeted removal*, the results suggests a transition region around $p_{\text{add}} \approx 0.7$. At $p_{\text{add}} \approx 0.6$, the number of components increases significantly, while for $p_{\text{add}} > 0.7$, the network appears to regain a more coherent structure, with a pronounced decrease in the number of components and a marked increase in f_{LCC}.
- For $m = 3$, this trend becomes even more pronounced. The LCC consistently increases in relative size across all tested values of p_{add}, and the number of components ($p_{\text{add}} \geq 0.6$) continues to decrease, even under targeted removal.

These results indicate that each additional connection per node (i.e., higher m) increases the probability that the network remains coherent despite node removal during growth.

Size of the largest component $m = 2, 3, 8$

We will again examine the size of the largest component (LCC) as a function of the parameter p_{add}, with $m = 2, 3$ and 8. The results are shown in Figure 7 to Figure 12.

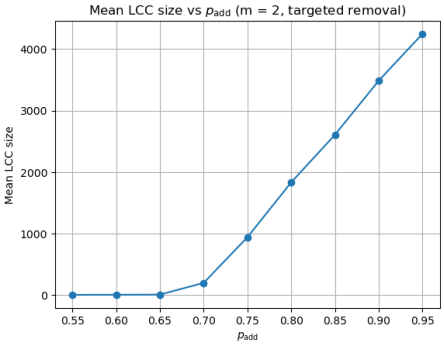

Figure 7: m = 2, removal strategy: targeted (high degree)

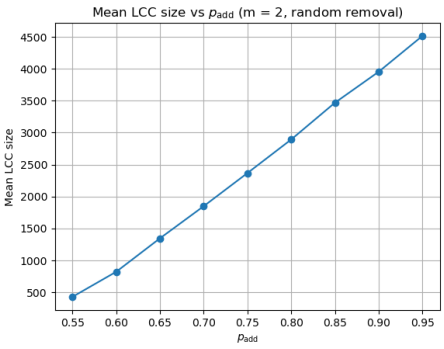

Figure 8: m = 2, removal strategy: random

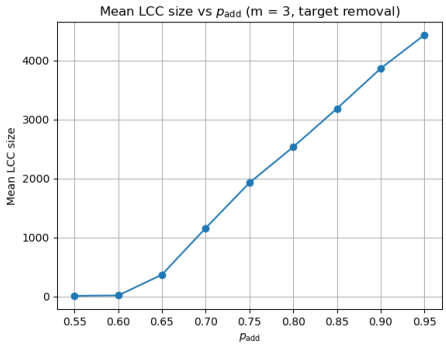

Figure 9: m = 3, removal strategy: targeted (high degree)

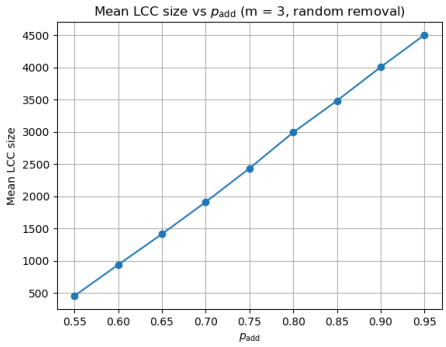

Figure 10: m = 3, removal strategy: random

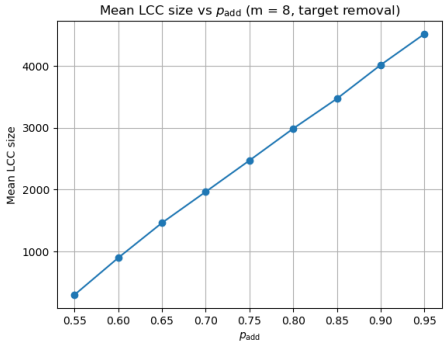

Figure 11: m = 8, removal strategy: targeted (high degree)

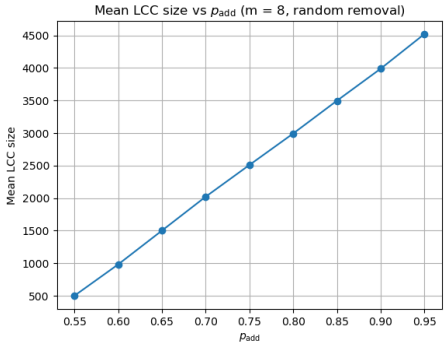

Figure 12: m = 8, removal strategy: random

We observe that, for all values of m, the mean LCC increases with p_{add}, but the growth rate and threshold behavior vary depending on the removal strategy.

In the targeted removal scenario, for $m = 2$, we can see that between $p_{\text{add}} = 0.55$ and $p_{\text{add}} = 0.65$ the network remains highly fragmented, with mean LCC values between 5 and 9. For $p_{\text{add}} = 0.70$ the mean LCC increases to around 200 and continues to grow, reaching approximately 4200 at the upper end of the range. In contrast, under random removal, the network retains a much larger connected component even at lower p_{add}, indicating that the network is significantly more robust to random node deletion.

For the highly connected network where $m = 8$, the results show an almost linear growth in the mean LCC size, regardless of removal strategy. This suggests that the network structure becomes increasingly resilient as each node connects to

many existing nodes. The removal of either random or high-degree nodes has limited impact on the integrity of the largest component, provided that p_{add} is sufficiently high.

Overall, the simulations illustrate how both the parameter m and the removal strategy critically influence the network's ability to maintain a large connected component. A higher m compensates for the destructive effect of node removal, while targeted strategies are consistently more effective at fragmenting the network, especially when m is small.

5 Conclusion

This report explored how a growing network governed by preferential attachment responds to node removal. By combining growth and deletion in a dynamic simulation model, we analyzed how varying the probability of node addition p_{add}, the number of connections per new node m, and the removal strategy (random vs. targeted) affects the network's structural resilience.

The results show that the network's ability to maintain connectivity is highly dependent on both m and p_{add}. A key finding is that networks with low m are fragile even under moderate levels of node deletion. This is particularly evident under targeted removal, which rapidly destroys the largest connected component. As m increases, the network gains redundancy and becomes more resilient to both random failures and targeted attacks.

We find strong support for the hypothesis that scale-free networks are robust to random failures but vulnerable to targeted attacks. This pattern is especially visible in the robustness curves and LCC growth figures. In addition, the emergence of threshold-like behavior in p_{add}, where the network transitions from fragmented to cohesive, highlights the relevance of percolation theory in understanding network connectivity.

An additional observation is that for $m > 1$, the size of the largest connected component increases approximately linearly with p_{add}, particularly under random removal. This suggests that as long as node addition dominates the process, the network maintains a growing core structure despite ongoing deletion.

6 Discussion

In this study, the simulations suggests a possible threshold or transition in the network's structural behavior, particularly under targeted node removal. For networks with $m > 1$, the largest connected component (LCC) tends to fragment significantly at lower values of p_{add}. At these lower values, the network struggles to sustain a dominant component and instead splits into smaller disconnected sub-networks. However, once p_{add} exceeds a critical region (approximately around $0.6 - 0.7$), the network becomes capable of maintaining a single

large component whose size grows proportionally with the total number of nodes n. Due to the discrete intervals used in the simulations (steps of 0.05), the exact value of this transition remains uncertain. Additional simulations with finer intervals would be valuable for accurately characterizing this threshold.

A critical factor influencing the resilience of the network is the removal strategy. Our results show that under random removal, the network is robust, maintaining a substantial LCC even at relatively low values of p_{add} (see, for example Table 6 and Table 8). This aligns with existing theory, which suggests random deletion rarely impacts highly connected, structurally important nodes. In contrast, under targeted removal, consistently removing nodes with the highest degree leads to rapid fragmentation of the network at moderate to low values of p_{add}, especially noticeable when m is small. As we observed, the threshold for structural collapse under targeted attacks appears significantly lower and varies depending on specific parameter settings.

Interestingly, the threshold for network fragmentation increases with larger m, for example, at $m = 8$ (see Table 9). Already at $p_{\text{add}} = 0.6$, the LCC corresponds to around 70% of the network and quickly grows to nearly the entire network as p_{add} increases. This suggests that highly connected networks can maintain global connectivity even under targeted removal, provided that growth is sufficiently strong.

A promising direction for future research is to explore probabilistic node removal strategies rather than deterministic targeting. For example, instead of always removing the highest-degree node, nodes could be selected for removal with probabilities proportional to their degrees. Such probabilistic removal could more realistically model scenarios like cyberattacks or failures in complex infrastructures, potentially smoothing out the observed sharp threshold effects.

In the report "Weighted Betweenness Preferential Attachment: A New Mechanism Explaining Social Network Formation and Evolution" [6] it is suggested that new nodes may not necessarily attach to those with the highest degree, but rather to those with high betweenness, an idea that has not been explored in this report. Betweenness centrality quantifies a node's role as an intermediary on shortest paths between other nodes, highlighting its importance for overall connectivity. Nodes with high betweenness centrality may serve as critical connectors whose removal could significantly disrupt the network, potentially more so than simply removing nodes based solely on degree. This could be an area to study for future research.

Overall, the concept of percolation threshold provides a useful theoretical framework for understanding how network resilience varies with different parameters and removal strategies. Our findings confirm the well-known structural characteristics of scale-free networks-namely, their robustness to random failures and vulnerability to targeted attacks. Moreover, the results underscore the importance of structural redundancy (larger m) in enhancing the network resilience.

References

[1] Barabási, A.-L. and Albert, R. (1999). *Emergence of scaling in random networks*. Science, 286(5439), 509–512.

[2] Deijfen, M. and Lindholm, M. (2009). *Growing networks with preferential deletion and addition of edges*. Physica A: Statistical Mechanics and its Applications, 388(21), 4507–4519.

[3] Wikipedia, *Erdős–Rényi model* `https://en.wikipedia.org/wiki/Erd%C5%91s%E2%80%93R%C3%A9nyi_model`

[4] Nylander, J. (2017). *FRA: IT-spioner förbereder attack mot elnätet*. SVT Nyheter. Accessed April 13, 2025.

[5] Hasheminezhad, R. and Brandes, U. (2023). *Robustness of preferential-attachment graphs*. Applied Network Science, 8(1), 36.

[6] Topirceanu, A., Udrescu, M. & Marculescu, R. (2018). *Weighted Betweenness Preferential Attachment: A New Mechanism Explaining Social Network Formation and Evolution*. ResearchGate. Accessed April 13, 2025.

[7] Sveriges Radio. *Så kan fiender attackera vårt elnät – granskning*. Accessed April 13, 2025. Published December 28, 2022.

[8] Wikipedia contributors. *Erdős–Rényi model*. `https://en.wikipedia.org/wiki/Erd%C5%91s%E2%80%93R%C3%A9nyi_model`, accessed April 13, 2025.

[9] Wikipedia contributors. *Robustness of complex networks* `https://en.wikipedia.org/wiki/Robustness_of_complex_networks`

[10] Wikipedia contributors. *Hurwitz zeta function* `https://en.wikipedia.org/wiki/Hurwitz_zeta_function`