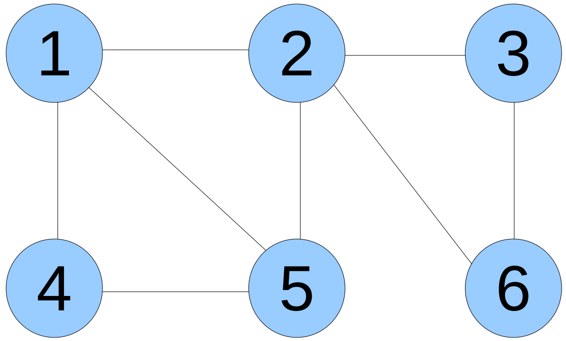
Redes Complexas
Aula 13

Roteiro

- Falhas em redes
- Medindo robustez
- Tipos de falha
- Influência da estrutura
- Ponto crítico

Redes e Falhas

- Rede: muitas vezes é uma abstração de um sistema real
  - ex. Internet, rede social, web
- “Componentes” da rede podem falhar
  - vértices ou arestas



Quando falhas ocorrem temos mudanças na estrutura da rede

Robustez da Rede

- Capacidade da rede de *operar* na presença de falhas (*fault tolerant*)
  - vértices ou/e arestas
- Medidas de robustez da rede
  - muitas métricas, depende do contexto
- Robustez em função da estrutura da rede
  - impacto da rede na robustez
- Aplicação depende do contexto
  - ex. robustez da Internet a falhas nos AS

Métricas de Robustez

- Métricas locais
  - impacto em um ou poucos vértices
  - ex. número de arestas para desconectar um vértice qualquer
- Métricas globais
  - impacto na rede como um todo
  - ex. tamanho da componente gigante

Maior interesse em métricas globais

Métricas Globais

- Tamanho da componente gigante
  - absoluto ou relativo
- Tamanho médio das componentes
  - excetuando a componente gigante
- Distância média entre todos os pares
- Diâmetro da rede
- Corte mínimo da rede

Muitas outras são possíveis!

Tipo de Falhas

- Modelo para falha de vértices ou arestas
- Aleatoriamente
  - uniforme: todos tem mesma prob de falhar
  - não-uniforme: seguindo algum fenômeno
- Deterministicamente
  - Definir ordenação: quem falha primeiro, segundo, etc.
  - ex. ordenação decrescente por grau
- Falhas por defeito: modelo aleatório
  - ex. roteador da rede queimou
- Falhas propositais: modelo determinístico
  - ex. roteador da rede foi atacado

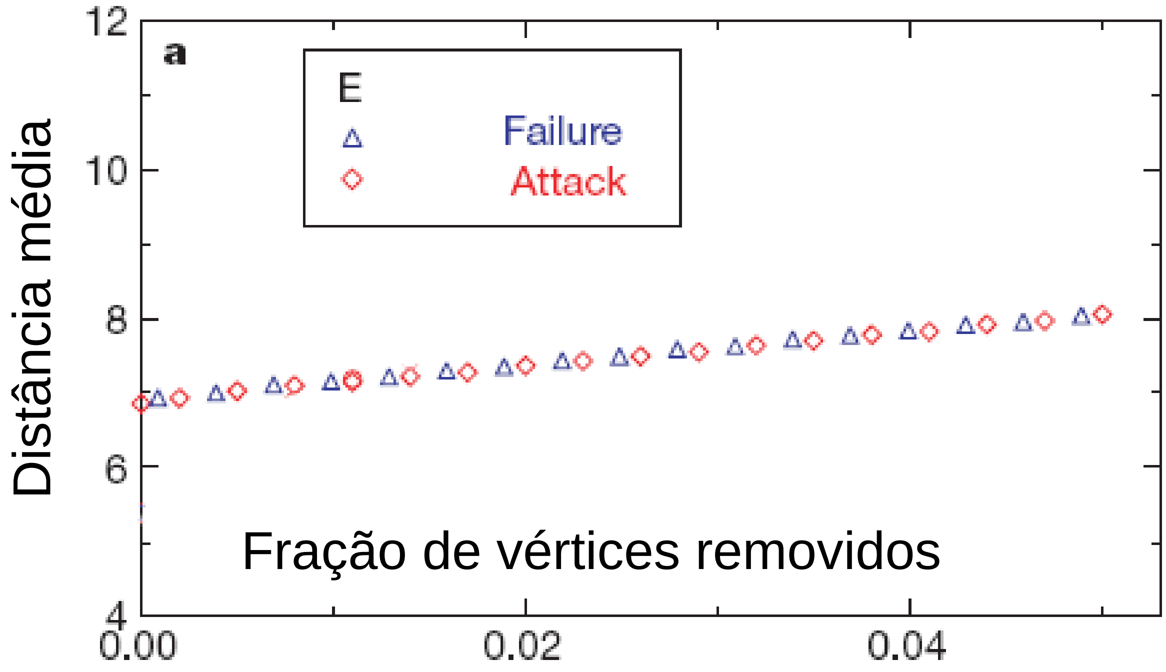
Robustez e Falhas

- Robustez da rede na presença de falhas
  - Aleatórias (uniforme), determinísitica (grau)
  - ex. distância média entre pares
- Diferença com relação ao tipo de falha?
  - para uma mesma fração que falha
- Influência da estrutura da rede?
  - para mesmo n e grau médio

Modelo G(n,p)? Modelo BA?

Falhas no G(n,p)

- Falhas aumentam (mas não muito) a distância média entre vértices
- Falhas aleatórias se parecem com falhas determinísticas
  - grau máximo é próximo ao grau médio

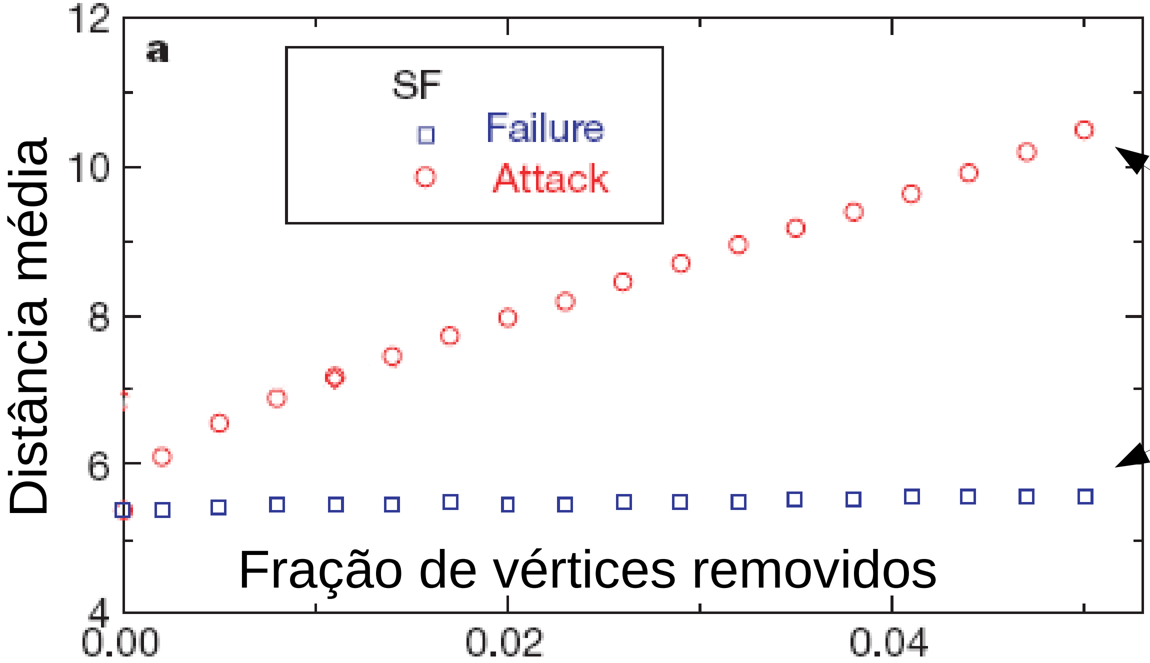


- n = 10000, <D> = 4

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Falhas no BA

- Falhas aleatórias **não** se parecem com falhas determinísticas
- Falhas aleatórias: pouco impacto
  falhas determinísticas: muito impacto



- n = 10000, <D> = 4

5% dos vértices removidos; distância média dobrou!

5% dos vértices removidos; distância média não variou

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Falhas Aleatórias

- Rede do Modelo BA

- Remoção aleatória (uniforme)
- Pouco impacto na estrutura da rede

Falhas Determinísticas

- Rede do Modelo BA

- Impacto devastador
- Tipo de falha e rede tem papel fundamental

Modelo BA

- Distribuição do grau segue lei de potência

- Maioria dos vértices tem grau pequeno
- Pouca importância na rede

- Poucos vértices com grau grande
- Interconectam a rede

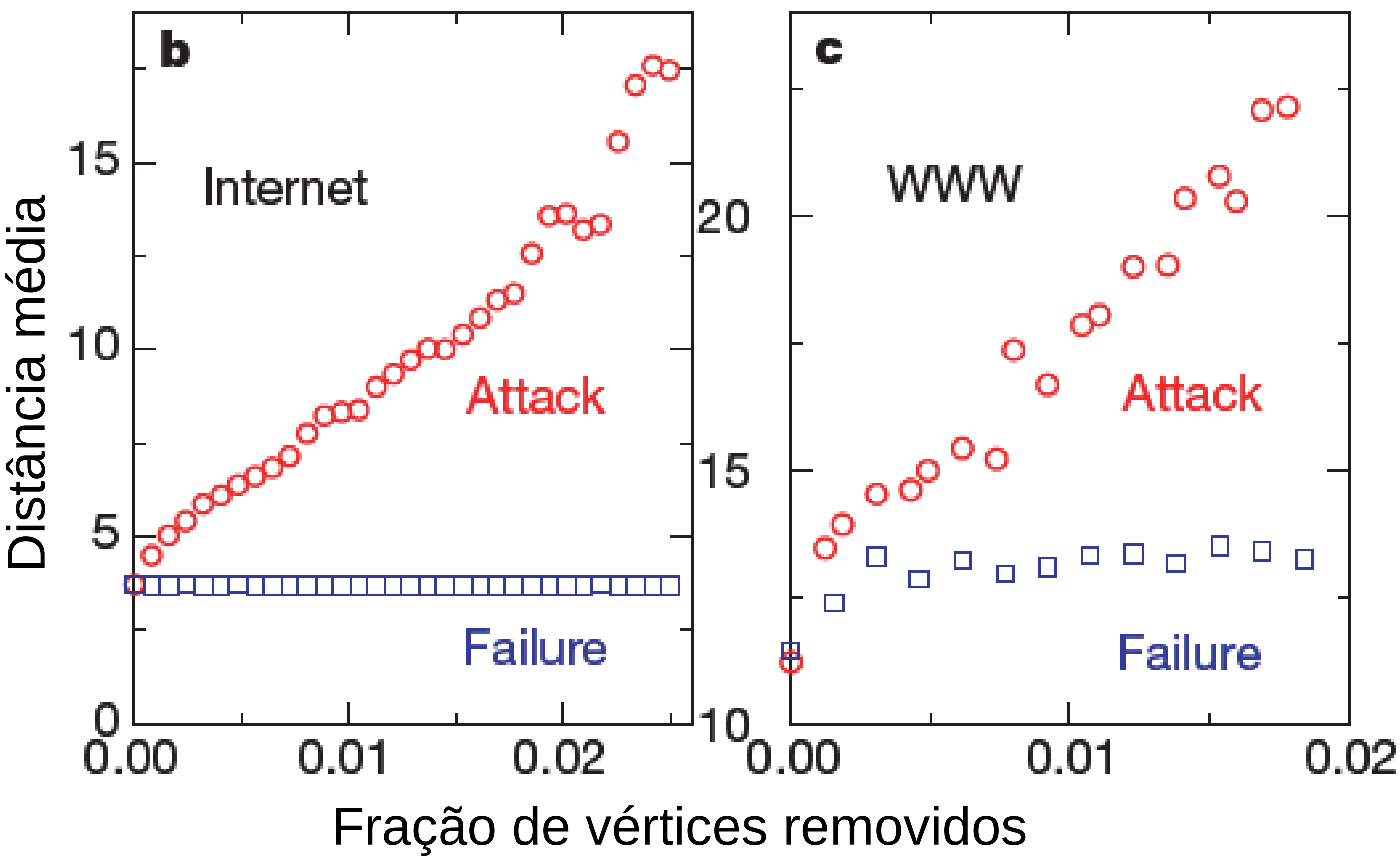
- Tolerante a falhas aleatórias

- Vulnerável a ataques direcionados

Propriedades de redes livre de escala!

Robustez em Redes Reais

- WebGraph, AS Graph
  - Redes seguem lei de potência no graus

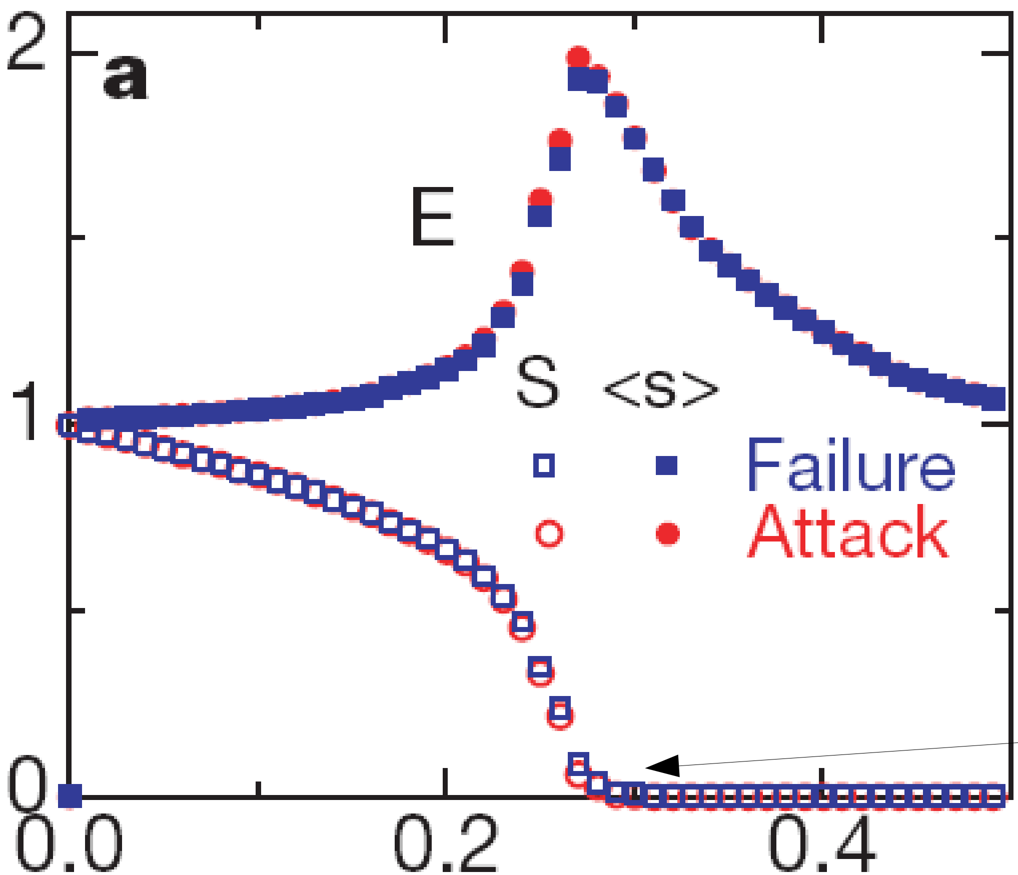


- Comportamento parecido com modelo BA
- Tolerante a falhas, vulnerável a ataques
- AS não é roteador!

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Outras Métricas: G(n,p)

- Tamanho relativo da componente gigante (GCC)
- Tamanho médio das outras componentes



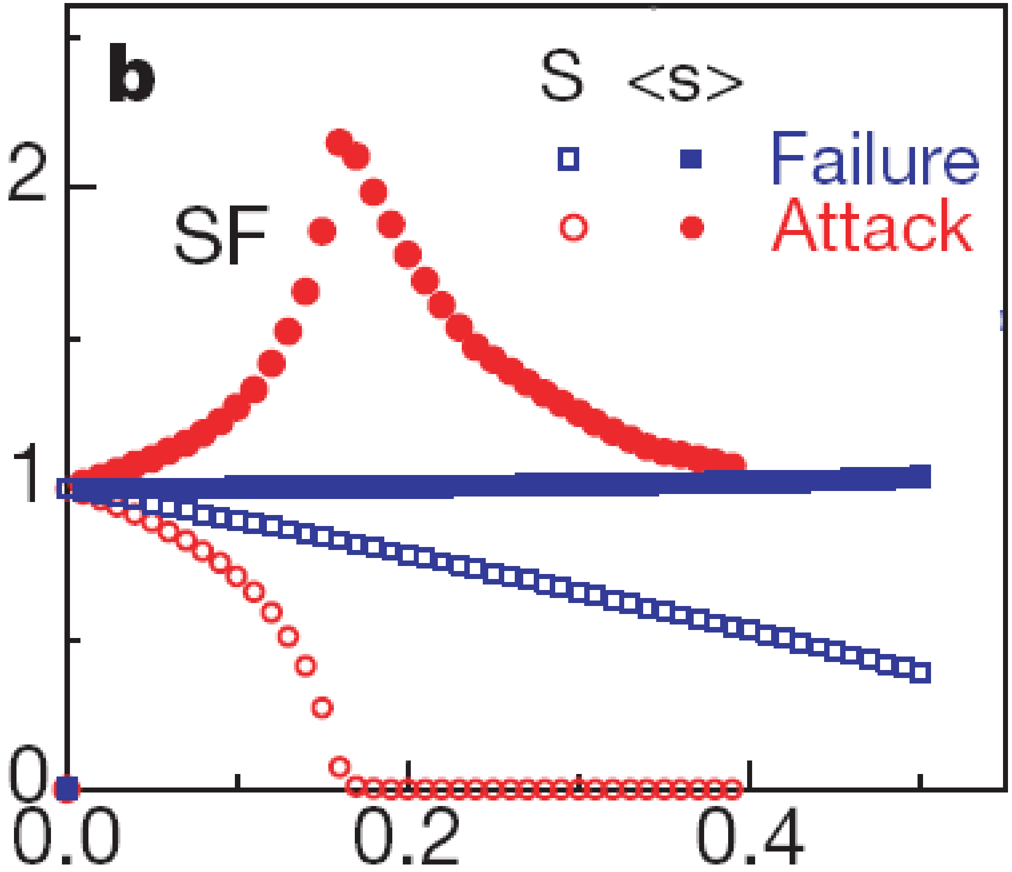
- Falhas eventualmente destroem componente gigante (S)
- Tamanho médio das outras componentes vai a um
- Rede despedaçada!

Transição de fase?

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Modelo BA

- Falha aleatória muito diferente de falha determinística



- Decrescismento linear do tamanho relativo da GCC (S)
- Tamanho médio das outras CC é 1
- Rede despedaça para falhas direcionadas
- Bem antes que rede do G(n,p)

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

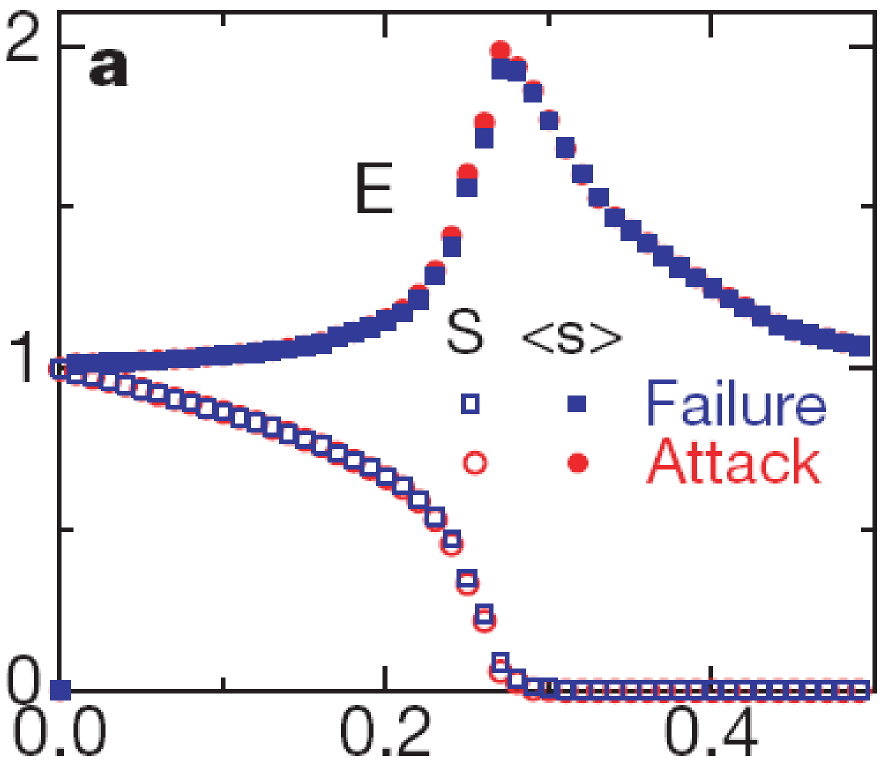
Transição de Fase

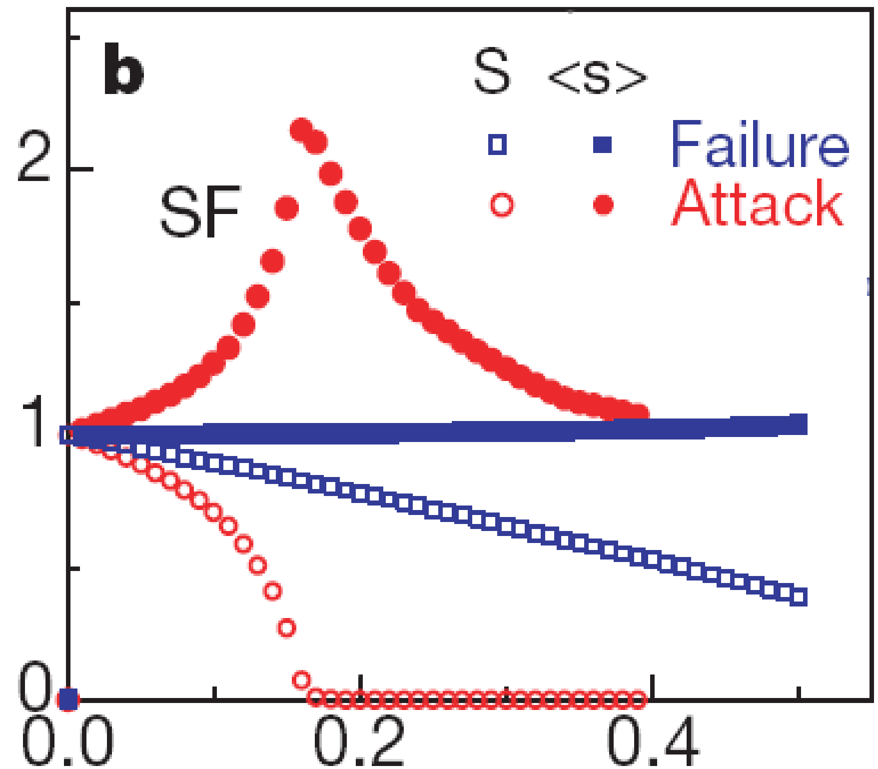
- Tamanho relativo da componente gigante
  - vai a zero rapidamente, para p grande suficiente

Valor de p que desintegra GCC?

- Depende do modelo de falhas
  - aleatório ou determinístico
- Depende da estrutura
  - G(n,p), BA, etc

Tamanho da Maior CC





- G(n,p), indiferente quanto ao tipo de falha
- BA, “robusta enquanto frágil”

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. Nature, 406(6794), 378-382.

Estudo Analítico

- GCC : componente conexa gigante
  - maior componente conexa tem εn vértices, para algum $\varepsilon > 0$, a.a.s.
- Condição (aprox) para termos uma GCC em um grafo aleatório qualquer

$$\kappa = \frac{E[d^2]}{E[d]} > 2$$

- Depende apenas do primeiro momento E[d] e do segundo momento $E[d^2]$ da distribuição do grau
- Condição para GCC no modelo G(n,p)?
  - $E[d] > 1$, grau médio maior que 1

Estudo Analítico

- Distribuição do grau após falhas determina existência da GCC
- Calcular os dois momentos da distribuição de grau (após a falha)
- Verificar a relação

$$\kappa = \frac{E[d^2]}{E[d]} > 2$$

Distribuição do Grau

- Considere distribuição de grau original
  - P[D = k], é dada
- Após falha dos vértices, qual nova distribuição do grau?
  - P[D' = k]
- Depende do modelo de falhas!
- Assumir modelo aleatório (uniforme)
- Obs: remover uma fração ***p*** dos vértices equivale a cada vértice ser removido com probabilidade ***p***

Distribuição do Grau

- Dado grau original k, probabilidade do grau ser k' após falha?
  - k – k’ vizinhos precisam falhar

$$P[D'=k' | D=k] = \binom{k}{k'} (1-p)^{k'} p^{k-k'}$$

- Descondicionando

$$P[D'=k'] = \sum_{k=k'}^{n-1} P[D=k] \binom{k}{k'} (1-p)^{k'} p^{k-k'}$$

Distribuição original
(antes das falhas)

Momentos e Ponto Crítico

- Podemos calcular os momentos de D' (distribuição do grau após falhas)
  - em função dos momentos da distribuição de grau

$$E[D']=E[D](1-p)$$

$$E[D'^2]=E[D^2](1-p)^2+E[D]p(1-p)$$

- Usando a condição, podemos determinar o ponto crítico, p_c

$$p_c=1-\frac{E[D]}{E[D^2]-E[D]}$$

Momentos da distribuição de grau original (pré-falhas)

- Valores menores de *p* mantém uma GCC

Graus com Lei Potência

- Ponto crítico em redes cujo grau segue lei de potência

$$p_c = 1 - \frac{E[D]}{E[D^2] - E[D]}$$

- Lei de potência: $P[D=k] = C k^{-\alpha}$
- Para $\alpha < 3$, segundo momento diverge
  - logo, $p_c = 1$
- Não existe transição de fase neste caso
- GCC nunca se desintegra (quando n tende infinito)
- Rede é altamente tolerante a falhas!

R Cohen, K Erez, D ben-Avraham, and S Havlin, "Resilience of the Internet to Random Breakdowns"
Phys. Rev. Lett. 85, 4626 (2000)

Graus com Lei Potência

- Para $\alpha > 3$, o que acontece?
- Temos os dois momentos defindos
  - dependem de α (exponente)
- Relação aproximada entre p_c e α
  - quanto maior α , menor é o valor de p_c
  - cauda menos pesada desintegra mais facilmente

R Cohen, K Erez, D ben-Avraham, and S Havlin, "Resilience of the Internet to Random Breakdowns".
Phys. Rev. Lett., 85, 4626 (2000)

Callaway, D. S., Newman, M. E., Strogatz, S. H., & Watts, D. J. “Network robustness and fragility: Percolation on random graphs”.
Phys. Rev. Lett., 85(25), 5468 (2000).

Generalizando Análise

- Análise anterior para falhas aleatórias e uniforme
- Generalização para falhas aleatórias em função do grau
- Generalização para falhas determinísticas
  - em função do grau
- Análise do ponto crítico, do tamanho das componentes gigante, tamanho médio das outras componetes
- Análise via percolação e função geradora

Cohen, R., Erez, K., Ben-Avraham, D., & Havlin, S. “Breakdown of the internet under intentional attack”. Phys. Rev. Lett., 86(16), 3682 (2001).

Callaway, D. S., Newman, M. E., Strogatz, S. H., & Watts, D. J. “Network robustness and fragility: Percolation on random graphs”. Phys. Rev. Lett., 85(25), 5468 (2000).