

Redes Complexas: Internet, Web e outras aplicações em computação

-Bloco #5-

2º semestre de 2008

“Robustez e Vulnerabilidade de Redes”

Virgílio A. F. Almeida

Setembro de 2008



Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

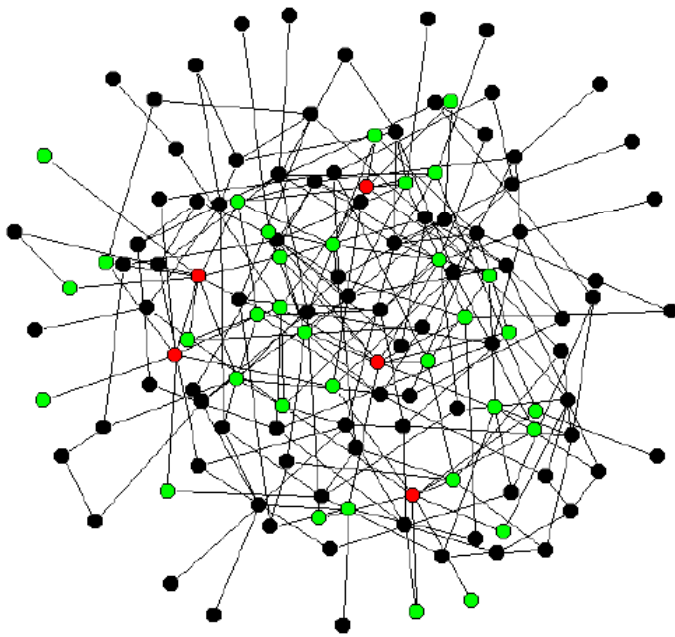
Redes: Robustez e Vulnerabilidade

- O que robustez? Robusto a que?
 - Falhas e ataques: qual a diferença
 - Aplicações (**)
- Tipos de redes:
 - Complexas
 - Randomicas (ER) e Power-Laws (***)
- Como testar:
 - S e <s>: por que?

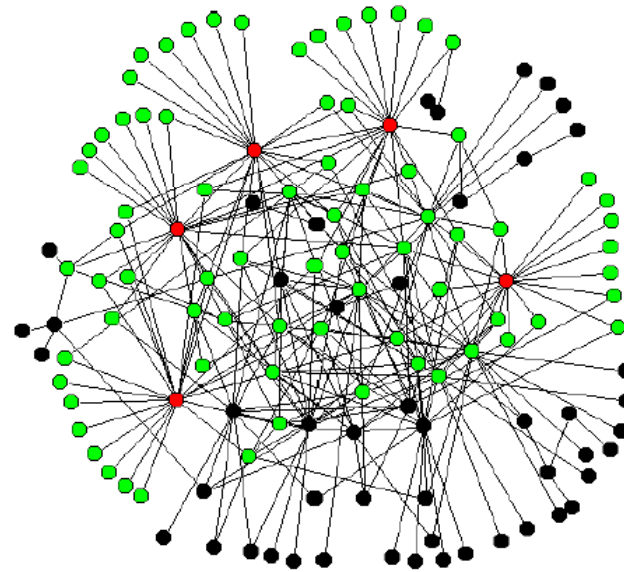
Revisão de Artigos

- **The internet's achilles' heel: Error and attack** tolerance of complex networks - R Albert, H Jeong, AL Barabasi - Nature, 2000
- http://www.nd.edu/~networks/PublicationCategories/JournalArticles/Physics/ErrorAttack_Nature.pdf
- **Efficiency of scale-free networks:** Error and attack tolerance of complex networks, Crucitti, V Latora, M Marchiori, A Rapisarda - Physica A: Statistical Mechanics and its Applications, 2004 – Elsevier
- http://www.ct.infn.it/~latora/next_errors.pdf

Ilustração visual das diferenças



Exponential



Scale-free

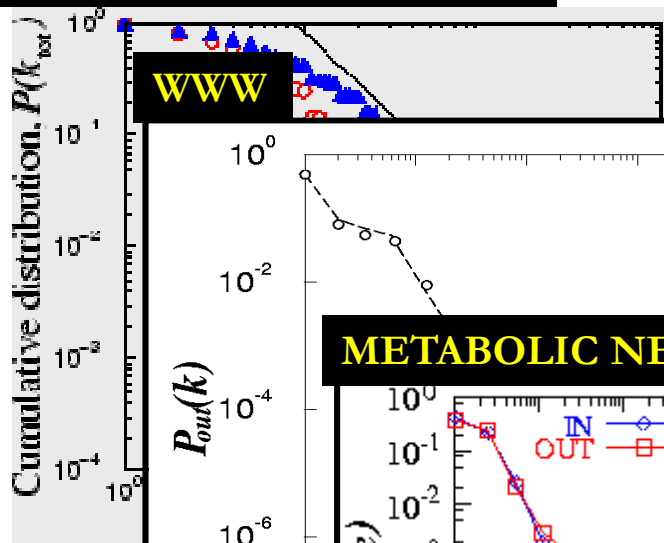
Falhas e Ataques a Redes

- Falha – remoção de nodos randômicos da rede
- Ataque – remoção de nodos escolhidos (i.e., importantes da rede).
- Consequência: perda de integridade da rede, caracterizada pela presença de um “giant connected component”.
- Métricas para medir o impacto do ataque
 - Caminho mínimo médio (distância)
 - Tamanho relativo do maior componente conectado
 - Tamanho médio dos componentes conectados, excluindo o gigante

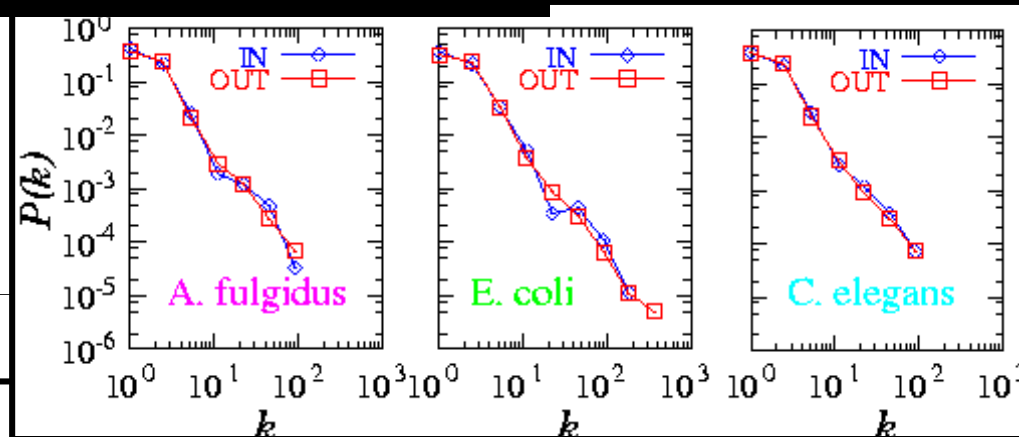
Redes com Distribuições Power-Law: Scale Free

-
-

SEXUAL PARTNERSHIPS



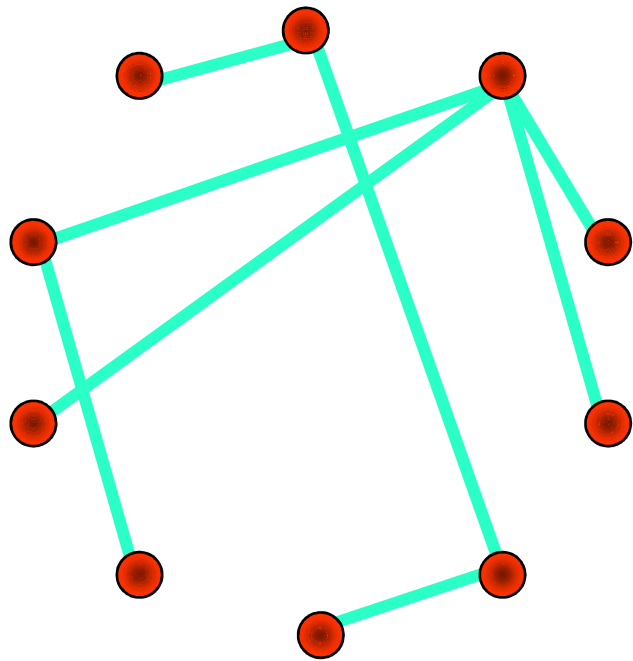
METABOLIC NETWORKS






H. Jeong et al, Nature, 407 651 (2000)

Referência para comparação

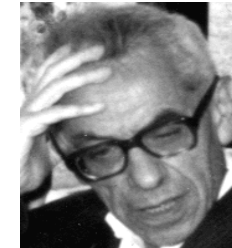
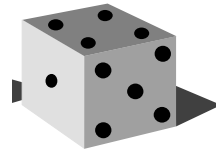
Rede Randomicas: Erdős-Renyi



-  = vertices (nodos)
-  = aresta (links)
-  = grau de vertice (# de links)

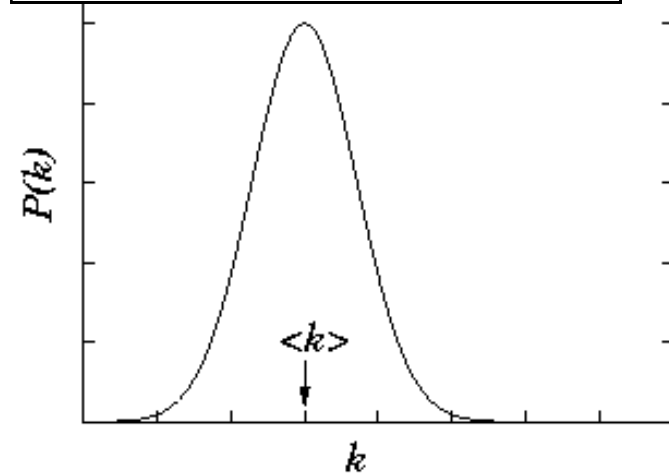
$$P(k) = \frac{e^{-\lambda} \lambda^k}{k!}$$

$$p=1/6$$
$$N=10$$
$$\langle k \rangle \sim 1.5$$



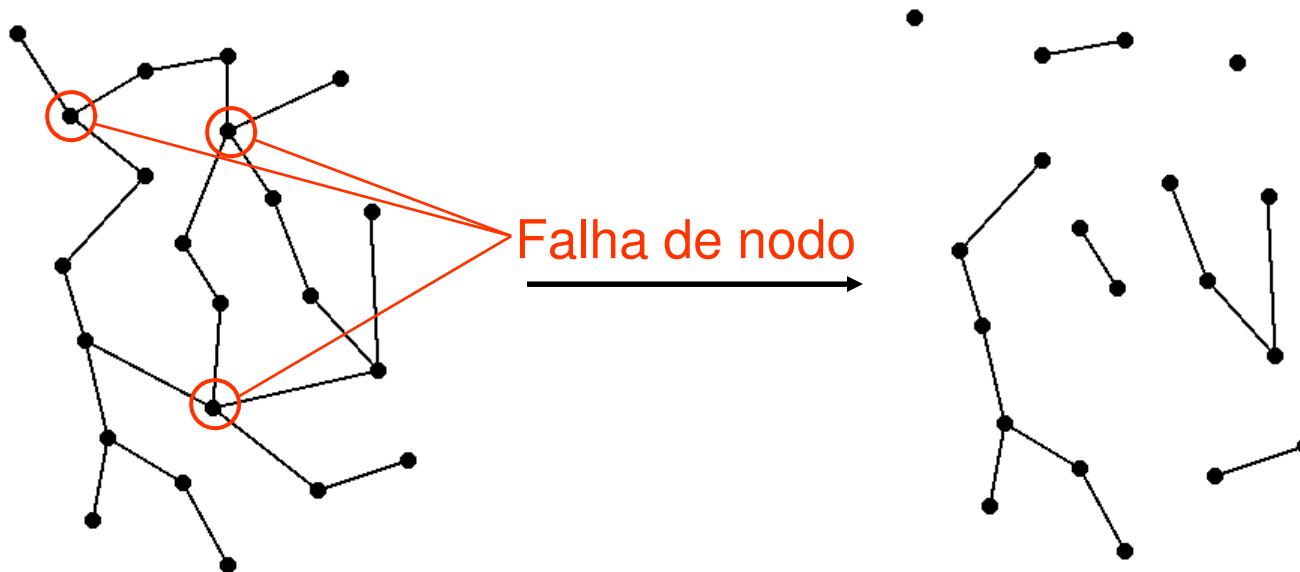
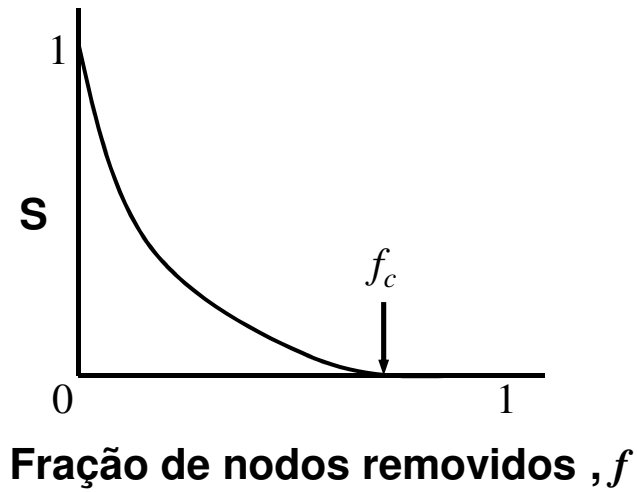
Pál Erdős
(1913-1996)

Distribuição de graus:
Poisson



Idéia de Robustez

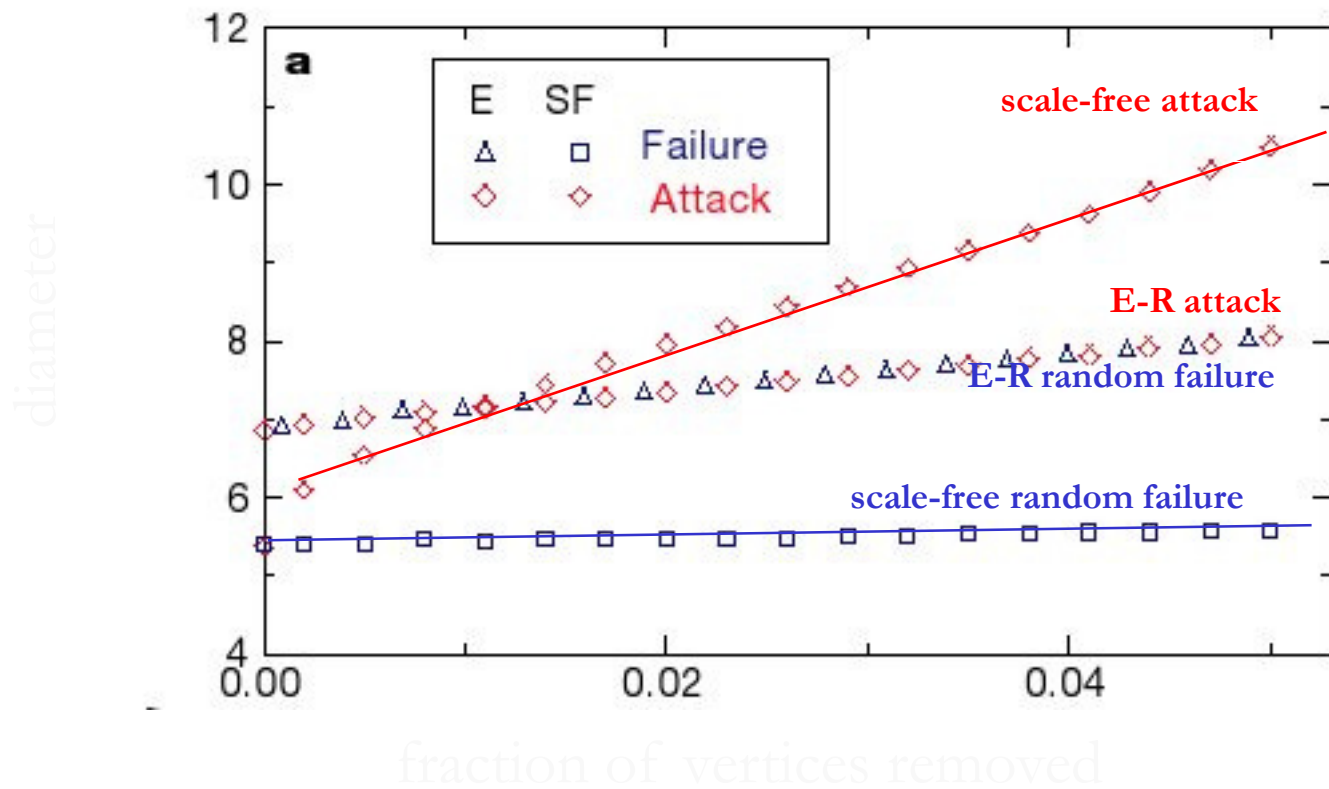
Sistemas complexos mantem suas funções básica mesmo em face de erros e falhas



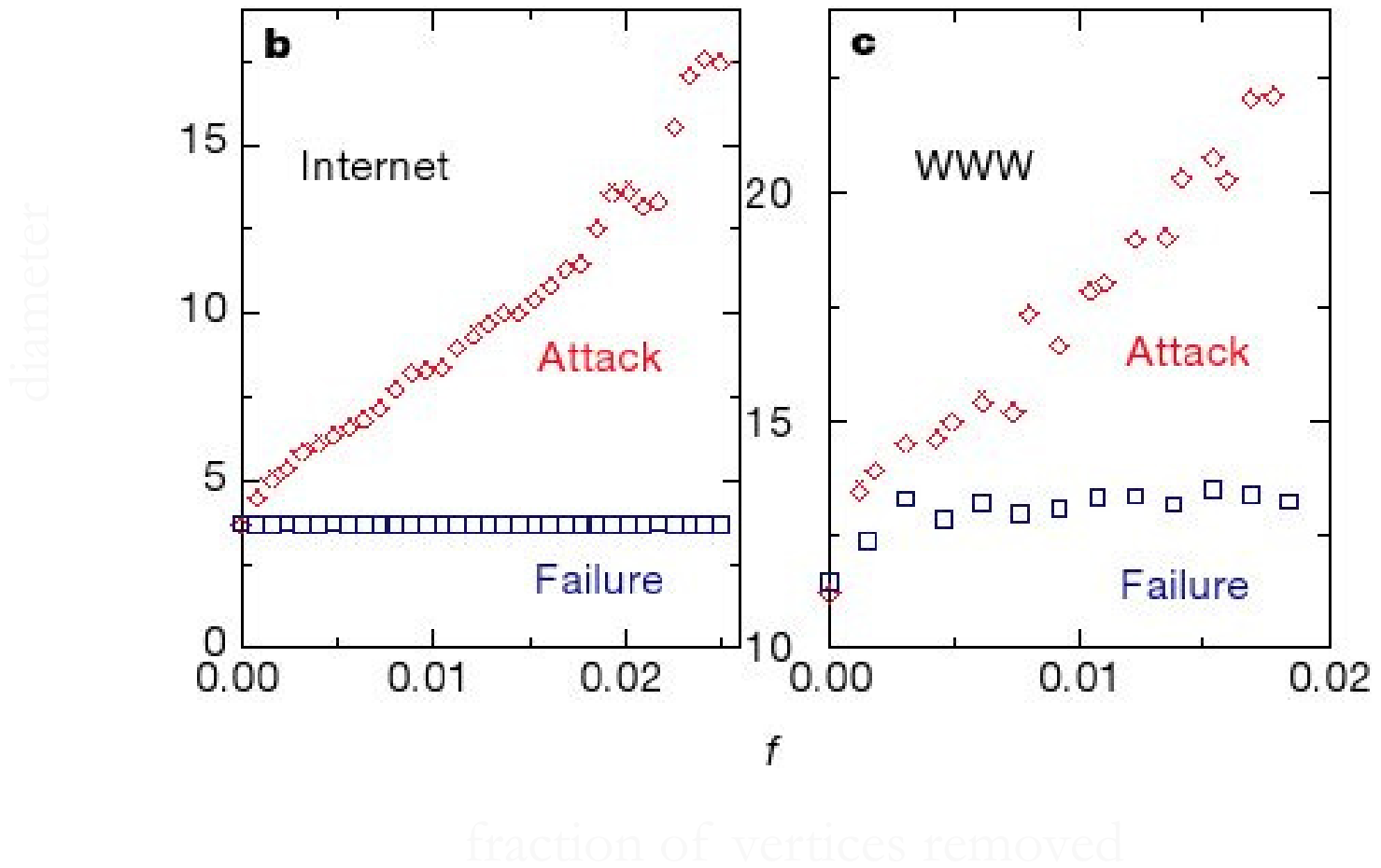
Experimento Numérico: mudança no diâmetro

- Comparar redes power laws (Scale free SF) e randomica

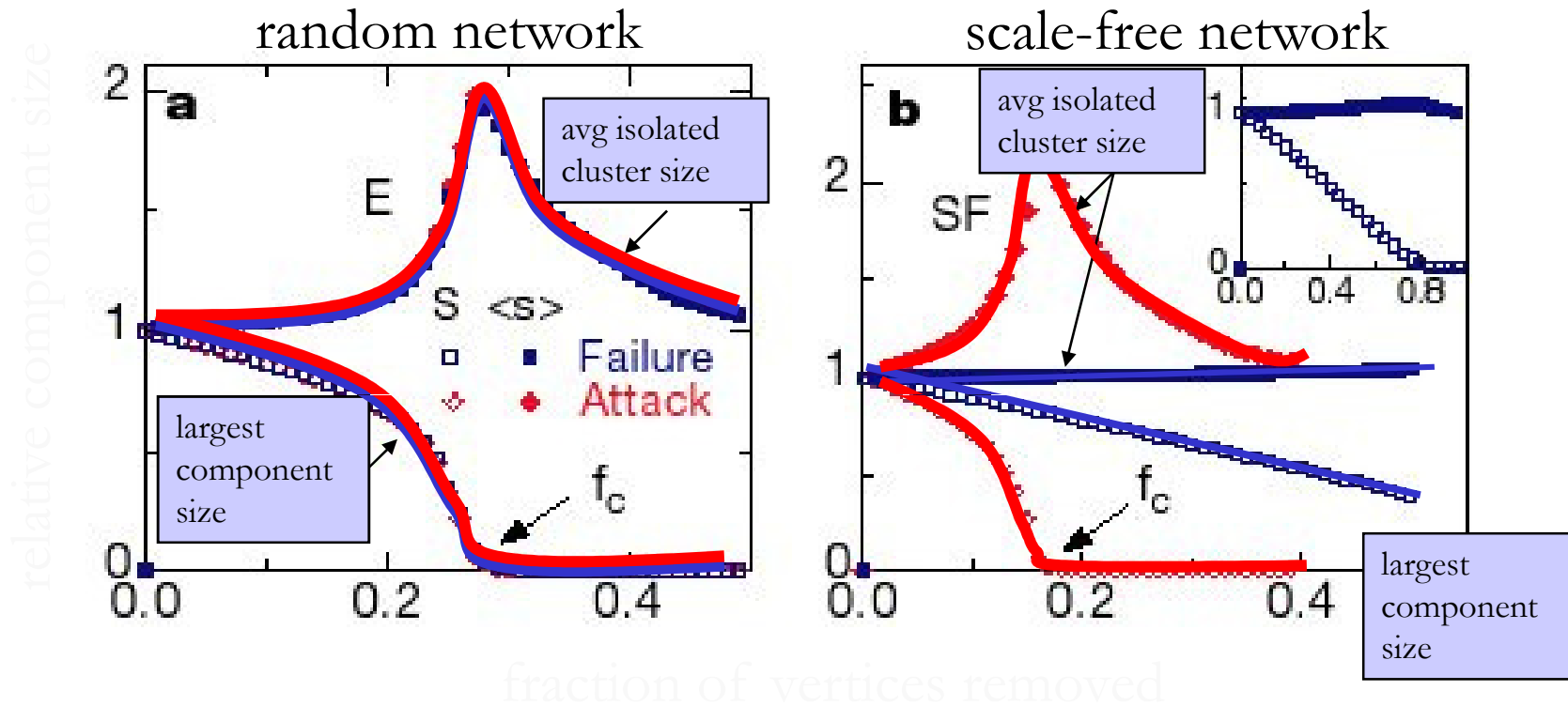
Redes scale-free robustas a falha aleatória, vulnerável a ataque



Experimento Numérico: mudança no diâmetro



Experimento Numérico: Tamanho (S) do Componente Conectado



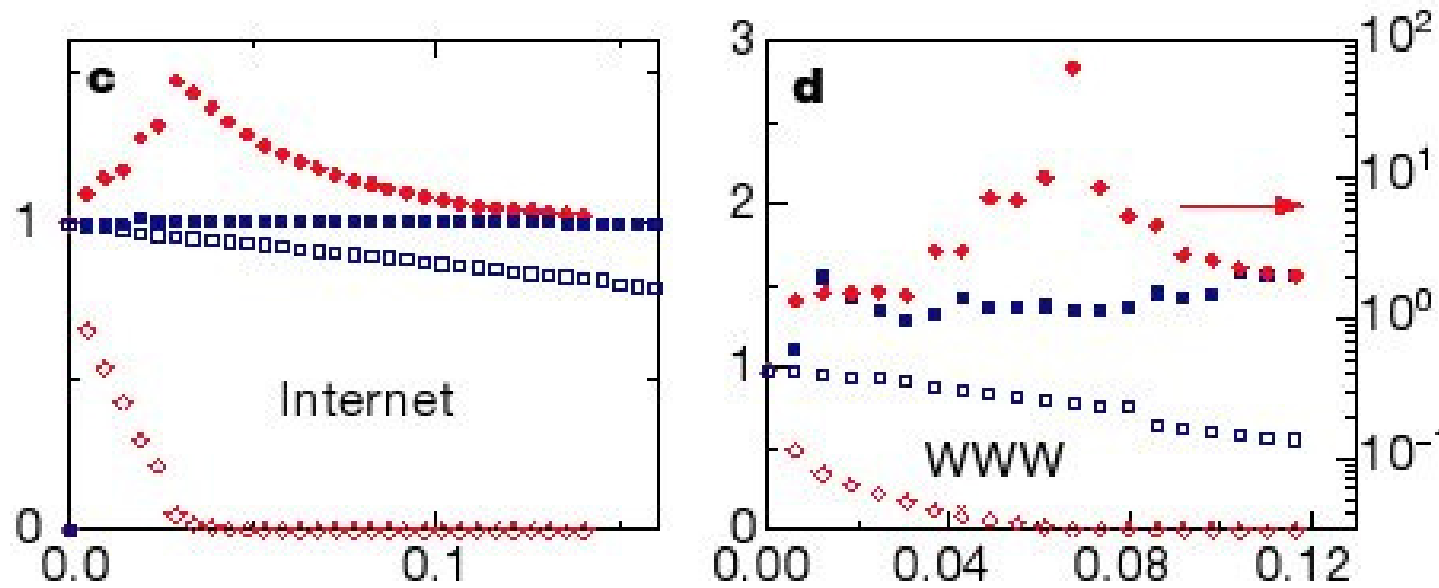
Rede randomica, falha

Rede randomica, ataque

Rede SF , falha

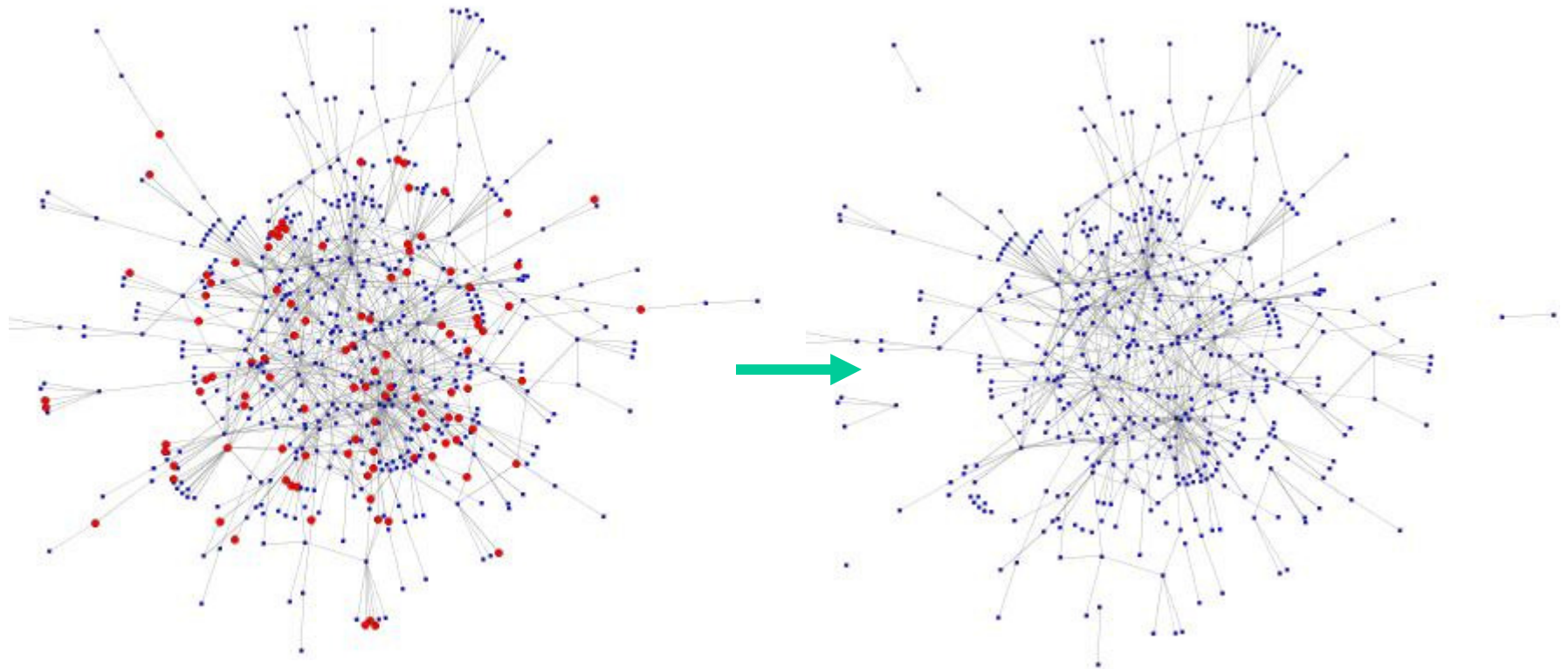
Rede SF , ataque

Experimento Numérico: Tamanho (S) do Componente Conectado



Resiliência de Redes SF reais a falhas

- Example: gnutella network, 20% of nodes removed

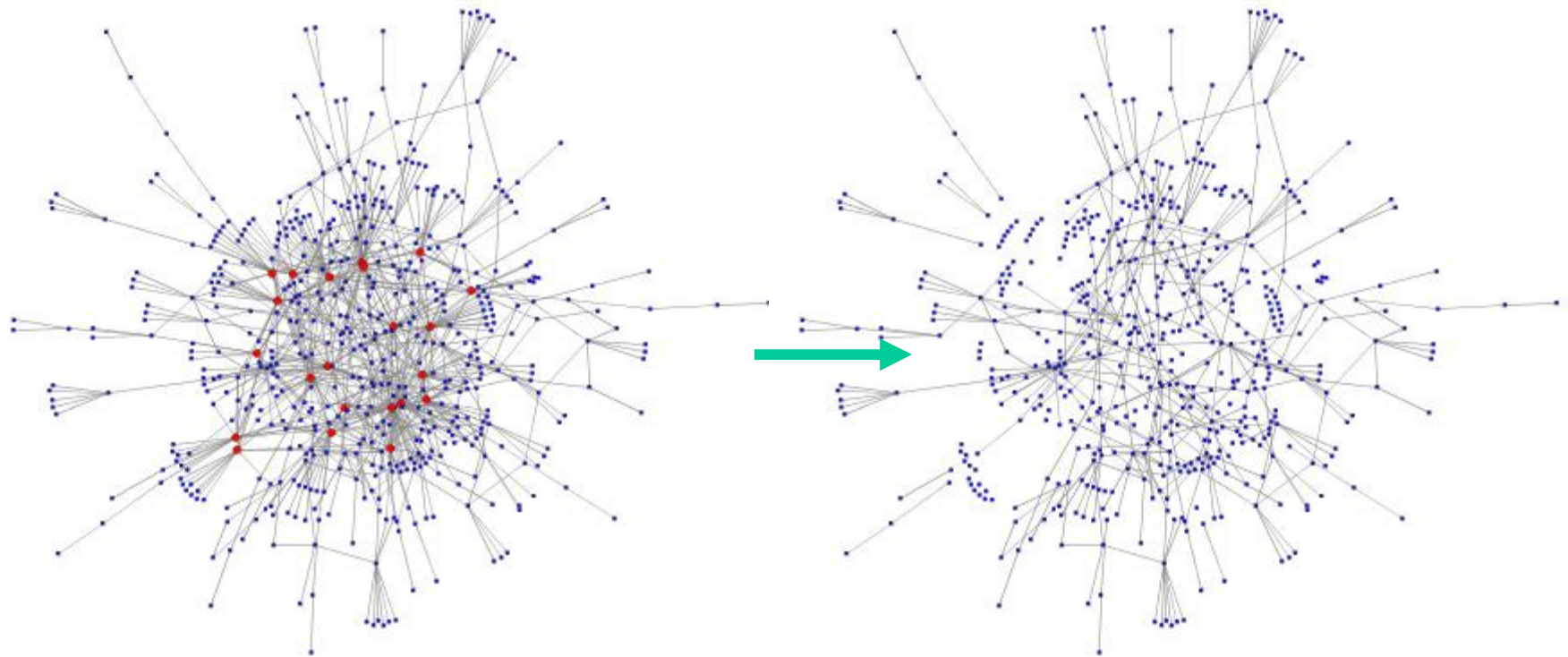


574 nodes in giant component

427 nodes in giant component

Resiliência de Redes SF reais a ataques

- Exemplo: mesma rede gnutella , 22 nodos mais conectados são removidos (2.8% dos nodos)

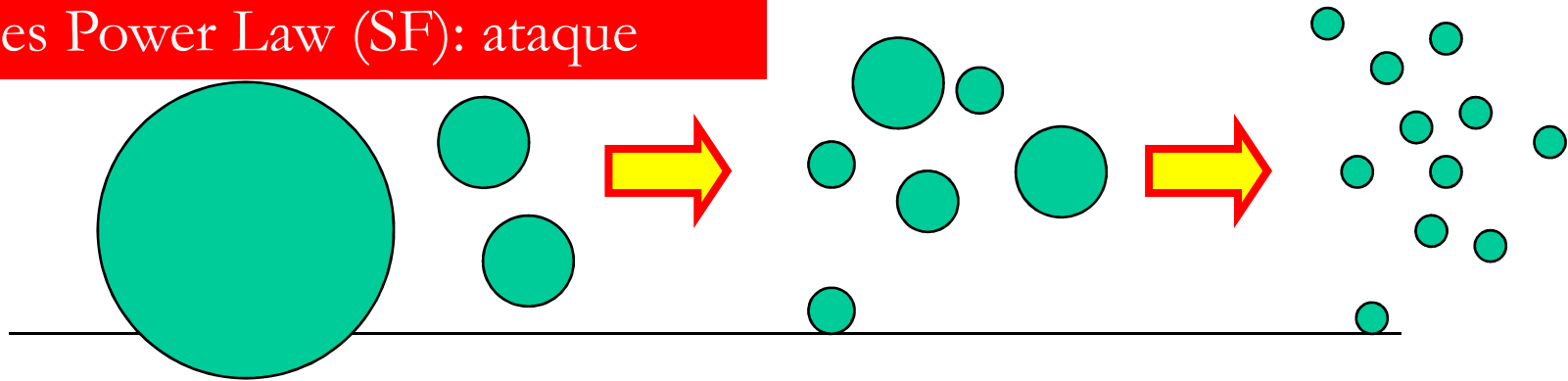


574 nodos CG

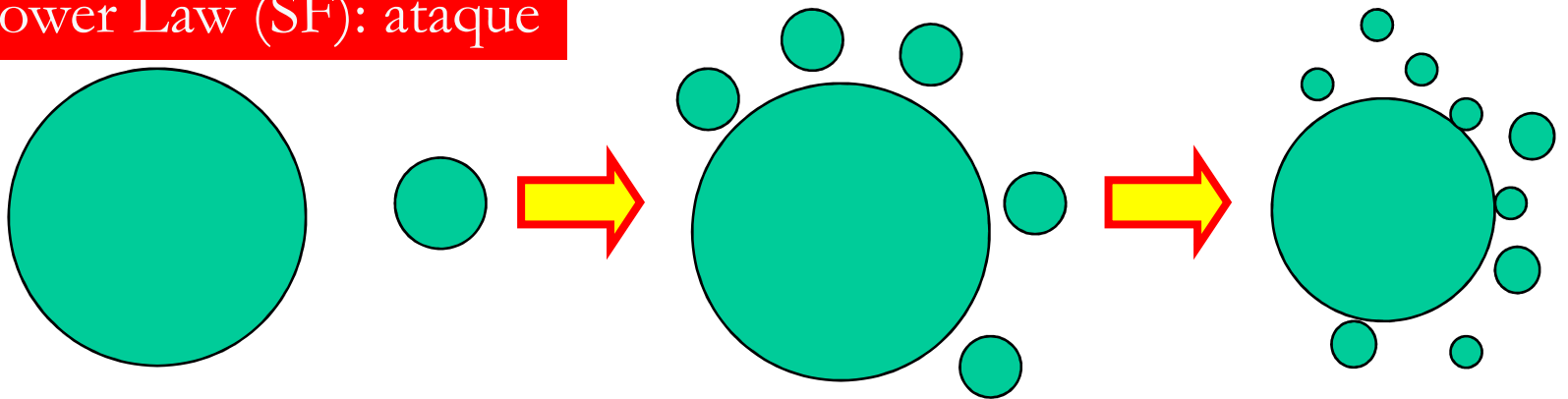
301 nodos CG

Sumário dos Resultados

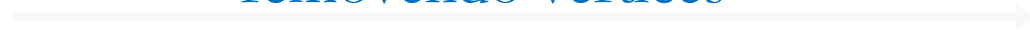
Redes randmônicas: falha, ataque
Redes Power Law (SF): ataque



Redes Power Law (SF): ataque

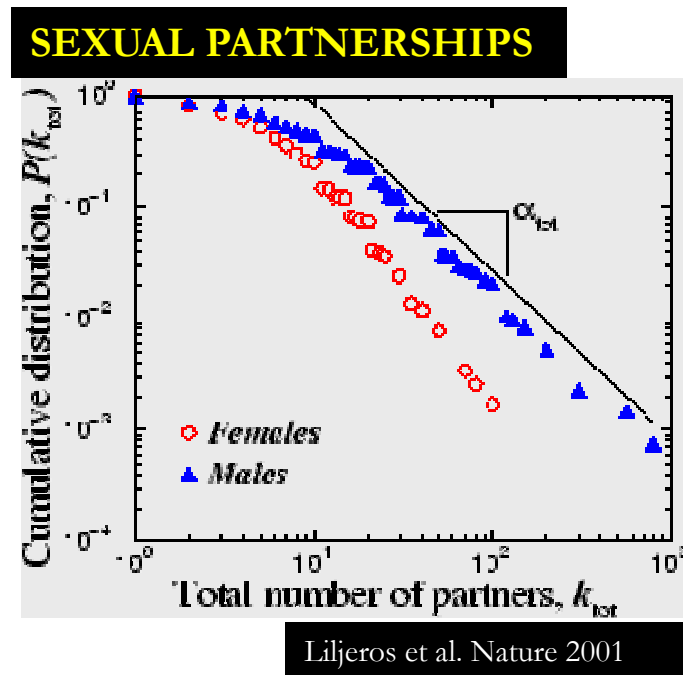


removendo vertices



E aí???

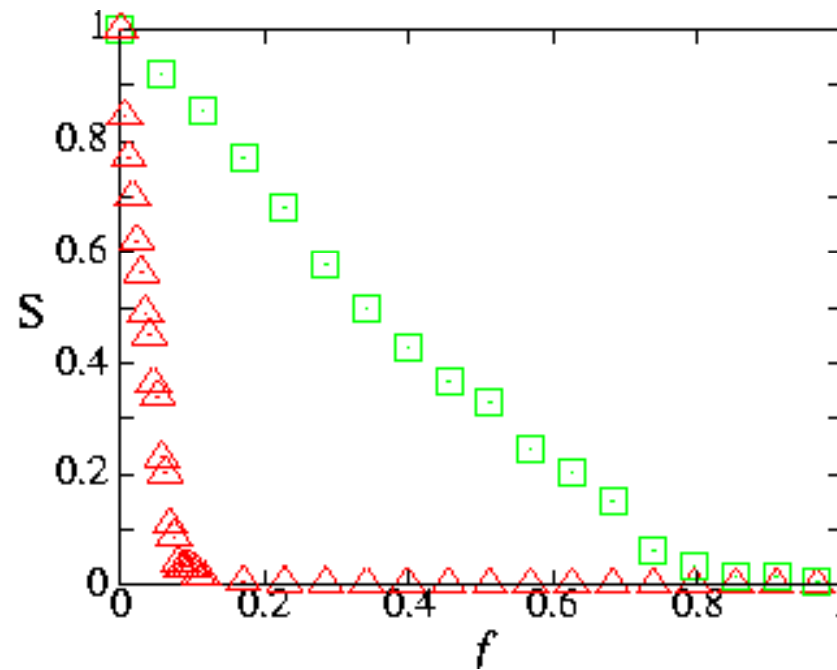
- Insight: por que da resistência e vulnerabilidade da Internet
- Novo insight sobre melhores estratégias
 - ex: Como melhor combater AIDS



Calcanhar de Aquiles das Redes Complexas

— falha
— ataque

Internet



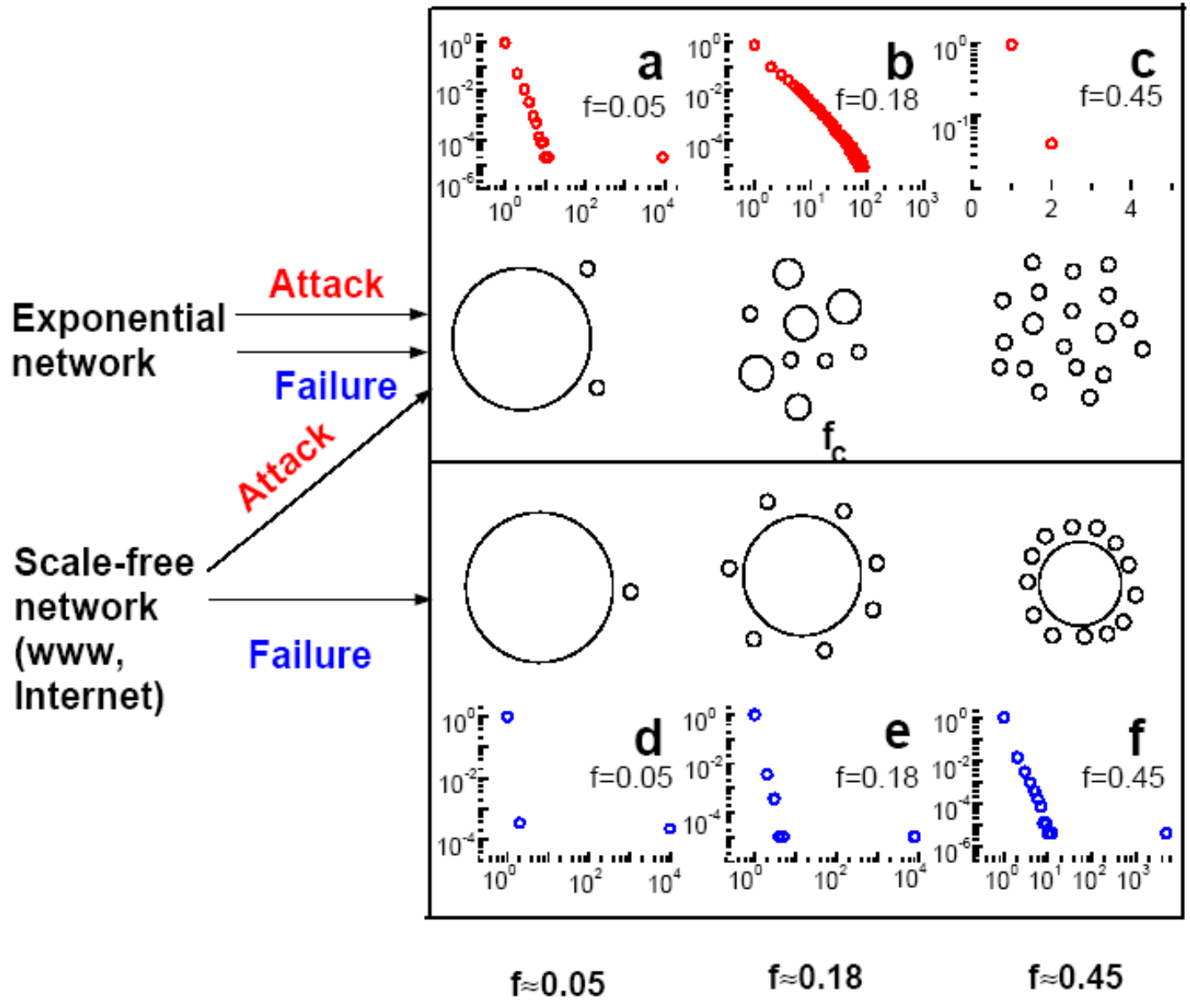
R. Albert, H. Jeong, A.L. Barabasi, Nature **406** 378 (2000)

Novos pontos de pesquisa: The Wireless Epidemic

- Virus de Computador → paralelo com biologia
- Sistemas computacionalmente imunes
- Redes de contato → redes de epidemias → links com potencial para infectar nodos → aeroportos
- Tradicionalmente, virus de computador propaga em redes diferentes das biológicas
- *Short-range wireless communication networks* → novos modelos

Short-range wireless communication networks

- Epidemias na Internet: virus (“piggyback on data”) e worms: padrões de comunicação de emails ou estruturas de comunicação
- Modelos baseados nas viagens humanaa
- Virus de computador cujo progresso segue de perto o mobilidade humana...
 - “A computer virus becomes something that you catch not necessarily from a compromised computer halfway around the world, but possibly from the person sitting next to you on a bus, or at nearby table in a restaurant.”



Classificação de Ataques

- **Ataques a Infraestrutura:**
 - Ataques com objetivo de desabilitar uma rede p2p, parcial ou totalmente
ex. Eliminando nodos, ataques protocolos de roteamento
- **Ataques Semânticos:**
 - Ataques que visam um sistema p2p, mas não para desabilitar mas para tirar usuários..
Ex. Conteúdo danificado ou poluído, consumo assimétrico de recursos...
- Ambos são efetivos, pois p2p é uma rede social de pessoas (**)

Redes Randômicas

- Criadas por Paul Erdos and Alfred Renyi em 1959 e 1960.
- Hipóteses básicas:
 - Número fixo de nodos
 - Conectados por arestas aleatórias.
 - Nodos são “democraticos” i.e. Maior parte dos nodos tem aproximadamente um número igual de arestas incidentes.

Introdução do conceito de *Scale-free networks*

- Introduzido por Barabasi e colaboradores em 1999.
- Em evolução e auto-organizadas.
- Duas regras fundamentais:
 - (a) crescimento no tempo pela adição de nodos e arestas.
 - (b) regra de ligação aos nodos, várias formas.

Notação Matemática

- Grau do vértice/nodo – no. de arestas incidentes
- Distribuição de graus - característica probabilística da rede
- **$P(k, s, N)$** - probabilidade que o vértice s na rede de tamanho N tenha k conexões (vizinhos mais próximos).

- Distribuição do grau total

$$P(k, N) = \frac{1}{N} \sum_{s=1}^N p(k, s, N)$$

Distribuição de graus

- Definição:
- A probabilidade que um vértice tem k arestas.
- A distribuição de Poisson para as *random networks* de Erdos-Renyi.

$$P(k) = \frac{e^{-\lambda} \lambda^k}{k!}$$

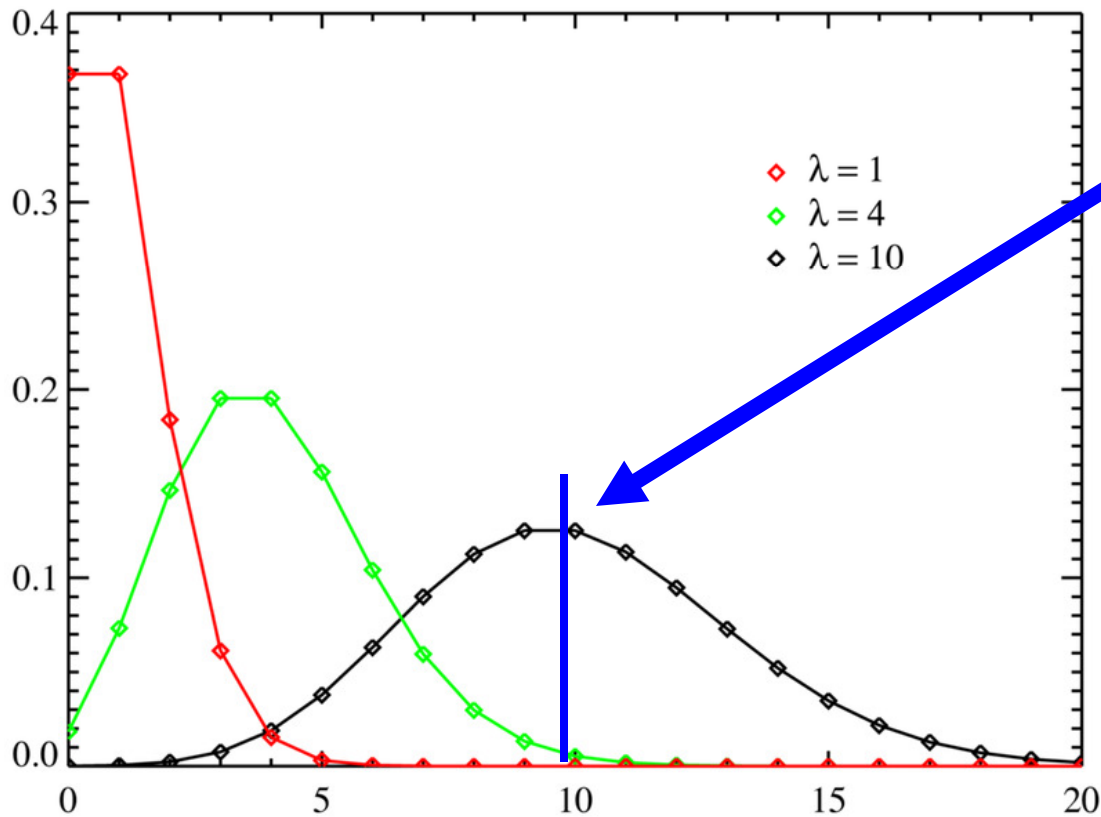
onde

$$\lambda = \sum_{k=0}^{\infty} kP(k)$$

Distribuição de Poisson

- Distribuição de graus

Escala característica.
Nodo médio típico



$$\lambda = \bar{k}$$

Distribuição Power law

para as redes em evolução e auto-organizadas propostas por Barabasi e colaboradores

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

$$2 < \gamma < 3$$

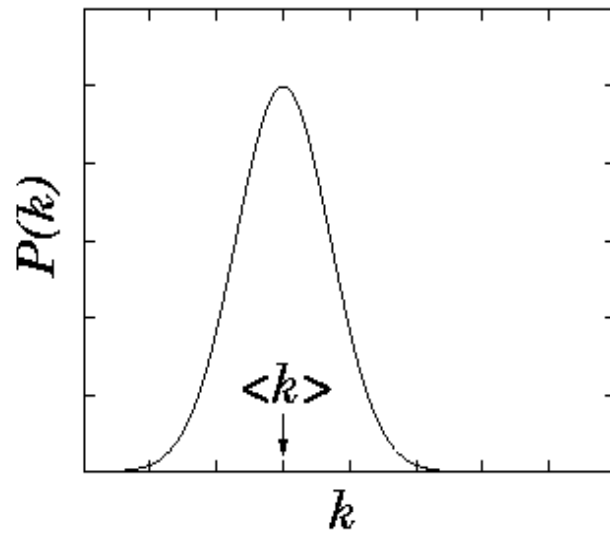
Intervalo típico

Essas redes não tem um número médio típico de arestas e são chamadas “scale-free”.

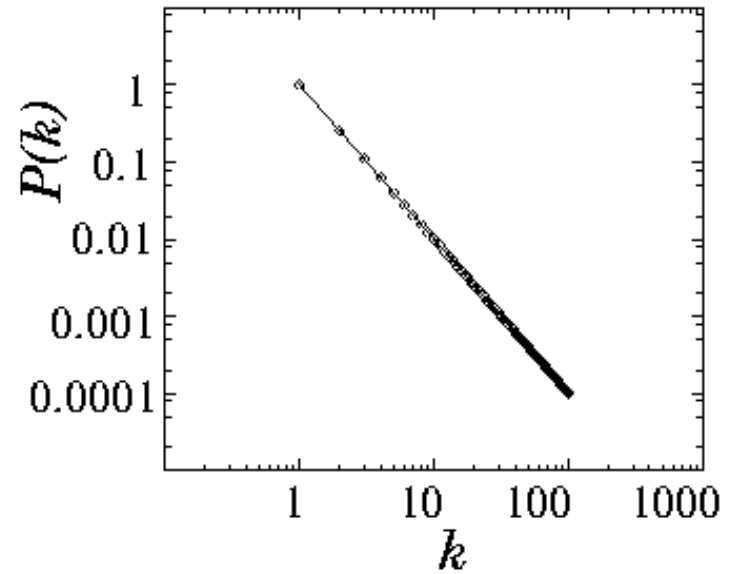
Random vs. Scale Free

- Exemplos:
- Rede de estradas nos EUA
 - Próxima de uma random network, com uma distribuição em forma de “bell”
- Ao contrário, aeroportos nos EUA
 - Formam uma rede scale free network com vários hubs ligando um grande número de aeroportos.

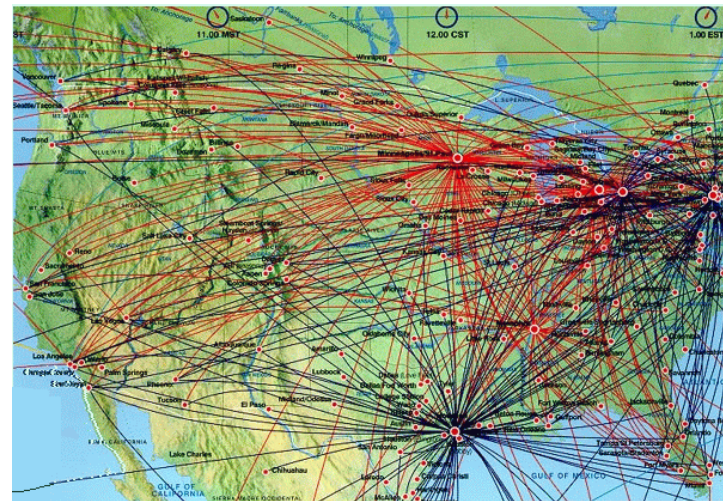
Poisson distribution



Power-law distribution



Random Network



Scale-free Network

Scale free: outros exemplos reais

- Redes de Comunicação: Internet e WWW
- Biológicas : interações entre proteínas no corpo humano.
- Food webs,
- Redes Sociais, citações científicas,

WWW

- Distribuição Power-law levemente modificada

$$P(k) \propto (k + c)^{-\gamma}$$

Home pages na Web

γ

C

Empresas

2.05

193

Universidades

2.62

1370

Cientistas da computação

2.66

12

A Web como um todo

2.1

0

Redes do Tipo Scale-free

- Redes Scale-free são uma categoria importante das redes reais.
- Elas tem nodos muitos conectados (**hubs**) que representam um papel chave nas propriedades das redes.
- Redes Scale-free são um resultado direto da “self-organization”.
- Tipo especial de crescimento chamado “**the preferential linking**” ou “**preferential attachment**”.
- Enquanto a rede cresce seu novo nodo torna-se preferencialmente conectado a vertices com maiores números de conexões: “rich gets richer”.
- Como resultado dessa auto-organização HUBS são criados. (***)