Network Robustness

Random Failures and Targeted Attacks

Giacomo Fiumara

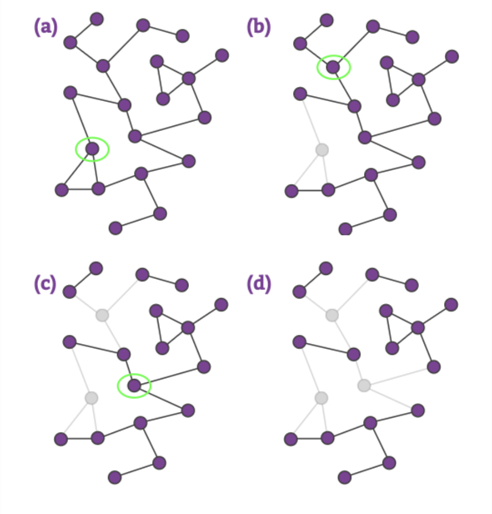
Outline

Introduction

Why Network Robustness?

- Networks underpin biological, technological, social and engineered systems.
- Robustness: ability to maintain function despite node or link failures.
- Structure determines survival: hubs, redundancy, clustering.
- Central to biology, infrastructure, engineering, and social systems.

Why Network Robustness?

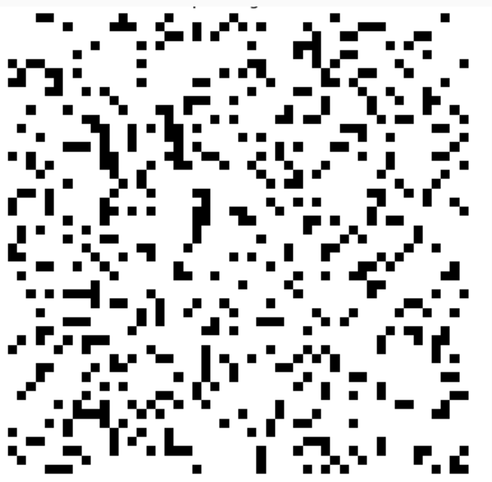


Percolation Theory

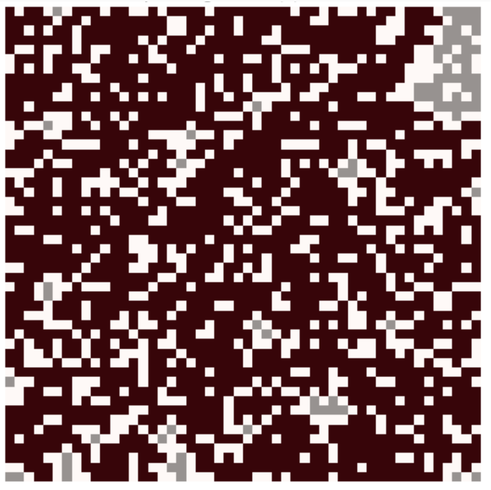
Percolation Basics

- Focus: Emergence and disappearance of large-scale connectivity under random removal.
- Percolation threshold p_c — critical point for global connectivity.
- Order parameter: Fraction P in largest cluster.
- Critical exponents describe phase transition's universality.

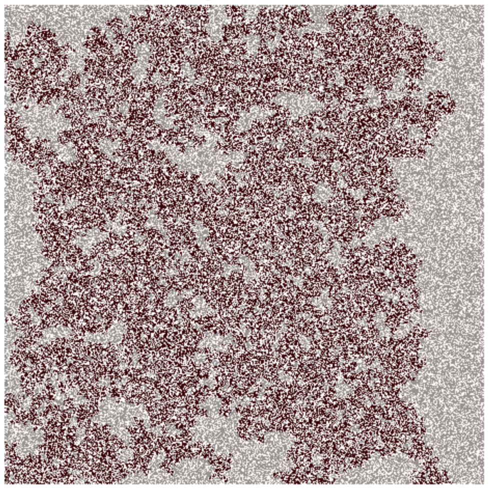
Percolation Transition and Universality



Percolation Transition and Universality



Percolation Transition and Universality



Percolation Transition and Universality

- At $p < p_c$, many small clusters; $p \geq p_c$, giant component emerges.
- All lattices and random network types show phase transition at critical occupation probability.
- Exponents (β, γ, ν) universal within dimensional class.

Percolation Transition and Universality

Three quantities are necessary to describe this phase transition:

- The average size of all finite clusters:

$$\langle s \rangle \propto |p - p_c|^{-\gamma_p}$$

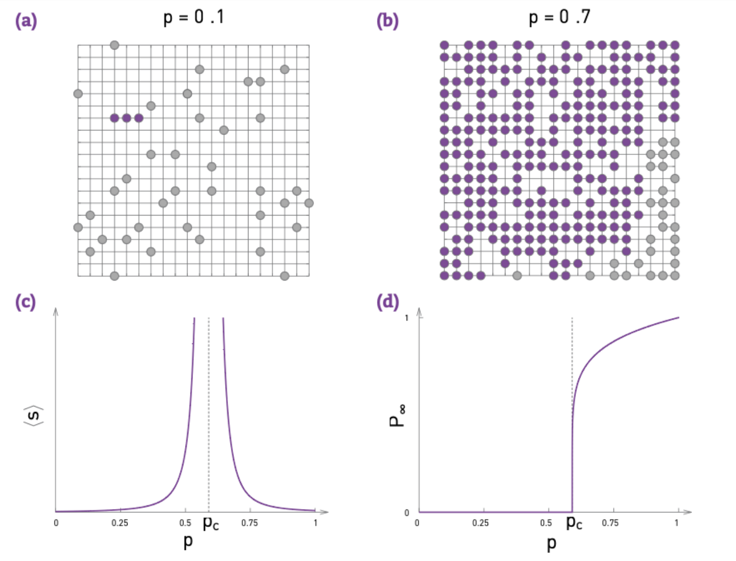
- The order parameter P_∞, namely the probability that a randomly chosen site belongs to the largest cluster:

$$P_\infty \propto (p - p_c)^{\beta_p}$$

- The correlation length ξ, namely the mean distance between two sites that belong to the same cluster:

$$\xi \propto |p - p_c|^{\nu}$$

Percolation Transition and Universality



Inverse Percolation

What is Inverse Percolation?

- Starts from a fully occupied system (all sites/nodes present).
- Nodes/sites are randomly removed, reducing connectivity.
- The network undergoes a fragmentation phase transition at a critical fraction removed f_c.
- Important model for network robustness: models failure and attack scenarios.

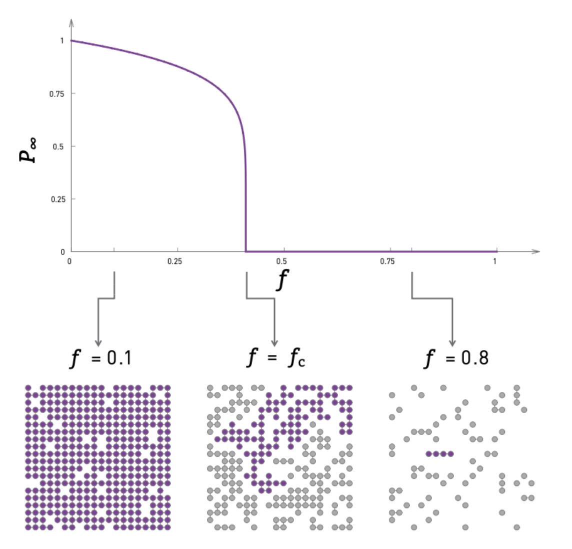
The Role of $f = 1 - p$

- Classical percolation is framed in terms of occupation probability p.
- Inverse percolation focuses on fraction f of sites removed: $f = 1 - p$.
- f represents the degree of damage or failure in the system.
- At critical point $f_c = 1 - p_c$, the giant component collapses and the network loses global connectivity.
- This inversion links classical percolation theory with network robustness perspectives.

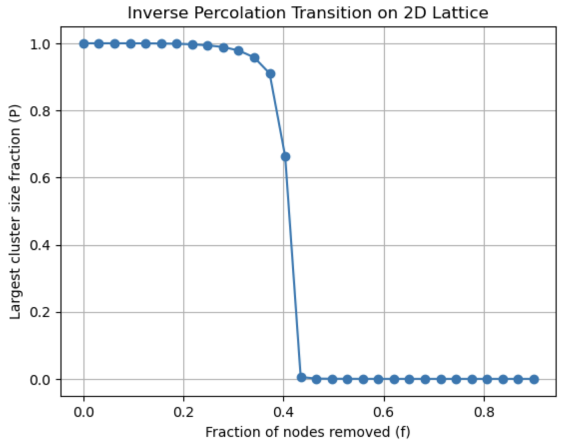
Inverse Percolation Transition

- Initially, there is a giant connected cluster occupying the entire lattice.
- As nodes are removed (as f increases), cluster sizes shrink and eventually fragment.
- The order parameter P (normalized largest cluster size) decreases and vanishes at f_c.
- This phase transition is characterized by universal critical exponents.

Inverse Percolation Transition



Inverse Percolation Transition



Applications and Relevance

- Models conceptually and practically important network robustness scenarios.
- Provides predictive power for system failures in infrastructure, biology, and social systems.
- Links statistical physics of percolation and real-world failure dynamics.
- Serves as a foundation for error and attack tolerance analyses.

Percolation on Networks

Percolation on Networks

- Percolation studies how connectivity is lost under node/link removal.
- Key: When does the giant component vanish?
- Transition depends on topology and degree distribution.
- Molloy-Reed criterion:

$$\frac{\langle k^2 \rangle}{\langle k \rangle} > 2$$

Critical Threshold for Fragmentation

- f = fraction nodes removed; network shatters at critical f_c:

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

- Random networks: finite f_c.
- Scale-free networks ($2 < \gamma < 3$): $f_c \to 1$ as network size grows — extraordinary robustness.

Finite-Size Effects and Node/Link Removal

- Real networks are finite; f_c rises but maxes below 1.
- Node removal usually fragments more than equivalent link removal.
- Impact depends on degree distribution and network size.

Random Failures

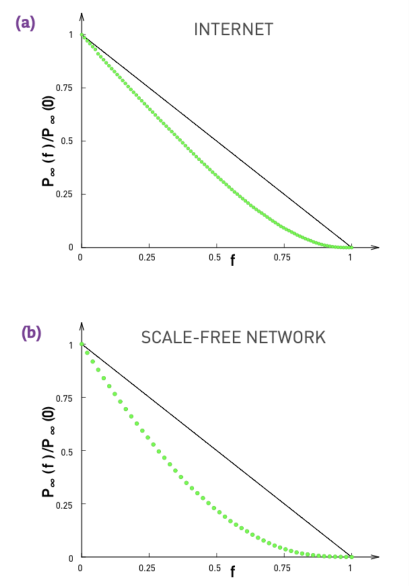
Impact of Random Failures

- In random networks, removal of a finite f_c of nodes destroys giant component—abrupt transition.
- In scale-free networks, giant component persists nearly until all nodes lost.
- Analytical result: robustness scales with second moment $\langle k^2 \rangle$.

Mechanism of Robustness

- Random failures hit mostly low-degree nodes (more numerous).
- Hubs remain intact, holding the network together.
- Probability of randomly removing a hub is low.
- Enhanced error tolerance is a generic property of broad degree distributions.

Mechanism of Robustness



Empirical Data: Random Failure Robustness

- Internet: $f_c \approx 97\%$ must be removed to fragment network.
- Large biological networks (protein interactions, metabolic): f_c high.
- Social networks: robust to random removal.
- Table: f_c values for ten reference networks (Internet, WWW, Power Grid, etc.).

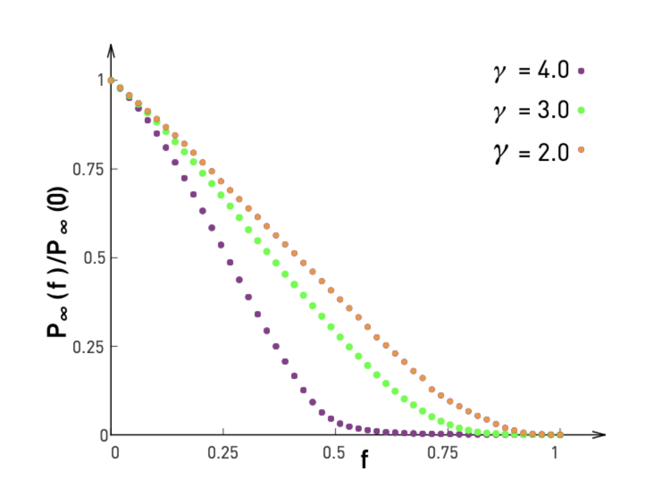
Empirical Data: Random Failure Robustness

NETWORK	RANDOM FAILURES (REAL NETWORK)	RANDOM FAILURES (RANDOMIZED NETWORK)	ATTACK (REAL NETWORK)
Internet	0.92	0.84	0.16
WWW	0.88	0.85	0.12
Power Grid	0.61	0.63	0.20
Mobile-Phone Call	0.78	0.68	0.20
Email	0.92	0.69	0.04
Science Collaboration	0.92	0.88	0.27
Actor Network	0.98	0.99	0.55
Citation Network	0.96	0.95	0.76
E. Coli Metabolism	0.96	0.90	0.49
Yeast Protein Interactions	0.88	0.66	0.06

Visualization: Giant Component Shrinkage

- Plot: $P(f)$—fraction in giant component vs. fraction removed.
- Show curves for random network and scale-free network.
- Scale-free curve decays gradually, random network curve drops sharply at f_c.

Visualization: Giant Component Shrinkage



Targeted Attacks

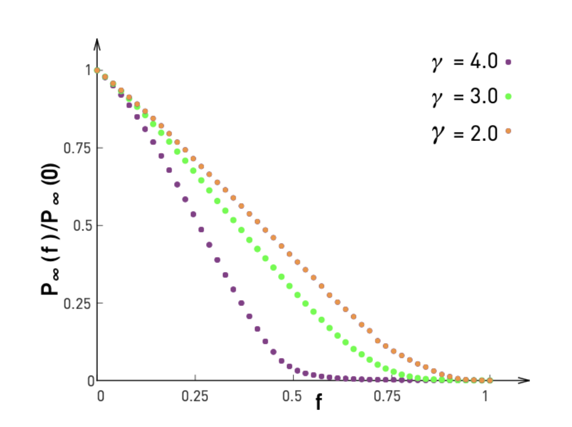
Attack Tolerance: Hub Removal

- Attacks deliberately remove nodes with highest degree.
- Network fragments rapidly, even with small fraction of nodes removed.
- Critical attack threshold f_c is much smaller than for random failures.

Why Are Hubs Critical?

- Hubs connect large parts of the network—removal deprives many nodes of connections.
- Result: cascading fragmentation, network quickly falls apart.
- Analytical threshold depends on degree exponent and hub structure.
- Figure: drop in giant component for attack (purple) vs. random (green).

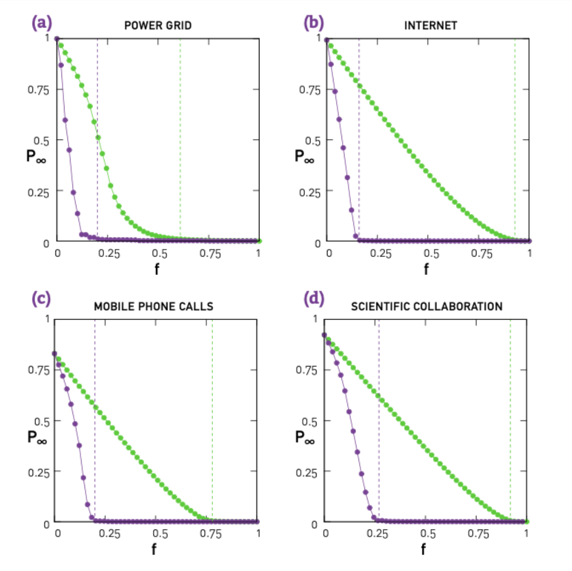
Why Are Hubs Critical?



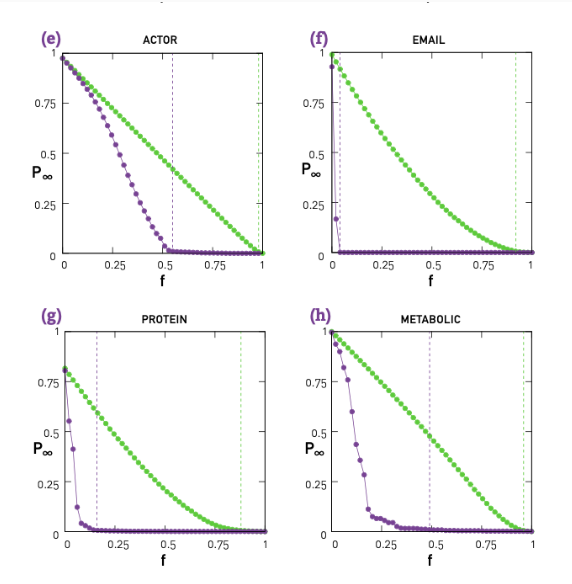
Empirical Attack Vulnerability

- Table: attack threshold f_c for real-world networks—much lower than error threshold.
- Example: Internet, mobile networks, biological networks.
- "Achilles Heel" effect: robust against random errors, fragile against targeted attacks.
- Separation between error and attack curves is key network diagnostic.

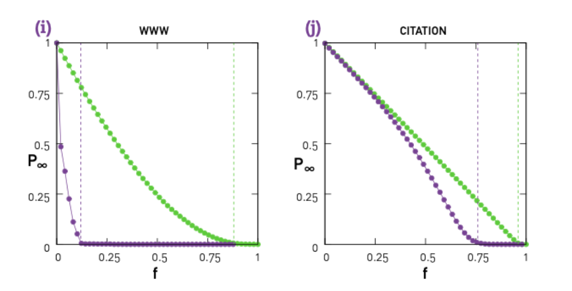
Empirical Attack Vulnerability



Empirical Attack Vulnerability



Empirical Attack Vulnerability



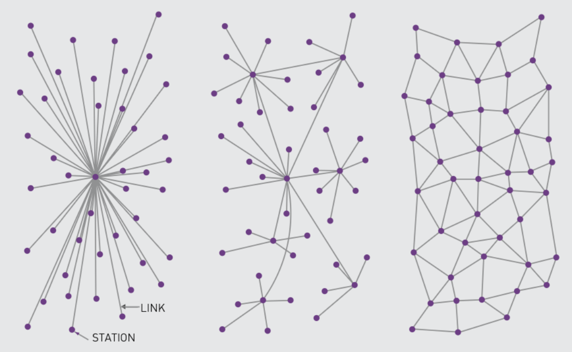
Practical Implications

- Internet and infrastructure systems are safe from random failures but vulnerable to targeted attack.
- Implies need for defense/better design for vital hubs (cybersecurity, redundancy).
- Positive for targeted medical interventions—dismantling pathogens by hitting hub proteins.

Designing Against Attacks

- Paul Baran's vision: distributed mesh-like networks more survivable than hub-and-spoke.
- Redundancy, decentralization can offset vulnerability of hubs.
- Cost/tradeoff: more links = higher resilience, but greater complexity and resource use.
- Case study: European Power Grid—topology and reliability.

Designing Against Attacks

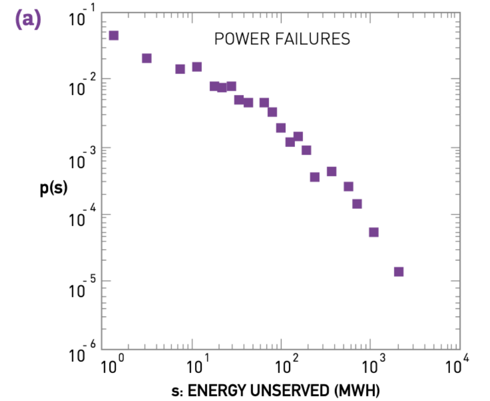


Cascading Failures

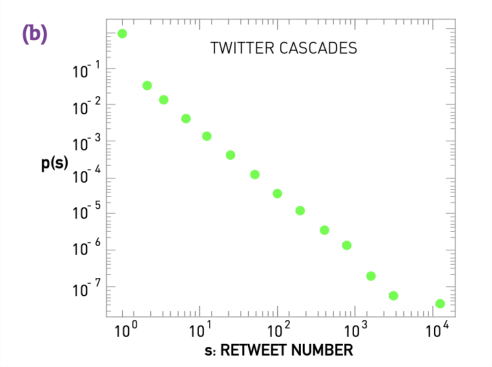
Cascading Failures and Avalanche

- Local failure can propagate via links, inducing global breakdown (blackouts, supply chains, viral memes).
- Avalanche size often follows power-law distribution ("many small, few catastrophic").
- Example: Power grid blackout, Twitter retweet cascade, earthquake sequence.

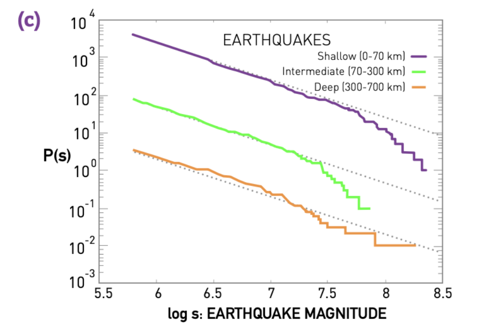
Cascading Failures and Avalanche



Cascading Failures and Avalanche



Cascading Failures and Avalanche



Summary

Key Takeaways

- Structure is destiny—network topology determines resilience and vulnerability.
- Scale-free networks are robust to random failures, fragile against hub attacks.
- Cascading failures are universal; their statistical signatures help risk assessment.
- Real-world function and design informed by robustness principles.