UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE FÍSICA DE SÃO CARLOS

Carlos Eduardo Toma da Silva

Efeitos das características topológicas em redes complexas na propagação de falhas em cascata

São Carlos
2025

Carlos Eduardo Toma da Silva

Efeitos das características topológicas em redes complexas na propagação de falhas em cascata

Trabalho de conclusão de curso apresentado ao Instituto de Física de São Carlos da Universidade de São Paulo para obtenção do título de Bacharel em Física Computacional. Orientador: Prof. Dr. Gonzalo Travieso - Instituto de Física de São Carlos.

São Carlos
2025

RESUMO

Redes complexas são grafos usados para simular contextos reais, neste trabalho elas serão usadas para simular falhas em sistemas que podem se propagar e possívelmente destruir a rede, assim são testados modelos de rede e características topológicas como eficiência, grau médio e o número de nós para encontrar vulnerabilidades na rede, para então relacionar quais características têm melhor efeito para suprir as falhas em cascata, que foram simuladas computacionalmente e os resultados analisados. Foi encontrado que a tolerância e o grau médio da rede afetam significativamente as chances de colapso, além de que as redes de Barabási-Albert, que gera uma rede usando conexão preferencial, e modelo de configuração dada uma distribuição de graus em uma lei de potências possuem maior resistência contra falhas, porém são vulneráveis a ataques em seus hubs, enquando o modelo de Erdős-Rényi, um gerador de rede aleatória, gera redes mais resistente a ataques nos hubs, porém é vulnerável a múltiplas falhas.

Palavras-chave: Redes Complexas, propagação de falhas, modelos de redes

1 INTRODUÇÃO

Com a rápida evolução tecnológica da humanidade, sistemas e infraestruturas aumentaram em escala e em complexidade e, por consequência, a ocorrência de uma ou mais falhas pode se propagar e causar danos enormes aos sistemas. A possibilidade de tais falhas leva à necessidade de existirem resiliência e medidas de segurança para garantir o menor dano possível neste evento.

Para construir um sistema de apoio em eventuais falhas, há grande relevância em conhecer o sistema, seus pontos fracos e pontos de importância, e então estabelecer uma meta de tolerância a ser alcançada. Assim serão estudados neste trabalho a identificação de tais pontos fracos e relações de toleràncias ao representar um sistema como uma rede complexa e executar simulações de falhas iniciais e seus efeitos em cascata, estabelecendo uma medida de carga para determinar se haverá ou não falhas subsequentes após uma iteração, procurando assim modelos e características de redes que promovem sua estabilidade.

1.1 Objetivo

Utilizar redes complexas para simular falhas em cascata a partir de diferentes remoções iniciais, comparando como diferentes modelos de redes, tolerâncias, grau médio e outros fatores afetam a rede a cada iteração ao tomar medidas da eficiência, número de nós da rede e do maior componente conexo, buscando encontrar características que garantem maior estabilidade da rede.

2 MATERIAIS E MÉTODOS

2.1 Conceitos de redes complexas

2.1.1 Definição

Grafos são estruturas de dados cujo objetivo é representar objetos abstratos que estão relacionados entre si, sem uma representação no mundo real, já redes complexas são grafos dentro de um contexto real e em grandes escalas ou com relações de conectividade não triviais, como por exemplo a Internet, malhas viárias e redes sociais.

2.1.2 Nós, arestas e grau

Nós ou vértices são objetos determinados por um contexto e que apresentam uma relação entre si, a qual é representada por uma ligação conhecida como aresta. Dado o exemplo de grafo da figura 1 a seguir.

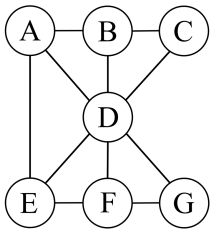


Figura 1: Exemplo de grafo com 7 nós e 11 arestas. Fonte: Elaborada pelo autor.

Para estudar o grafo, são necessárias medidas para caracterizá-lo[3], sendo a primeira grandeza a ser utilizada em sua caracterização o grau de um nó, determinado pelo número de arestas incidentes a ele, exemplificando pela figura 1, o nó A possui 3 arestas incidentes e, portanto, possui grau 3. São conhecidos como hubs os nós com maiores graus da rede, no caso da figura 1, o nó D é o maior hub do grafo tendo grau 6.

Dentro de um grafo podem ser determinados subconjuntos de nós e arestas que formam outro grafo dentro do original, sendo assim denominado um subgrafo. Caso existam subgrafos que não compartilham nós e que não são conectados entre si, cada subgrafo é um componente do grafo total, sendo aquele com o maior número de nós chamado maior componente conexo do grafo.

Há ainda o grau médio $\langle k \rangle$ da rede que indica, em média, o grau de cada nó na rede, calculado pela equação a seguir, sendo P(k) a distribuição de graus da rede.

$$\langle k \rangle = \sum_{k=0}^{\infty} P(k)k \tag{1}$$

2.1.3 Caminhos, centralidade e eficiência

No caso de grafos não ponderados, que foram utilizados neste trabalho, os caminhos entre dois nós são dados pelas sequências de nós percorridos a partir do nó de origem até o nó de destino, com o tamanho de um caminho sendo o número de arestas.

Dentre os caminhos de um par de nós, aqueles com o menor número de nós percorridos são os caminhos mínimos deste par, sendo possível existir múltiplos caminhos mínimos entre os nós.

A centralidade é um conceito que busca determinar uma ordem de importância entre os nós, sendo, por exemplo, definida pelos caminhos na rede.

Uma medida de centralidade é a intermediação, que define a importância de um nó i ao contar o número de caminhos mínimos entre todos os outros nós n, m da rede que passam por i. Não são inclusos caminhos onde i é um nó de origem ou destino.

A distância (d_{if}) entre dois nós é dada pelo número de arestas no caminho mínimo entre eles, e a eficiência deste par é o inverso de sua distância. Assim a eficiência global da rede é a média das eficiências de todos os pares de nós na rede, vista na equação 2.

$$E_{global} = \frac{1}{N(N-1)} \sum_{i \neq f} \frac{1}{d_{if}} \tag{2}$$

2.1.4 Carga

A carga é um indicador para definir se um nó irá falhar após algum evento na rede, que depende de sua carga anterior (C_0), sua nova carga (C_1) e a tolerância (T) do nó.

Um nó falha caso sua nova carga satisfaça a condição de sobrecarga

$$C_1 > (1+T)C_0. \tag{3}$$

Ao falhar, o nó e suas arestas incidentes são removidos da rede, possivelmente causando outras falhas por conta da mudança de caminhos mínimos de outros nós e assim ocorrendo uma falha em cascata.

Neste trabalho a carga foi definida pela intermediação, seguindo a equação 4, sendo $\sigma(i, f)$ o número de caminhos mínimos entre i e f, e $\sigma(i, f|v)$ o número de caminhos mínimos que passam pelo nó v.

$$C_B(V) = \sum_{i,f \in V} \frac{\sigma(i, f|v)}{\sigma(i, f)} \tag{4}$$

Para iniciar o efeito em cascata na rede é necessária a retirada inicial de um ou múltiplos nós, essa retirada inicial é uma falha quando os nós são removidos aleatóriamente, ou um ataque quando os nós são removidos seletivamente, como por exemplo removendo apenas o maior hub da rede.

Após a retirada inicial é verificado se há nós que satisfaçam a condição 3, se houver eles são destruídos junto com suas arestas e ao fim dessas remoções a condição 3 é verificada novamente na

rede, cada conjunto de remoções é uma iteração da falha em cascata, que se repete até não haver nós que satisfaçam a condição 3.

2.2 Modelos de redes complexas

2.2.1 Rede de livre escala

As redes de livre escala são definidas por suas distribuições de graus que seguem uma lei de potências conforme a equação 5, tal distribuição faz com que a rede tenha hubs muito característicos com graus muito maiores que a média da rede.

$$P(k) \sim k^{-\gamma} \tag{5}$$

A variável γ é um número real qualquer que costuma ser entre 2 e 3 quando aplicada a redes complexas. Um exemplo de rede de livre escala é a World Wide Web, cujo valor $\gamma = 2{,}1$ [4].

2.2.2 Modelo de Barabási-Albert

O modelo de Barabasi-Albert[5] é um gerador de grafo que utiliza conexão preferencial e gera uma rede de livre escala. O modelo é alimentado com um parâmetro natural m e inicia um grafo com ao menos m nós, adicionando por iteração um novo nó e o conectando com m nós existentes, priorizando nós com maior grau, até o tamanho estabelecido para a rede. A probabilidade da aresta ser criada com um nó de grau k é dada pela equação

$$p(k) = \frac{k}{\sum_i k_i} \tag{6}$$

sendo k_i o grau de cada nó já existente na rede.

Sendo uma rede de livre escala, a distribuição de graus é dada por uma lei de potência, com $\gamma \approx 3$.

$$P(k) \approx \alpha k^{-3} \tag{7}$$

.

Ao adicionar m ligações por novo nó, que contribui para o grau do novo nó e para outro já existente, o grau médio esperado de um grafo gerado pelo modelo de Barabasi-Albert é

$$\langle k \rangle = 2m \tag{8}$$

.

2.2.3 Modelo de Erdős-Rényi

O modelo de Erdos-Renyi[6] é caracterizado por gerar arestas aleatóriamente com probabilidade (p) constante, iterando entre todos pares de nós e determinando se a aresta será gerada. Pela probabilidade constante o modelo gera hubs menos característicos e grau médio que melhor descreve a rede, sendo calculado pela equação 9 com n sendo o número de nós da rede.

$$\langle k \rangle = p(n-1) \tag{9}$$

.

Pelo objeto de trabalho ser uma rede complexa, $n \gg 1$, assim

$$\langle k \rangle = pn \tag{10}$$

Igualando ao grau médio de Barabasi-Albert da equação 8, são relacionadas as grandezas do modelo de Erdos-Renyi com Barabasi-Albert.

$$p = \frac{2m}{n} \tag{11}$$

2.2.4 Modelo de configuração

O modelo de configuração[6] gera uma rede com uma sequência de graus providenciada em forma de lista, onde cada elemento da lista é o grau de um nó da rede. Detalhadamente, o gerador cria o grafo com n nós e atribui a cada nó um número de pontas livres dado pela sequência de graus, por fim são conectadas tais pontas livres em pares, formando assim as arestas da rede. Consequentemente, é exigido que o número de pontas livres seja par, portanto a soma dos graus na rede deve ser par. O algoritmo permite a geração de laços, que foram removidos de cada rede antes de iniciar cada simulação.

Assim foi escolhida uma sequência de graus que corresponde à distribuição de graus de uma rede de livre escala com grau mínimo fixo k_0.

$$P(k) = \alpha k^{\gamma} \tag{12}$$

Aplicando 12 na equação 1, é obtido o grau médio do gerador modelo de configuração dada uma distribuição de graus que segue uma lei de potência.

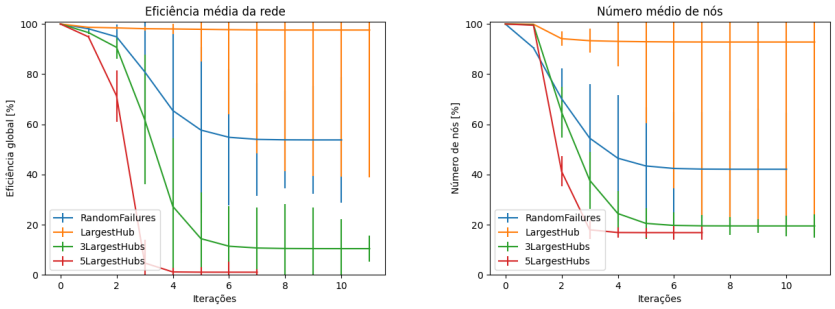
$$\langle k \rangle = \frac{\gamma - 1}{\gamma - 2} k_0 \tag{13}$$

3 RESULTADOS

3.1 Modelo de Barabási-Albert

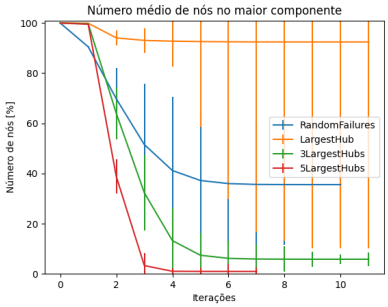
3.1.1 Remoção inicial

O primeiro conjunto de dados foi realizado com o modelo de Barabási-Albert, comparando os métodos de remoção, sendo eles ataques no maior hub, nos 3 e 5 maiores hubs, e 10% de falhas. A remoção inicial é aplicada na iteração 1 da figura 2, seguida das falhas em cascata nas iterações subsequentes.



(a)

(b)



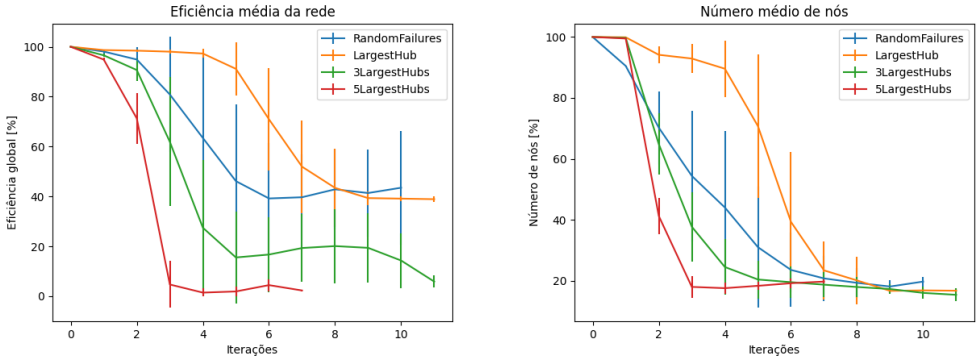
(c)

Figura 2: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede de Barabási-Albert, com 1000 simulações e parâmetros N = 1000, m = 5, T = 40%, com falhas iterando pela rede até que não ocorram mais sobrecargas. Fonte: Elaborada pelo autor.

Neste conjunto de parâmetro é notável a resistência de uma rede gerada por Barabási-Albert contra falhas, dado que mesmo com apenas 45% dos nós restando ao final da falha em cascata, a rede manteve perto de 55% de sua eficiência original.

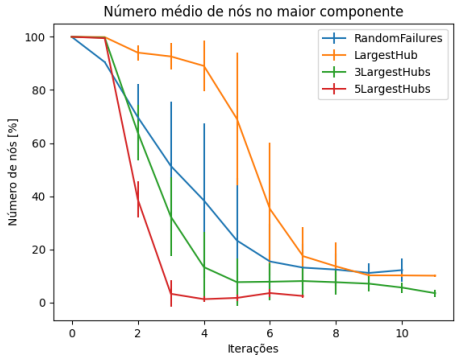
A rede porém se mostrou vulnerável a ataques dado que com apenas um ataque nos 3 maiores hubs, a rede perde cerca de 90% de sua eficiência e com um ataque nos 5 maiores hubs a rede é certa de se colapsar. Vemos ainda que o maior componente se manteve similar ao total da rede, indicando que não houve grandes separações em componentes na rede.

O enorme desvio padrão na remoção do maior hub é dado pelo fato que nem todas as simulações alcançam 11 iterações, dado que a maioria se estabilizou antes, por volta da quinta iteração sem colapsar a rede. Podemos ver na figura 3 abaixo as simulações ao descartar da média as redes que já estabilizaram.



(a)

(b)



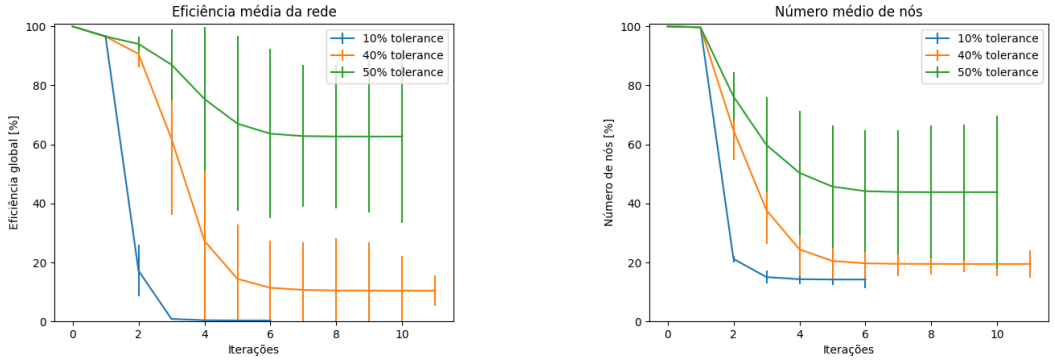
(c)

Figura 3: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede ao ignorar simulações finalizadas na média, com 1000 simulações e parâmetros N = 1000, m = 5, T = 40%. Fonte: Elaborada pelo autor.

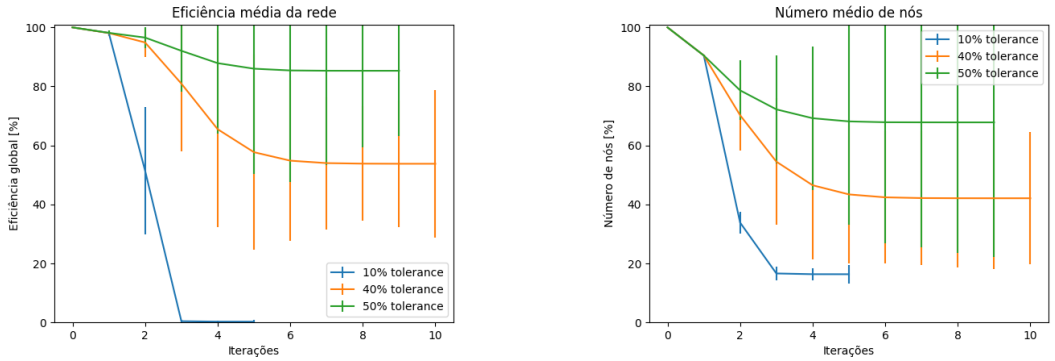
Pela figura 3 vemos que simulações que se estendem por mais iterações tenderam a se aproximar do colapso da rede, sendo que poucas chegaram nesse estado, causando assim o aumento do desvio padrão nas últimas iterações sem afetar significativamente a média das simulações.

3.1.2 Tolerância

Comparando agora valores para tolerância, foram simulados com ataque no maior hub e 10% de falhas, resultando, respectivamente, nos gráficos (a) e (b) da figura 4.



(a)



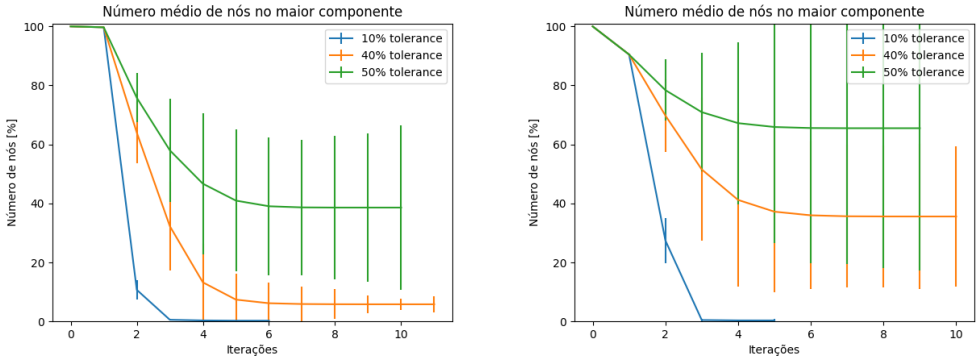
(b)

Figura 4: Evolução normalizada da eficiência e da contagem total de nós com 1000 simulações, N = 1000, m = 5, (a) ataque nos 3 maiores hubs, (b) 10% falhas. Fonte: Elaborada pelo autor.

Em 50% de tolerância a rede é quase estável após o ataque nos 3 maiores hubs, perdendo 30% de eficiência, enquanto perde cerca de 15% de eficiência após as 10% de falhas. Sabendo pela figura 2 que o ataque nos 3 maiores hubs foi a segunda remoção menos estável, é inferido que 50% de tolerância não é suficiente para a remoção dos 5 maiores hubs da rede, exigindo assim uma enorme tolerância para ser evitado.

Portanto, não é viável buscar apenas aumentar a tolerância da rede até obter resultados estáveis, dado que ao aplicar em um sistema real apenas este método seria financeiramente inviável.

Analisando o maior componente conexo da rede, vemos pela figura 5 que ele colapsou para apenas 5% de sua contagem de nós originais em 40% de tolerância no ataque nos 3 maiores hubs, indicando a separação do componente em diversos componentes menores, que enfraquece muito a rede ao gerar pares de nós que não possuem caminhos entre si.



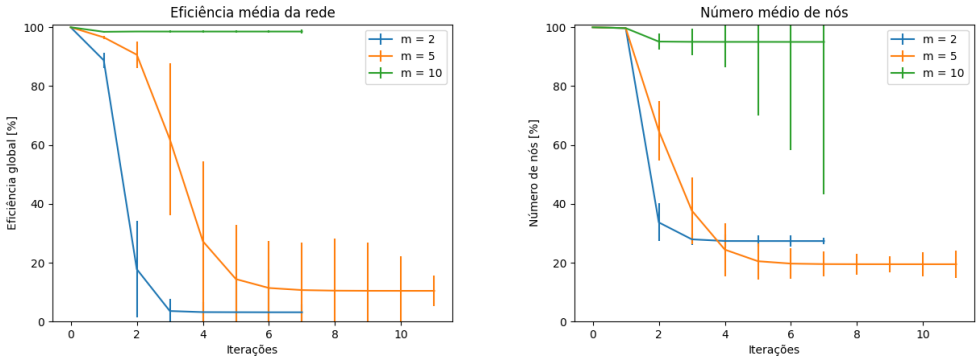
(a) (b)

Figura 5: Evolução normalizada da contagem de nós do maior componente da rede, com 1000 simulações e parâmetros N = 1000, m = 5, T = 40% com (a) ataque nos 3 maiores hubs, (b) 10% falhas. Fonte: Elaborada pelo autor.

3.1.3 Grau médio

Como último conjunto de medidas do modelo de Barabási-Albert, o grau médio dado pela equação 8 determina o quão robusta é a rede, como pode ser visto na figura 6.

Os valores de m usados nas simulações foram 2, 5 e 10, que equivalem aos graus médios, respectivamente, 4, 10 e 20.



(a) (b)

Figura 6: Evolução normalizada da (a) eficiência e (b) contagem total de nós para diferentes valores de m, com 1000 simulações e parâmetros N = 1000, T = 40% com ataque nos 3 maiores hubs. Fonte: Elaborada pelo autor.

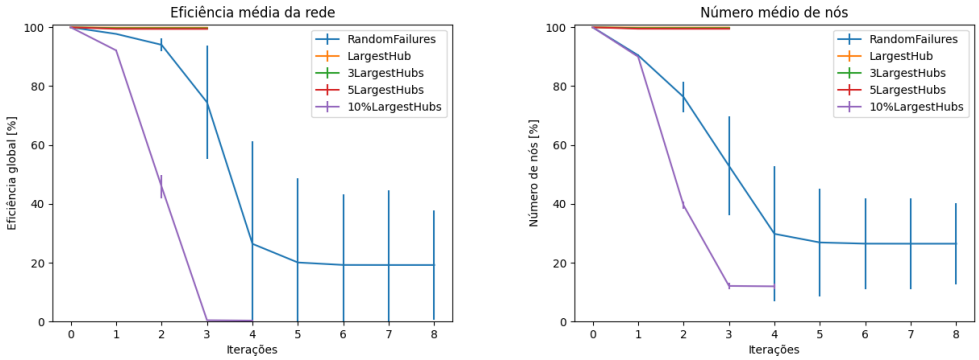
Notando que esta simulação foi realizada com um ataque nos 3 maiores hubs, a segunda remoção mais impactante testada neste modelo, praticamente não afetou a eficiência da rede quando m = 5, mesmo após perder 5% de seus nós, dado que há múltiplos caminhos mínimos entre a maioria dos pares de nós.

O aumento de m resulta no aumento do grau médio da rede e, portanto, do quão resiliente ela é, se mostrando a medida mais relevante para obter uma rede mais segura.

3.2 Modelo de Erdős-Rényi

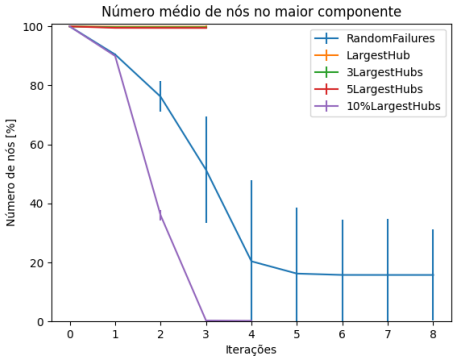
3.2.1 Remoção inicial

Utilizando agora o gerador de grafo aleatório, o modelo de Erdős-Rényi, serão realizadas comparações similares às de Barabasi-Albert, começando pelos tipos de remoção inicial comparados na figura 7.



(a)

(b)



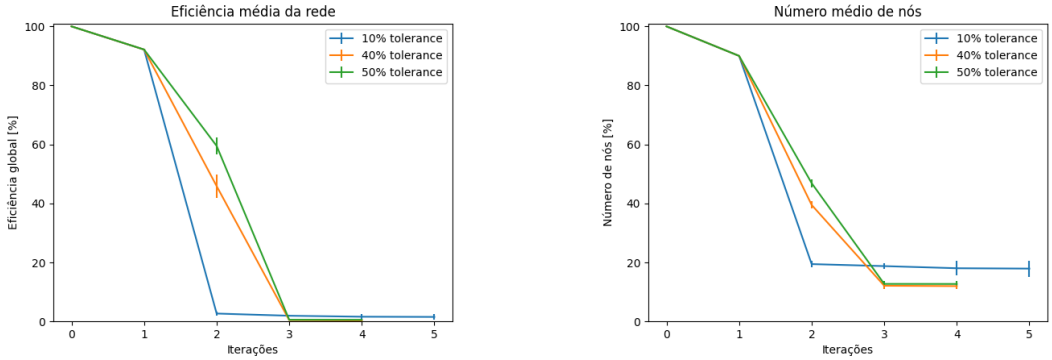
(c)

Figura 7: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede de Erdős-Rényi, com 1000 simulações e parâmetros N = 1000, p = 1%, T = 40% e 10% dos nós removidos nas falhas aleatórias. Fonte: Elaborada pelo autor.

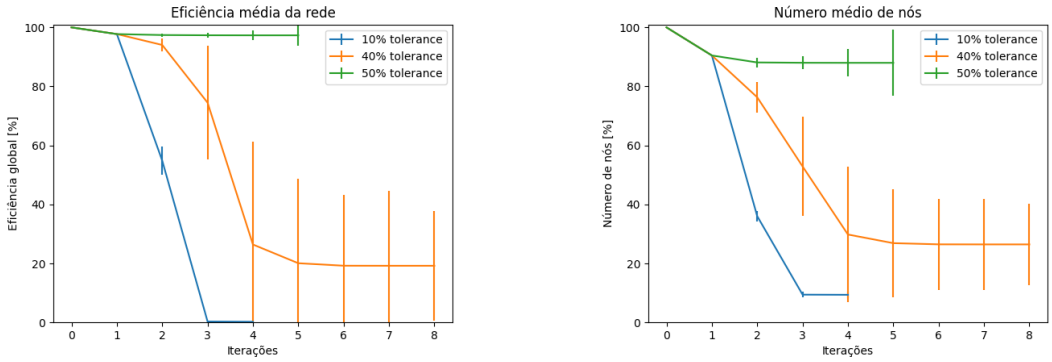
Assim como o modelo de Barabasi-Albert, o maior componente conexo do modelo de Erdős-Rényi também se apresentou similar à rede total, porém a eficiência da rede permanece aparentemente intocada ao atacar o maior, 3 maiores e 5 maiores hubs, colapsando totalmente apenas quando removidas quantidades significativas de hubs da rede.

3.2.2 Tolerância

Dado que a retirada de poucos hubs afetam minimamente a rede, foram simuladas as tolerâncias após o ataque nos 10% maiores hubs e após 10% de falhas com resultados apresentados na figura 8.



(a)



(b)

Figura 8: Evolução normalizada da eficiência e da contagem total de nós. comparando diferentes tolerâncias na rede, com 1000 simulações, N = 1000, p = 1%, (a) ataque nos 10% maiores hubs, (b) 10% falhas. Fonte: Elaborada pelo autor.

Pela figura 8 (a), é indicado que a existência de hubs ainda tem importância mesmo na rede aleatória, visto que após os 10% de falhas na figura 8 (b) a rede foi muito resistente com 50% de tolerância, permanecendo quase ilesa das falhas em cascata, promovendo um excelente aumento de confiabilidade da rede.

3.2.3 Grau médio

Com grau médio obtido pela equação 10, foram simulados conjuntos com probabilidades 0,4%, 1% e 2%, equivalendo respectivamente em graus médios 4, 10 e 20, com resuldados mostrados na figura 9.

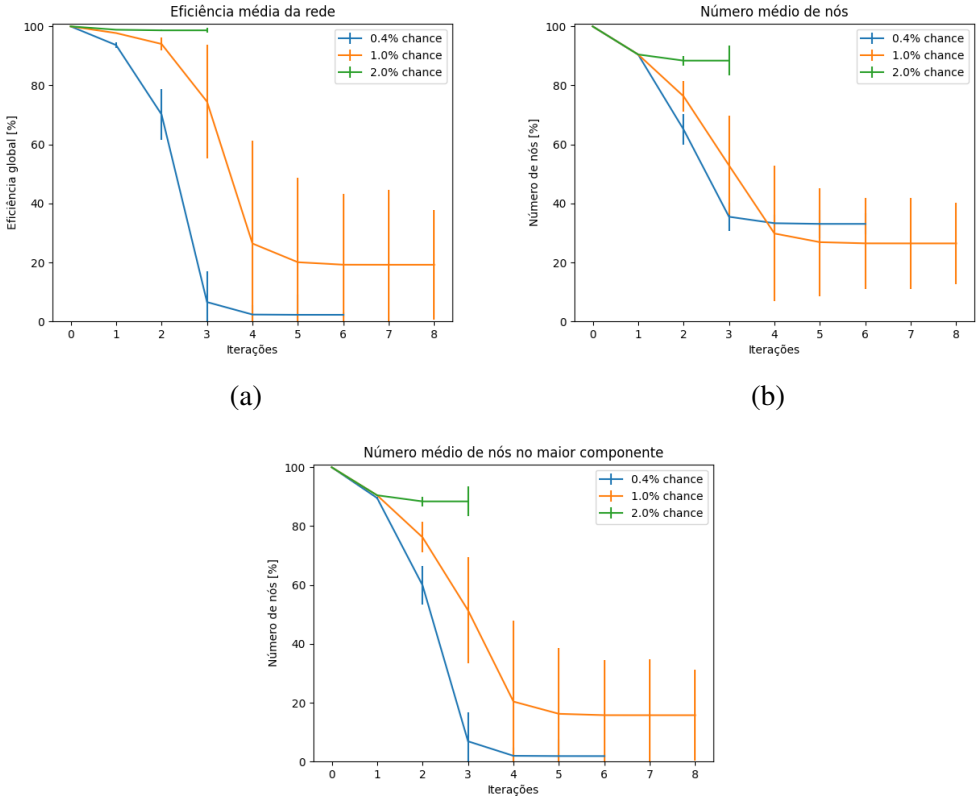


Figura 9: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede de Erdős-Rényi, comparando as probabilidades de gerar arestas, com 1000 simulações e parâmetros N = 1000, T = 40% com 10% de falhas. Fonte: Elaborada pelo autor.

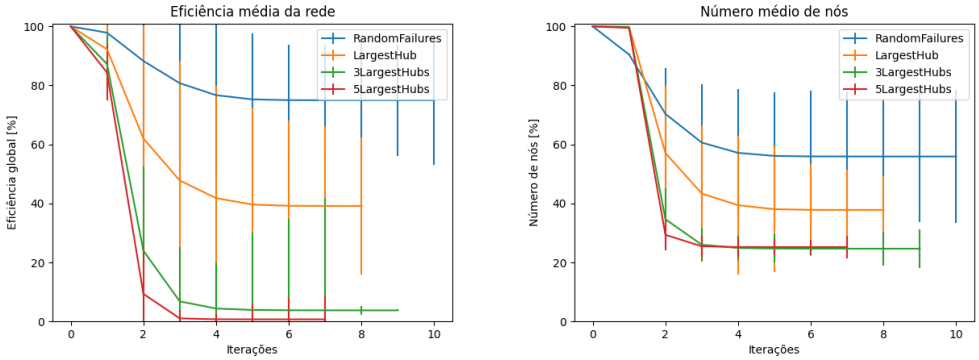
Similarmente ao modelo de Barabasi-Albert, o aumento do grau médio impacta significativamente na resistência da rede, estabilizando as falhas em cascata em apenas 4 iterações ao aumentar o grau médio para 20.

Nesta simulação ocorreu uma diferença entre os nós totais da rede e do maior componente conexo, que perdeu cerca de 99% dos nós no caso p = 0,4%, que foi a principal causa do colapso da rede dado que mesmo com 35% de seus nós originais, a eficiência da rede caiu para quase nula. A importância do maior componente é notável no fato que em p = 1%, mesmo com aproximadamente 5% de nós a menos que em p = 0,4%, a rede não colapsou totalmente e estabilizou em 30% de eficiência.

3.3 Modelo de configuração

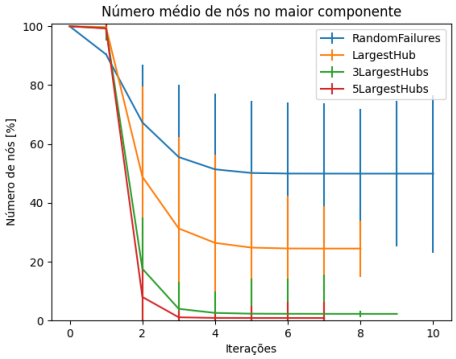
3.3.1 Remoção inicial

O último modelo simulado foi o modelo de configuração escolhendo a distribuição de graus dada pela equação 12.



(a)

(b)



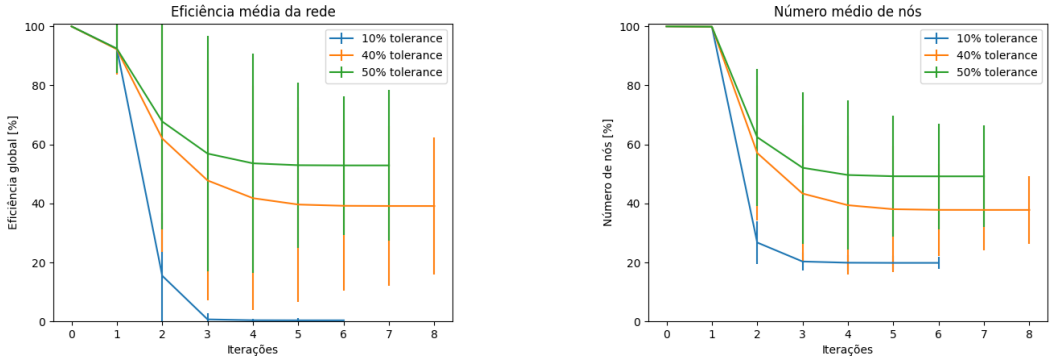
(c)

Figura 10: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede do modelo de configuração, com 1000 simulações e parâmetros N = 1000, $\langle k \rangle = 10$, $\gamma = 2{,}5$ e T = 40% e 10% dos nós removidos nas falhas aleatórias. Fonte: Elaborada pelo autor.

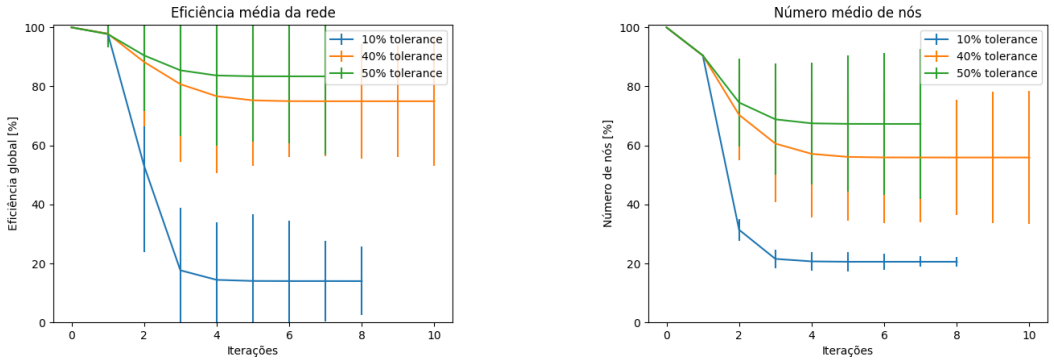
Analisando a figura 10, vemos que o modelo se mostrou similar ao de Barabasi-Albert na característica que possui maior resistência contra falhas, mas é vulnerável a ataques nos maiores hubs, o que é esperado dado que ambos são redes de livre escala ao escolher a equação 12 como distribuição de graus do modelo de configuração. O maior componente foi um fator importante nas simulações de ataque nos 3 e 5 maiores hubs, que causaram seu colapso total mesmo com 30% dos nós restantes.

3.3.2 Tolerância

As mesmas tolerâncias de 10%, 40% e 50% foram testadas no modelo de configuração.



(a)



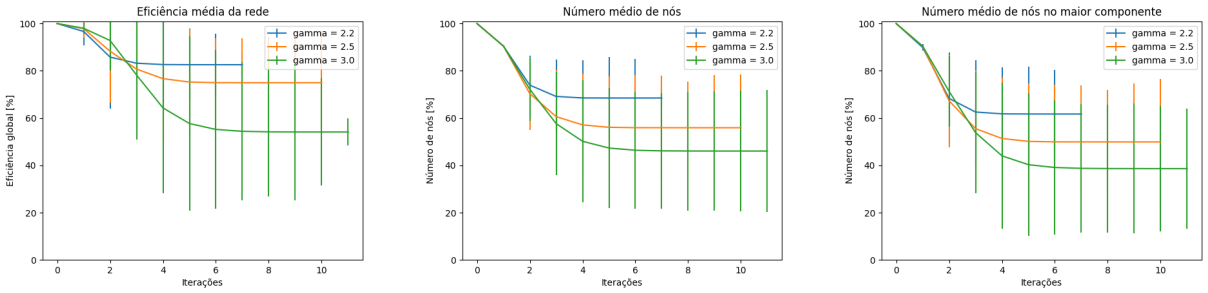
(b)

Figura 11: Evolução normalizada da eficiência e da contagem total de nós com 1000 simulações, N = 1000, $\langle k \rangle = 10$, $\gamma = 2{,}5$ com (a) ataque no maior hub, (b) 10% falhas. Fonte: Elaborada pelo autor.

No cenário da figura 11 não houve grande salto na eficiência da rede entre 40% e 50% de tolerância como ocorreu em Barabási-Albert e em Erdős-Rényi tanto no ataque quanto na falha, indicando que é necessário outro fator para melhorar a confiabilidade da rede, sendo esse o grau médio.

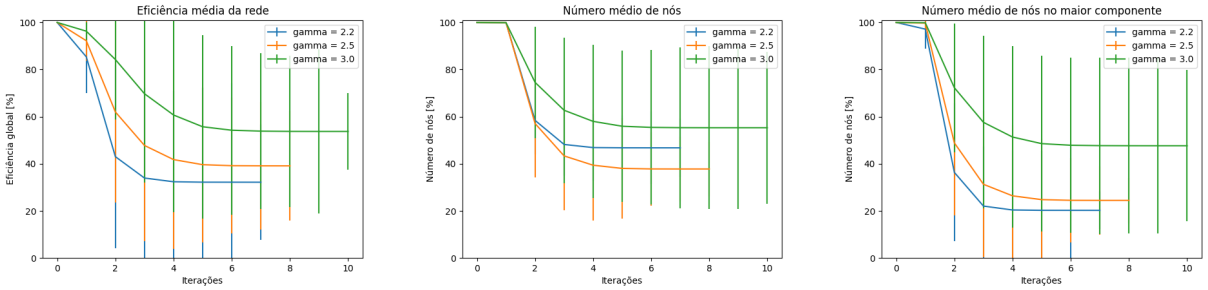
3.3.3 Coeficiente γ

Fixando o grau médio $\langle k \rangle = 10$, pode ser analisado o efeito da forma da lei de potências na distribuição de graus da rede ao variar γ e k_0 na equação 13, resultando nas figuras 12 e 13, respectivamente com 10% de falhas e ataque no maior hub.



(a) (b) (c)

Figura 12: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede do modelo de configuração, comparando diferentes γ com grau médio fixo $\langle k \rangle = 10$ e 10% de falhas, com parâmetros N = 1000 e T = 40% e 1000 simulações. Fonte: Elaborada pelo autor.



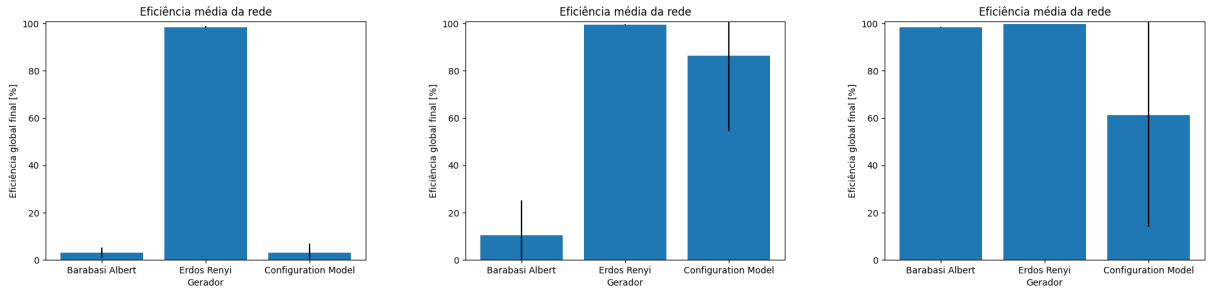
(a) (b) (c)

Figura 13: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente da rede do modelo de configuração, comparando diferentes γ com grau médio fixo $\langle k \rangle = 10$ e ataque no maior hub, com parâmetros N = 1000 e T = 40% e 1000 simulações. Fonte: Elaborada pelo autor.

Com 10% de falhas vistas na figura 12, a rede se torna mais resistente quanto mais γ se aproxima de 2, sendo que no ataque do maior hub na figura 13 o contrário acontece, isso se dá pelo fato que para manter o grau médio constante, ao aumentar γ é necessário aumentar k_0 também, fazendo com que a rede tenha um grau mínimo maior, que contribuem mais na eficiência da rede durante falhas. Simultaneamente, ao aumentar γ, os hubs se tornam menos característicos, fortalecendo a rede contra ataques.

3.4 Comparação entre os modelos

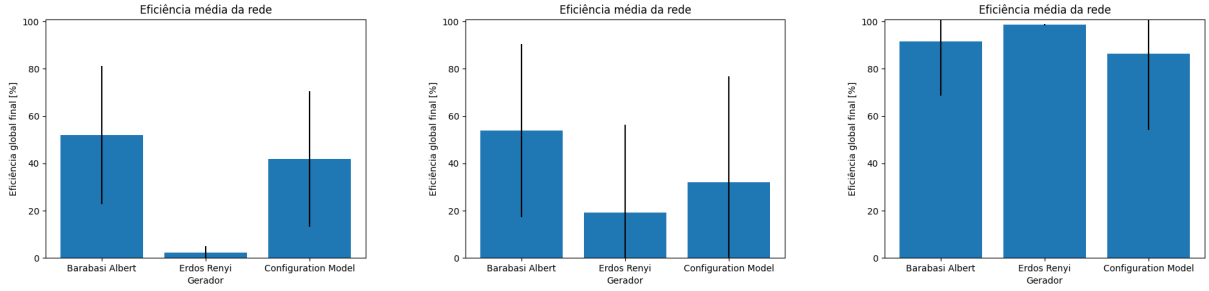
Ao longo das comparações por modelo de rede, os tipos de remoção mais relevantes foram o ataque nos 3 maiores hubs e 10% falhas, sendo assim os resultados finais das falhas em cascata por modelo foram comparados com essas remoções com 40% de tolerância. Na figura 14 foram comparados os modelos com diferentes graus médios.



(a) (b) (c)

Figura 14: Resultado das eficiências das redes por modelo com (a) $\langle k \rangle = 4$ e $\gamma = 2{,}98$, (b) $\langle k \rangle = 10$ e $\gamma = 4{,}31$, e (c) $\langle k \rangle = 20$ e $\gamma = 3{,}49$, atacando os 3 maiores hubs e usando N = 1000, T = 40%, 1000 simulações. Fonte: Elaborada pelo autor.

O modelo de Erdős-Rényi, por não possuir hubs característicos, predominou como o mais resistente em ataques na rede, perdendo apenas 1,5% de eficiência após as falhas em cascata ao atacar os 3 maiores hubs, enquanto o modelo de Barabási-Albert foi o que lidou pior com ataques, colapsando facilmente por conta de seus hubs muito característicos, precisando de um grau médio alto $\langle k \rangle = 20$ para resistir tal ataque, porém a vulnerabilidade em seus hubs permanece mesmo com o grau médio maior, essencialmente com mais hubs ainda maiores para suprir a ausência dos hubs que falham. Já o modelo de configuração apresentou características similares ao de Barabási-Albert, porém com maior número de hubs de grau menor, possibilitando que a sobrevivência da rede em $\langle k \rangle = 10$, porém apresentando resultados muito variados em $\langle k \rangle = 20$.



(a) (b) (c)

Figura 15: Resultado das eficiências das redes por modelo com (a) $\langle k \rangle = 4$ e $\gamma = 2{,}98$, (b) $\langle k \rangle = 10$ e $\gamma = 4{,}31$, e (c) $\langle k \rangle = 20$ e $\gamma = 3{,}49$, com 10% de falhas e usando N = 1000, T = 40%, 1000 simulações. Fonte: Elaborada pelo autor.

Já em 10% de falhas, o modelo de Barabasi-Albert é significativamente melhor, retendo metade de sua eficiência mesmo com grau médio $\langle k \rangle = 4$, porém com resultados variados conforme vistos na figura 3, onde algumas simulações se estendem até a rede chegar perto de colapsar, tal comportamento foi similar no modelo de configuração, enquanto o modelo de Erdős-Rényi tende a colapsar em cenários de falha.

É esperada similaridade entre os modelos de Barabási-Albert e modelo de configuração quando $\gamma = 3$ pela equação 7, assim foram feitas as comparações nas figuras 16 e 17.

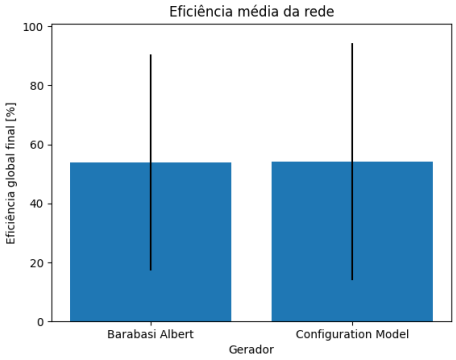
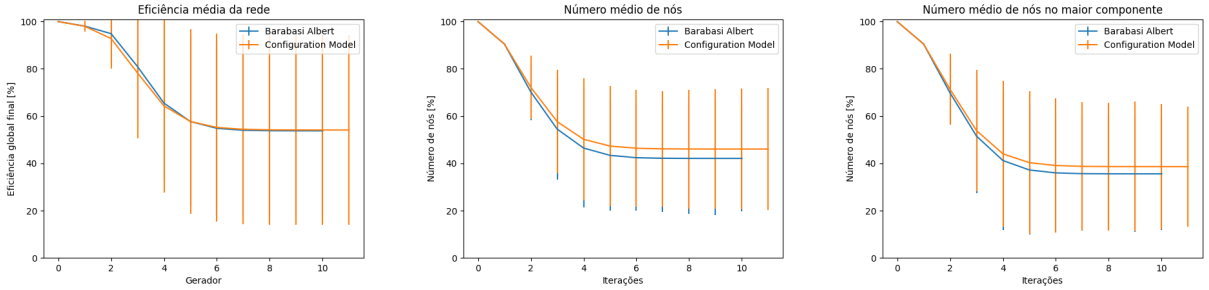


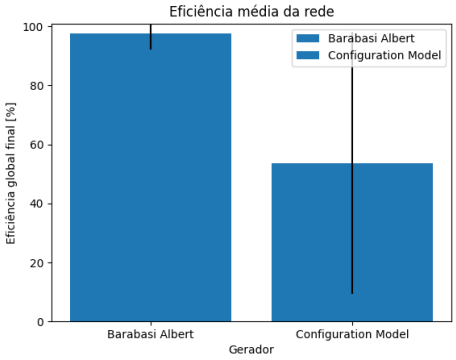
Figura 16: Resultado das eficiências das redes dos modelos de Barabási-Albert e modelo de configuração com grau médio $\langle k \rangle = 10$, usando N = 1000, T = 40%, 1000 simulações e 10% de falhas. Fonte: Elaborada pelo autor.



(a) (b) (c)

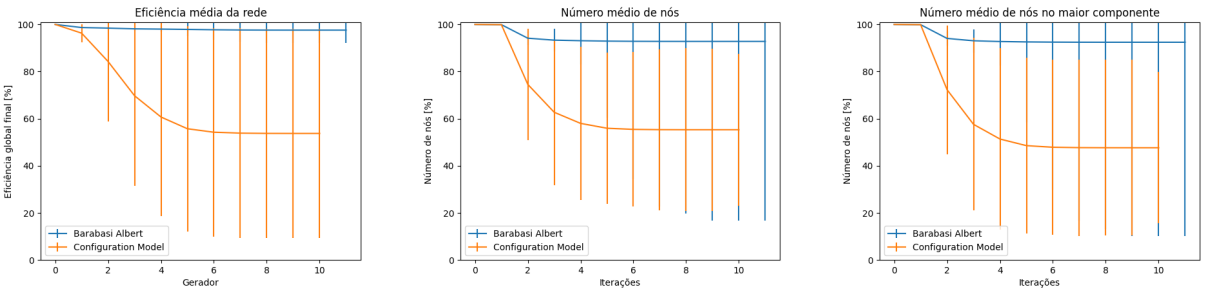
Figura 17: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente das redes de Barabási-Albert e modelo de configuração, com 1000 simulações e parâmetros N = 1000, $\langle k \rangle = 10$, $\gamma = 3$, m = 5, T = 40% com 10% de falhas. Fonte: Elaborada pelo autor.

Vemos que no cenário de 10% de falhas das figuras 16 e 17, os modelos se comportaram de forma idêntica, mesmo que com alto desvio padrão. Comparando agora pelo ataque no maior hub temos as figuras 18 e 19.



(a)

Figura 18: Resultado das eficiências das redes por modelo com (a) $\langle k \rangle = 4$ e $\gamma = 2{,}98$, (b) $\langle k \rangle = 10$ e $\gamma = 4{,}31$, e (c) $\langle k \rangle = 20$ e $\gamma = 3{,}49$, atacando o maior hub e usando N = 1000, T = 40%, 1000 simulações. Fonte: Elaborada pelo autor.



(a) (b) (c)

Figura 19: Evolução normalizada da (a) eficiência, (b) contagem de nós total e (c) do maior componente das rede de Barabási-Albert e modelo de configuração, com 1000 simulações e parâmetros N = 1000, $\langle k \rangle = 10$, $\gamma = 3$, m = 5, T = 40% com ataque no maior hub. Fonte: Elaborada pelo autor.

Com o ataque no maior hub da rede os modelos resultaram em falhas em cascata diferentes, com Barabási-Albert apresentando maior confiabilidade que modelo de configuração, ocorrendo pela diferença nas constantes multiplicativas das redes, que mesmo com graus médios iguais, causam diferentes graus mínimos e grau do maior hub, assim desencadeando diferenças nas simulações.

4 CONCLUSÕES E CONSIDERAÇÕES FINAIS

Com isso foram estudados diferentes características topológicas, modelos de redes complexas, falhas em cascata e a progressão de tais falhas ao relacionar com tais características, o modelo de Barabási-Albert provou grande confiabilidade em falhas, porém grande vulnerabilidade em ataques, onde ao remover cerca de 3 maiores hubs da rede foi suficiente para fazê-la colapsar por usar a conexão preferencial durante a geração da rede, que tende a atribuir novas arestas a nós que possuem maior grau, no entanto as cascatas geradas por ataques podem ser suprimidas com o aumento da tolerância

e do grau médio da rede, cujo impacto na eficiência da rede foi efetivo em medidas razoáveis quando considerada a viabilidade desta melhoria.

As redes geradas pelo modelo de Erdős-Rényi apresentaram distribuição de graus que não favorecem a geração de hubs, criando uma rede com graus mais próximos da média e assim essas redes foram intocadas por ataques nos maiores hubs, apenas colapsando no cenário de múltiplas falhas, porém com a tolerância afetando fortemente a ocorrência de cascatas, permitindo uma rede que antes perdia 80% de eficiência a perder menos de 5% apenas ao subir a tolerância dos nós de 40% para 50%, tendo influência semelhando quando variado o grau médio.

O modelo de configuração por fim apresentou resultados potencialmente balanceados entre ataques e falhas, com γ idealmente entre 2 e 3 visto que abaixo de 2 a distribuição de graus da rede diverge, enquanto acima de 3 a rede se torna mais dispersa, com grau médio, tamanho e quantidade de hubs menores, proporcionando melhor resistência contra ataques, porém mais vulnerável a múltiplas falhas. Foram ainda comparados os modelos Barabási-Albert e modelo de configuração quando $\gamma = 3$ e $\langle k \rangle = 10$, sendo encontrado que os modelos se comportam de forma idêntica em falhas, porém o modelo de configuração gerou redes com hubs mais dominantes, que causou na maior perda de eficiência durante ataques no maior hub, sendo assim o modelo de Barabási-Albert gerou redes mais seguras que as de modelo de configuração com distribuição de nós como uma lei de potências.

Assim foram estudados fatores que podem influênciar na segurança de uma rede complexa, que pode representar, por exemplo, o tráfego de informações na Internet e de veículos nas ruas, permitindo que nos eventos de queda de servidores e interdições em trechos da malha viária, seja possível prever os pontos que o fluxo será redirecionado e estabelecer medidas para aliviar possíveis sobrecargas.

REFERÊNCIAS

[1] VALDEZ, Lucas D.; SHEKHTMAN, Louis; LA ROCCA, Cristian E.; ZHANG, Xin; BULDYREV, Sergey V.; TRUNFIO, Paul A.; BRAUNSTEIN, Lidia A.; HAVLIN, Shlomo.*Cascading failures in complex networks*.**Journal of Complex Networks**, v. 8, n. 2, cnaa013, abr. 2020.

[2] HASEGAWA, Takehisa. *An Introduction to Complex Networks*. **Graduate School of Information Sciences, Tohoku University, Sendai**, 980-8579, Japan, received Sept. 6, 2011; final version accepted Oct. 11, 2011.

[3] COSTA, L. da F.; RODRIGUES, F. A.; TRAVIESO, G.; VILLAS BOAS, P. R. *Characterization of complex networks: a survey of measurements*. **Advances in Physics**, v. 56, n. 1, p. 167–242, abr. 2007.

[4] ALBERT, R.; BARABÁSI, A.-L. *Statistical mechanics of complex networks*. **Reviews of Modern Physics**, v. 74, n. 1, p. 47–51, jan. 2002.

[5] BARABÁSI, A.-L.; ALBERT, R. *Emergence of scaling in random networks*. **Science**, v. 286, n. 5439, p. 509–512, 1999.

[6] BOLLOBÁS, B. *Modern Graph Theory*. New York: Springer, 1998. (Graduate Texts in Mathematics, v. 184).