A new Information Theory Perspective on Network Robustness

Panos M. Pardalos

Center For Applied Optimization,
Industrial and Systems Engineering, University of Florida,
Florida, USA.
www.ise.ufl.edu/pardalos
and
National Research University Higher School of Economics,
Laboratory of Algorithms and Technologies for Network
Analysis, Nizhny Novgorod, Russia
http://nnov.hse.ru/en/latna/

Network Robustness Definition

- There are several works dealing with the concept of robustness, however, there is still no consensus on a definitive definition.
- Robustness is usually described as the ability of the network to continue performing, or, as the capacity in maintaining its functionality after failures or attacks.
- A robust network is failure resilient.

Network Robustness Definition

- There are several works dealing with the concept of robustness, however, there is still no consensus on a definitive definition.
- Robustness is usually described as the ability of the network to continue performing, or, as the capacity in maintaining its functionality after failures or attacks.
- A robust network is failure resilient.

Network Robustness Definition

- There are several works dealing with the concept of robustness, however, there is still no consensus on a definitive definition.
- Robustness is usually described as the ability of the network to continue performing, or, as the capacity in maintaining its functionality after failures or attacks.
- A robust network is failure resilient.

Applications

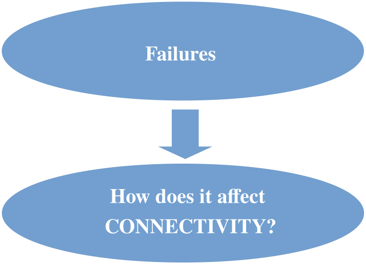
- Evacuation planning
- Fragmentation of terrorist organizations
- Epidemic contagion analysis and immunization planning
- Social network analysis (Prestige and dominance)
- Transportation (Cross-dock and hub-and-spoke networks)
- Marketing and customer services design
- Biomaterials and drugs design

Problems

- Critical element detection
- How to measure network robustness?
- Network similarity

Problems

- Critical element detection
- How to measure network robustness?
- Network similarity



Failure

Let G be a network defined by a set $V(G)$ of N nodes, a set $\mathcal{E}(G)$ of M links and a set $W(E(G))$ containing the edges strengths. A network failure event f is defined as the removal of a subset of edges $f \subset \mathcal{E}(G)$.

- A link failure is the removal of a single link
- A node failure consists in the removal of all it incident links

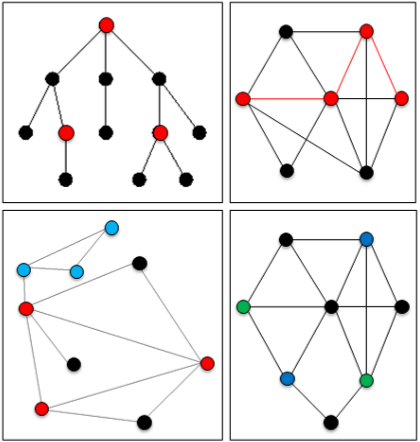
Failure

Let G **be a network defined by a set** $V(G)$ **of** N **nodes, a set** $\mathcal{E}(G)$ **of** M **links and a set** $W(E(G))$ **containing the edges strengths. A network failure event** f **is defined as the removal of a subset of edges** $f \subset \mathcal{E}(G)$**.**

- A link failure is the removal of a single link
- A node failure consists in the removal of all it incident links

Critical Elements Detection

Given a graph $G(V, E)$ and an integer k, find a set of at most k **elements**, whose deletion minimizes the **connectivity** of the residual network.



Elements?

- Nodes (arcs)
- Paths
- Cliques
- Node subsets

Connectivity?

- Max flow
- Number of pairwise connections
- Number of components

The problem is proven to be NP-hard in the general case for different elements:

- Nodes (Arcs)
- Paths
- Cliques

A. Arulsevan and C. W. Commander and L. Elefteriadou and P. M. Pardalos, ***Detecting Critical Nodes in Sparse Graphs***, Computers and Operations Research, 2009, pp. 2193-2200

T. N. Dinh and Y. Xuan and M. T. Thai and P. M. Pardalos, ***On New Approaches of Assessing Network Vulnerability: Hardness and Approximation***, IEEE ACM Transactions on Networking, 2012, pp. 609-619

J. Walteros and P. M. Pardalos, ***A Decomposition Approach for Solving Critical Clique Detection Problems***, Experimental Algorithms, Springer, 2012, pp. 393-404

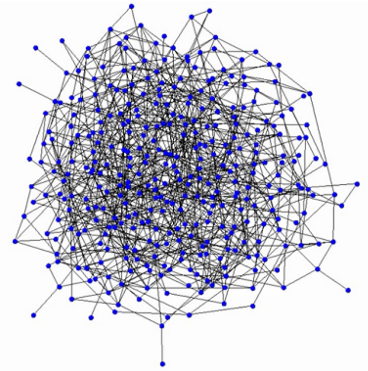
Why should we study this problem?

Disconnecting a network by element removal is not trivial!

- 350 nodes, 900 arcs
- **Network 1:** U(0,1)
- **Network 2:** greedy construction
- **Network 3:** Power law a=0.44 b=50

Click on the network for video

*



Connectivity Measures

Network Flow Measures

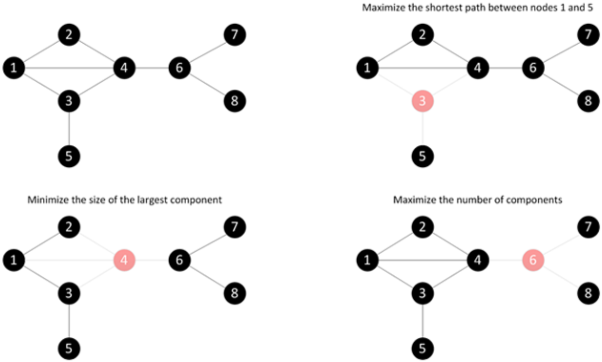
- Single/Multiple commodity shortest path
- Single/Multiple commodity maximum flow
- Single/Multiple commodity minimum cost

Topological Measures

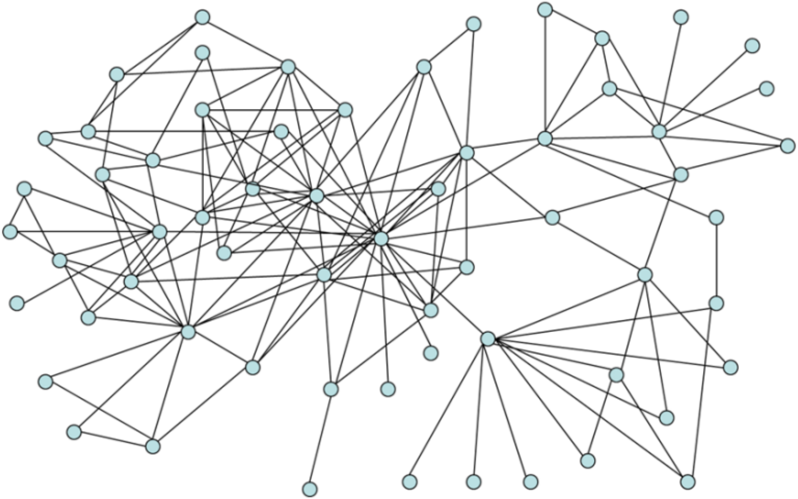
- Pairwise (weighted) connectivity
- Largest component size
- Total number of components

Connectivity Measures: Different results

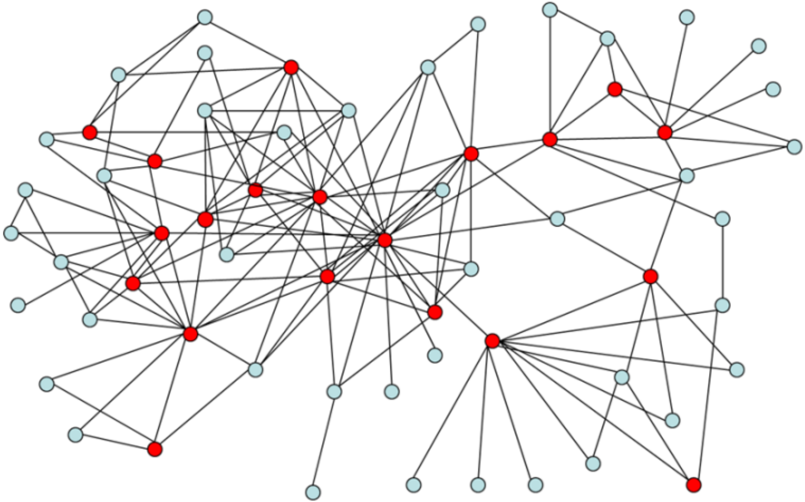
- The selection of the connectivity measure is crucial
- In a node failure, despite the fact that all these measures account for a disconnection level, using one over the other may lead to different critical elements



Critical Nodes Detection Problem

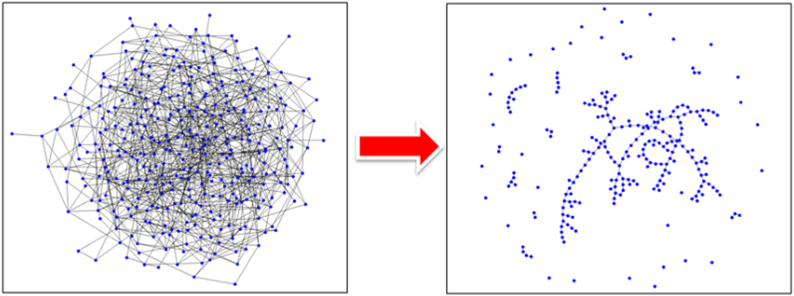


Critical Nodes Detection Problem



Critical node detection problem (CNP)

Given a graph $G(V, E)$ and an integer k, find a set of at most k nodes, whose deletion minimizes the pairwise connections of the residual network. (The critical edge detection problem is similar).



CNP - Formulation

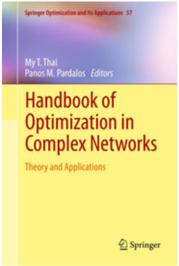
- V := Set of vertices
- E := Set of edges
- k := Number of critical nodes to identify
- $v_i := \begin{cases} 1 & \text{if node } i \text{ is critical} \\ 0 & \text{otherwise} \end{cases}$
- $u_{ij} := \begin{cases} 1 & \text{if } i \text{ and } j \text{ are in the same component} \\ 0 & \text{otherwise} \end{cases}$

$$
\begin{aligned}
\min \; & \sum_{i,j \in V} u_{ij} \\
\text{s.t. } & u_{ij} + v_i + v_j \geq 1 && \forall (i,j) \in E \\
& u_{ij} + u_{jk} - u_{ki} \leq 1 && \forall (i,j,k) \in V \\
& u_{ij} - u_{jk} + u_{ki} \leq 1 && \forall (i,j,k) \in V \\
& -u_{ij} + u_{jk} + u_{ki} \leq 1 && \forall (i,j,k) \in V \\
& \sum_{i \in V} v_i \leq k \\
& u_{ij} \in \{0,1\} && \forall (i,j) \in V \\
& v_i \in \{0,1\} && \forall i \in V
\end{aligned}
$$

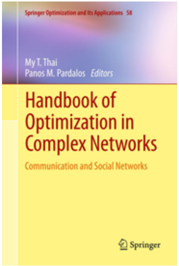
A. Arulsevan and C. W. Commander and L. Elefteriadou and P. M. Pardalos,
Detecting Critical Nodes in Sparse Graphs, Computers and Operations Research, 2009, pp. 2193-2200

Handbook of Optimization in Complex Networks

- Theory and Applications. My T. Thai and Panos M. Pardalos (Eds.) Springer. Series: Springer Optimization and Its Applications , 2012. Vol. 57. ISBN 978-1-4614-0753-9.

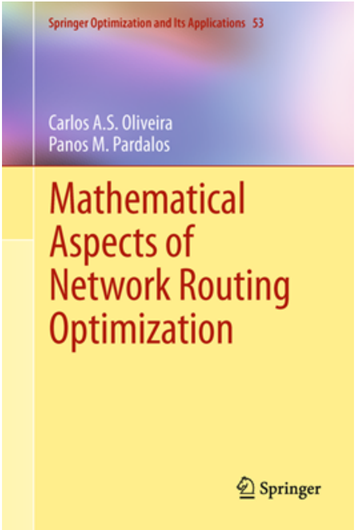


- Communications and Social Networks. My T. Thai and Panos M. Pardalos (Eds.) Springer. Series: Springer Optimization and Its Applications , 2012. Vol. 58. ISBN 978-1-4614-0856-7.



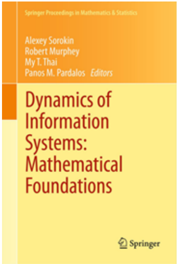
Handbook of Optimization in Complex Networks

- Mathematical Aspects of Network Routing Optimization. Carlos Oliveira and Panos M. Pardalos. Springer. Series: Springer Optimization and Its Applications , 2011. Vol. 53. ISBN 978-1-4614-0310-4.

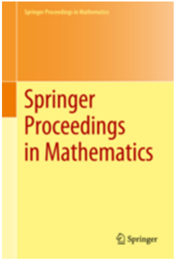


Handbook of Optimization in Complex Networks

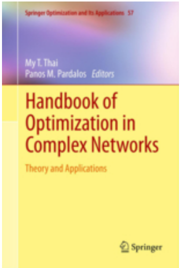
- Dynamics of Information Systems: Mathematical Foundations. Alexey Sorokin, Robert Murphey, My T. Thai, and Panos M. Pardalos (Eds.) Springer. Springer Proceedings in Mathematics & Statistics, 2012. Vol. 20. ISBN 978-1-4614-3905-9.



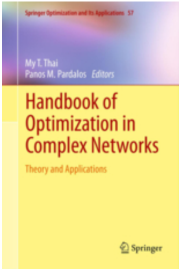
- Dynamics of Information Systems: Algorithmic Approaches. Alexey Sorokin, Robert Murphey, My T. Thai, and Panos M. Pardalos (Eds.) Springer. Springer Proceedings in Mathematics & Statistics., 2013. Vol. 51. ISBN 978-1-4614-3905-9.



- Handbook of Optimization in Complex Networks: Theory and Applicatios. My T. Thai, and Panos M. Pardalos (co-eds.) Springer (2011).

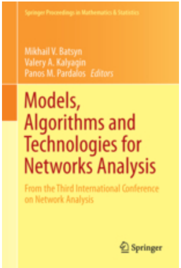


- Handbook of Optimization in Complex Networks: Communication and Social Networks. My T. Thai, and Panos M. Pardalos (co-eds.) Springer (2011).



Handbook of Optimization in Complex Networks

- Models, Algorithms and Technologies for Networks Analysis: From the Third International Conference on Network Analysis. Mikhail V. Batsyn, Valery A. Kalyagin and P. Pardalos.



Quantification of Network Robustness

Quantification of network robustness could be thought as the distance that a given topology is apart from itself after a failure.

T. Schieber, L. Carpi, A. Frery, O. Rosso, **Panos M. Pardalos**, M. Ravetti, **Information theory perspective on network robustness**, Physics Letters A, 2016

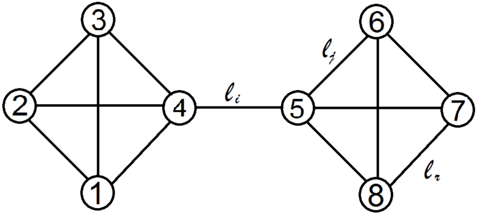
Classical Robustness Measurements

There are two commonly used methods based on the largest connected component (R_{bc}) and percolation (R_{π_d}) to measure network robustness after failures

- R_{bc} is obtained by computing the fraction of nodes belonging to the largest connected component
- R_{π_d} indicates the variation of the original diameter d_0 with respect to diameter d after a sequence of failures, computed by $R_{\pi_d} = d_0/d$

Classical Robustness Measurements

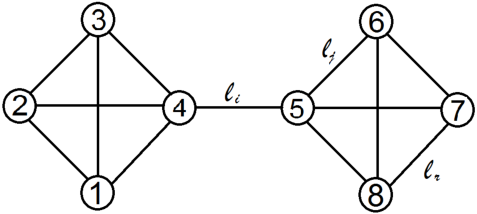
- R_{bc} is obtained by computing the fraction of nodes belonging to the largest connected component
- R_{π_d} indicates the variation of the original diameter d_0 with respect to diameter d after a sequence of failures, computed by $R_{\pi_d} = d_0/d$



Edge Removed	R_{bc}	R_{π_d}
ℓ_i	0.500	0.000
ℓ_j	1.000	0.750
ℓ_r	1.000	1.000

Classical Robustness Measurements - Problem

- Methodologies based on the size of the largest connected component, or on the diameter, are not able to properly capture some failures.



Edge Removed	R_{bc}	R_{π_d}
ℓ_i	0.500	0.000
ℓ_j	1.000	0.750
ℓ_r	1.000	1.000

Robustness - Information Theory Quantifiers

- Several network characteristics can be represented by a probability distribution
- Degree distribution of a graph characterizes **global statistical patterns** underlying the dataset this graph represents
- Interestingly, the degree distribution of all considered real-life graphs has a well-defined **power-law** structure: The probability that a vertex has a degree k is:

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

("Self-organized" networks)

Robustness - Information Theory Quantifiers

- Several network characteristics can be represented by a probability distribution
- Degree distribution of a graph characterizes **global statistical patterns** underlying the dataset this graph represents
- Interestingly, the degree distribution of all considered real-life graphs has a well-defined **power-law** structure: The probability that a vertex has a degree k is:

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

("Self-organized" networks)

The distance distribution gives the fraction of pairs of nodes connected distance d and $\mathbf{P}(\infty)$ gives the the fraction of pairs of disconnected nodes. It is possible to obtain:

- Average degree
- Average path length
- Diameter

Robustness - Information Theory Quantifiers

You can also get a local information

The node distance distribution is a set of probability distributions associated with each node i a probability distribution $\mathbf{P}_i(d)$ representing the fraction of nodes connected to i at distance d and $\mathbf{P}_i(\infty)$ is the fraction of disconnected nodes from i.

- Network distance distribution
- Degree sequence
- Closeness centrality
- Number and the size of connected clusters

We propose a measure for network robustness based on the Jensen-Shannon divergence, a *square of a metric* between probability distributions, that already showed to be very effective in measuring small topological changes in a network.

$$\mathcal{J}^H(P,Q) = H\left(\frac{P+Q}{2}\right) - \frac{H(P)+H(Q)}{2},$$

being $H(P) = -\sum_i p_i \log_2 p_i$, the Shannon entropy that measures the *amount of uncertainty* in a probability distribution.

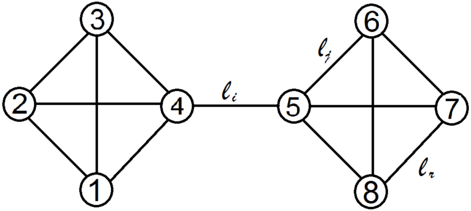
Robustness - Information Theory Quantifiers

Let G' be a failure in G and P a probability distribution representing some network characteristics, the robustness of G given the failure G' is given by:

$$R_P(G|G') = 1 - \mathcal{J}^H(P(G), P(G')). \quad (1)$$

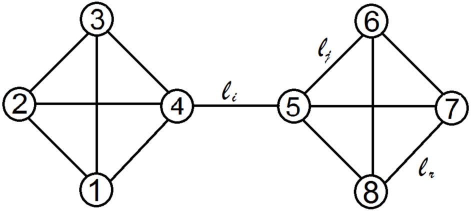
The robustness value ranges from 0, the largest variation, to 1, unchanged characteristics.

Computation of the structural robustness for three different single edge removal: ℓ_i, ℓ_j and ℓ_r.
P_δ and P_{deg} are the distance and degree distributions, respectively.



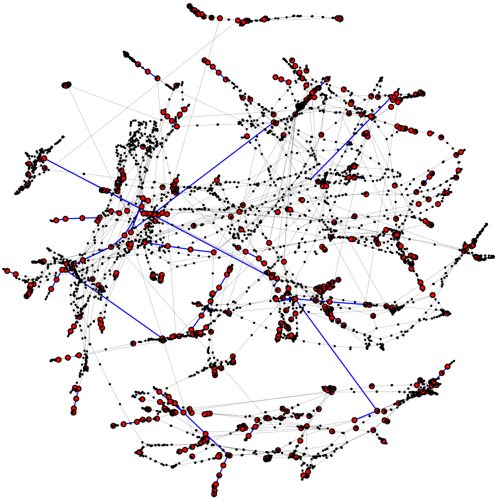
Edge Removed	R_{P_δ}	$R_{P_{deg}}$	R_{bc}	R_{π_d}
ℓ_i	0.447	0.862	0.500	0.000
ℓ_j	0.943	0.922	1.000	0.750
ℓ_r	0.998	0.857	1.000	1.000

Computation of the structural robustness for three different single edge removal: ℓ_i, ℓ_j and ℓ_r.
P_δ and P_{deg} are the distance and degree distributions, respectively. The measure captures all changes, including those perceived by R_{bc} and R_{π_d}.



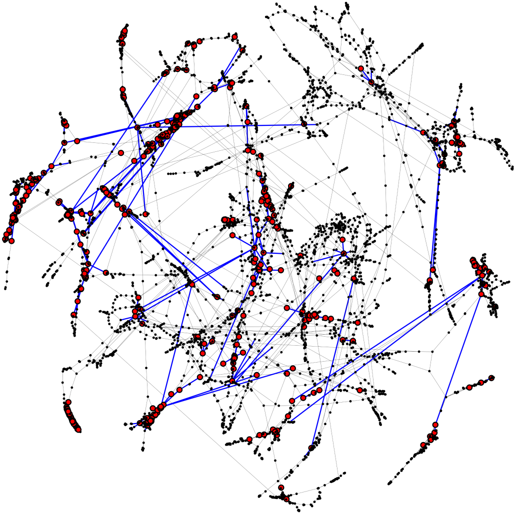
Edge Removed	R_{P_δ}	$R_{P_{deg}}$	R_{bc}	R_{π_d}
ℓ_i	0.447	0.862	0.500	0.000
ℓ_j	0.943	0.922	1.000	0.750
ℓ_r	0.998	0.857	1.000	1.000

Detecting critical elements. US POWER GRID using the distance distribution R_{P_δ}.



Edge ID	R_δ
4220 – 2544	0.9695
4220 – 4165	0.9960
3046 – 2523	0.9962
3046 – 3045	0.9964
3048 – 2523	0.9964
3048 – 3047	0.9968
363 – 270	0.9974
3074 – 3047	0.9974
347 – 270	0.9978
347 – 342	0.9980
Node ID	**R_δ**
4220	0.9675
2544	0.9677
727	0.9786
693	0.9887
2529	0.9914
2523	0.9919
2605	0.9941
4165	0.9946
363	0.9949
427	0.9955

Detecting critical elements. US POWER GRID using the degree distribution $R_{P_{deg}}$.



Edge ID	R_{deg}
3129 – 2554	0.5013
2909 – 2554	0.5013
3285 – 2554	0.5013
2844 – 2554	0.5013
2875 – 2554	0.5013
2972 – 2554	0.5013
2802 – 2554	0.5013
2871 – 2554	0.5013
2872 – 2554	0.5013
2873 – 2554	0.5013
Node ID	**R_{deg}**
2554	0.5012
3129	0.5013
2909	0.5013
3285	0.5013
2844	0.5013
2871	0.5013
2872	0.5013
2873	0.5013
3150	0.5013
2875	0.5013

Robustness to a sequence of failures

A network may suffer a time-dependent sequence of failures since the degree to which a networked system continues to function, as its component parts are degraded, typically depends on the integrity of the underlying network.

- A time-ordered sequence of failures $\mathcal{F} = \{f_{t_1}, f_{t_2}, \ldots, f_{t_n}\}$ in G can be interpreted as a sequence of the resulting networks after each event $(G_{t_i})_{i \in \{0,\, 1, \ldots, n\}}$ such that $G_{t_0} = G$ and G_{t_i} is the network obtained after the failure f_{t_i} in $G_{t_{i-1}}$.

Robustness to a sequence of failures

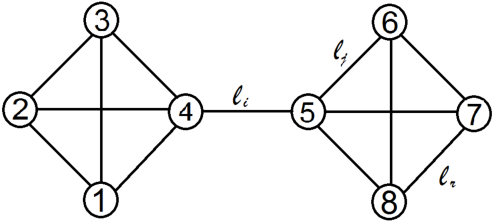
A network may suffer a time-dependent sequence of failures since the degree to which a networked system continues to function, as its component parts are degraded, typically depends on the integrity of the underlying network.

- A time-ordered sequence of failures $\mathcal{F} = \{f_{t_1}, f_{t_2}, \ldots, f_{t_n}\}$ in G can be interpreted as a sequence of the resulting networks after each event $(G_{t_i})_{i \in \{0,\,1,\ldots,n\}}$ such that $G_{t_0} = G$ and G_{t_i} is the network obtained after the failure f_{t_i} in $G_{t_{i-1}}$.

Robustness to a sequence of failures

Comparing two sequences of failures:

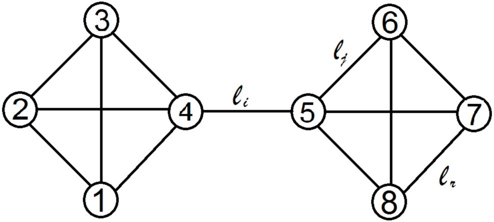
- Sequence 1: link ℓ_i fails at instant $t = 1$ and link ℓ_j fails at instant $t = 2$
- Sequence 2: link ℓ_j fails at instant $t = 1$ and link ℓ_i fails at instant $t = 2$
- At $t = 2$ the same degraded network is obtained but the sequence 1 should possess a lower robustness value considering network connectivity because a big disconnection is caused by the failure of link ℓ_i at the beginning of the process ($t = 1$)



Robustness to a sequence of failures

Comparing two sequences of failures:

- Sequence 1: link ℓ_i fails at instant $t = 1$ and link ℓ_j fails at instant $t = 2$
- Sequence 2: link ℓ_j fails at instant $t = 1$ and link ℓ_i fails at instant $t = 2$
- At $t = 2$ the same degraded network is obtained but the sequence 1 should possess a lower robustness value considering network connectivity because a big disconnection is caused by the failure of link ℓ_i at the beginning of the process ($t = 1$)



Robustness to a sequence of failures

For any given sequence of n failures $(G_t)_{t\in\{1,\,2,\ldots,n\}}$ and probability distribution P the network robustness is given by:

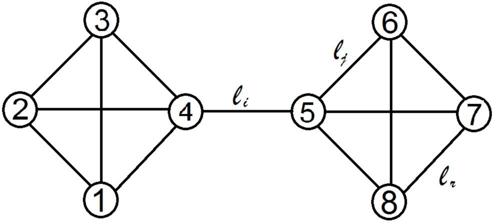
$$R_P(G|(G_t)_{t\in\{1,\,2,\ldots,n\}}) = \prod_{t=1}^{n} R_P(G_{t-1}|G_t)$$

in which, for each time step, $R_P(G_{t-1}|G_t)$ indicates how affected the topology of the network G_{t-1} is after a single failure resulting in G_t.

Robustness to a sequence of failures

Comparing two sequences of failures:

- Sequence 1: link ℓ_i fails at instant $t = 1$ and link ℓ_j fails at instant $t = 2$ ($R_{P_\delta} = 0.4377$)
- Sequence 2: link ℓ_j fails at instant $t = 1$ and link ℓ_i fails at instant $t = 2$ ($R_{P_\delta} = 0.4564$)
- At $t = 2$ the same degraded network is obtained but the sequence 1 should possess a lower robustness value considering network connectivity because a big disconnection is caused by the failure of link ℓ_i at the beginning of the process ($t = 1$)



We test the proposed methodology on several real networks and for different stochastic measures:

- P_{deg} - degree distribution
- P_{δ} - distance distribution
- P_{C} - clustering coefficient
- P_{B_v} - vertex betweenness centrality
- P_{Cl} - closeness centrality

Computational Experiments

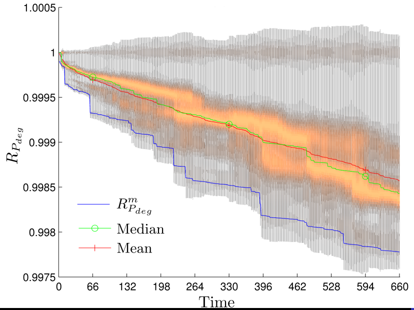
- Random Failure Experiment: At each time step a single link is randomly removed until the global disconnection of 10
- Targeted attack: at each time step, the most central element fails

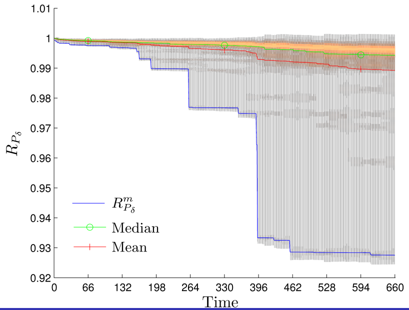
Example 1: Random Failure at US POWER GRID

The US Power Grid Network is the undirected and unweighted representation of the topology of the Western States Power Grid of the United States, compiled by Duncan Watts and Steven Strogatz.

At each time step a single link is randomly removed until the global disconnection of approximately 10% of their links

Violin plots for $R_{P_{deg}}$ and R_{P_δ}.





Example 2: Targeted attack - Florida ecosystem wet and dry

- Both networks contains the carbon exchanges in the cypress wetlands of South Florida during the wet and dry seasons, respectively. Nodes represent taxa and an edge denotes that a taxon uses another taxon as food with a given trophic factor (feeding level).
- The networks are directed and weighted

Example 2: Targeted attack - Florida ecosystem wet and dry

- The experiment consists in the attack of the most central nodes of the network given by the α centrality.

$$C_\alpha^{in}(v) = (k_v^{in})^{1-\alpha}(w_v^{in})^\alpha \qquad \text{and} \qquad C_\alpha^{out}(v) = (k_v^{out})^{1-\alpha}(w_v^{out})^\alpha$$

$\alpha = 0$ the centrality is given only by the degree centrality (the weights are forgotten). By setting $\alpha = 1$ the centrality is given by the total vertex weight (the connections are forgotten)

- At each time step, the most central vertex is disconnected from the network until its the complete disconnection.
- Which α gives the best strategy in destroying the network more efficiently?

Example 2: Targeted attack - Florida ecosystem wet and dry

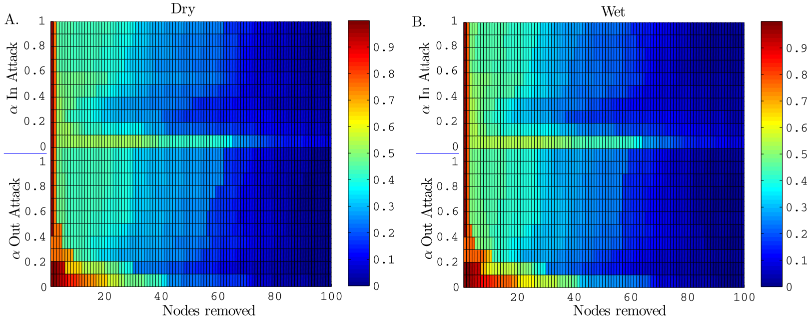
- The experiment consists in the attack of the most central nodes of the network given by the α centrality.

$$C_\alpha^{in}(v) = (k_v^{in})^{1-\alpha}(w_v^{in})^\alpha \qquad \text{and} \qquad C_\alpha^{out}(v) = (k_v^{out})^{1-\alpha}(w_v^{out})^\alpha$$

$\alpha = 0$ the centrality is given only by the degree centrality (the weights are forgotten). By setting $\alpha = 1$ the centrality is given by the total vertex weight (the connections are forgotten)

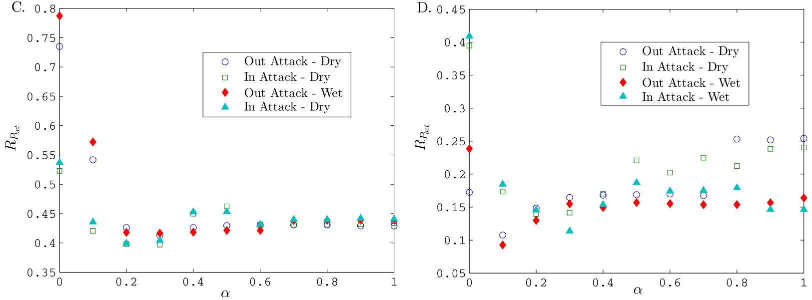
- At each time step, the most central vertex is disconnected from the network until its the complete disconnection.
- Which α gives the best strategy in destroying the network more efficiently?

Example 2: Florida ecosystem wet and Florida ecosystem dry



Example 2: Florida ecosystem wet and Florida ecosystem dry

Comparing strategies: C. After the removal of 10% of the nodes and D. After the removal of 50% of the nodes.



Robustness - Information Theory Quantifiers - References

For more examples and applications.

- T. Schieber, M. Ravetti and L. Carpi, ***Evaluation of the copycat model for predicting complex network growth*** In: Vogiatzis, C., Walteros, J. L., **Pardalos, P. M. (Eds.)**, Dynamics of Information Systems. Vol. 105 of Springer Proceedings in Mathematics Statistics. Springer International Publishing, pp. 91108.

- T. Schieber, L. Carpi, A. Frery, O. Rosso, **Panos M. Pardalos**, M. Ravetti, **Information theory perspective on network robustness**, Physics Letters A, 2016

Network Robustness and Network Similarity - An Information Theory Perspective

- Quantification of network robustness could be thought as the distance that a given topology is apart from itself after a failure measuring distances between networks by differences in the topological connectivity
- We propose the use of the network node distance distribution (NND): a set of probability distributions associated with each node i a probability distribution $\mathbf{P}_i(d)$ representing the fraction of nodes connected to i at distance d and $\mathbf{P}_i(\infty)$ is the fraction of disconnected nodes from i.

Network Robustness and Network Similarity - An Information Theory Perspective

- Quantification of network robustness could be thought as the distance that a given topology is apart from itself after a failure measuring distances between networks by differences in the topological connectivity
- We propose the use of the network node distance distribution (NND): a set of probability distributions associated with each node i a probability distribution $\mathbf{P}_i(d)$ representing the fraction of nodes connected to i at distance d and $\mathbf{P}_i(\infty)$ is the fraction of disconnected nodes from i

Network Robustness and Network Similarity - An Information Theory Perspective

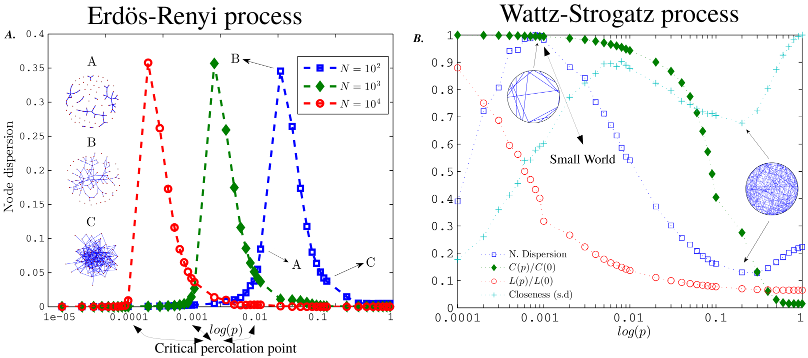
- Quantification of network robustness could be thought as the distance that a given topology is apart from itself after a failure measuring distances between networks by differences in the topological connectivity
- We propose the use of the network node distance distribution: a set of probability distributions associated with each node i a probability distribution $\mathbf{P}_i(d)$ representing the fraction of nodes connected to i at distance d and $\mathbf{P}_i(\infty)$ is the fraction of disconnected nodes from i

Network Node Dispersion

$$NND(G) = \mathcal{J}_H(\mathbf{P}_1, \ldots, \mathbf{P}_n)$$

Compares internal characteristics given by the heterogeneity of the connectivity via the Jensen-Shannon divergence

Network Node Dispersion - Characterization



Network Robustness and Network Similarity - An Information Theory Perspective

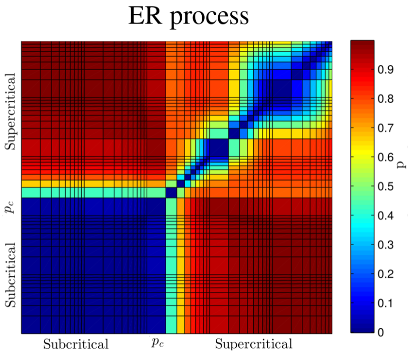
- We define a measure of network dissimilarity by incorporating the Jensen-Shannon divergence between the average node distance distributions differences between their global network connectivities.
- The dissimilarity $D(G, G')$ between G and G' of size n and m, respectively:

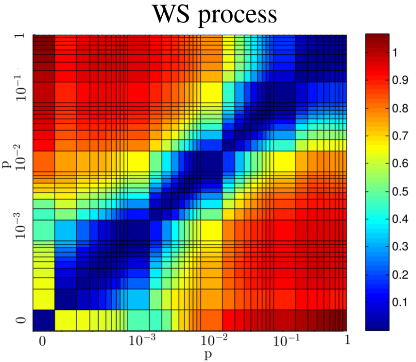
$$D(G, G') = \frac{1}{2}\sqrt{\frac{\mathcal{J}_H(P_G, P_{G'})}{\log 2}} + \frac{1}{2}\left|\sqrt{\frac{NND(G)}{\log n}} - \sqrt{\frac{NND(G')}{\log m}}\right|$$

being, respectively, P_G, $P_{G'}$, the average node distance distribution of networks G and G'

- $D(G, G') = 0$ indicates that G and G' possess the same average of the node distance distributions, and also, identical normalized *NND*
- D is a size independent pseudometric between networks

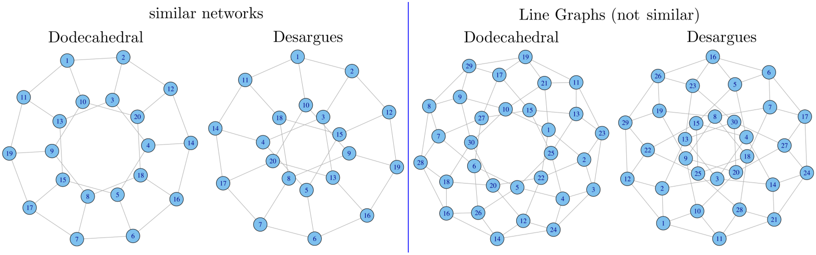
- *D* between all pairs of networks





Network Robustness and Network Similarity - An Information Theory Perspective

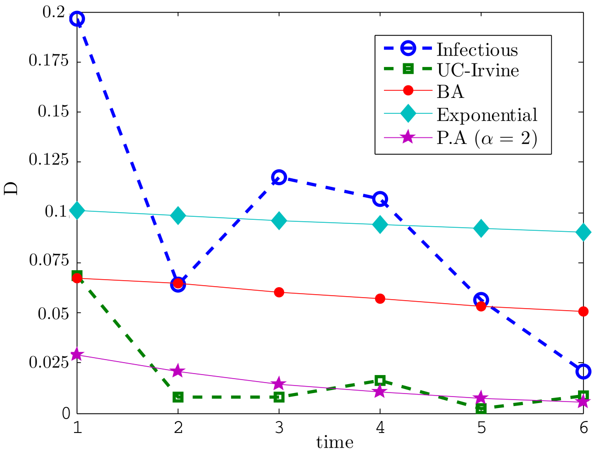
- Graph isomorphism problem



$D = 0$ $D > 0$

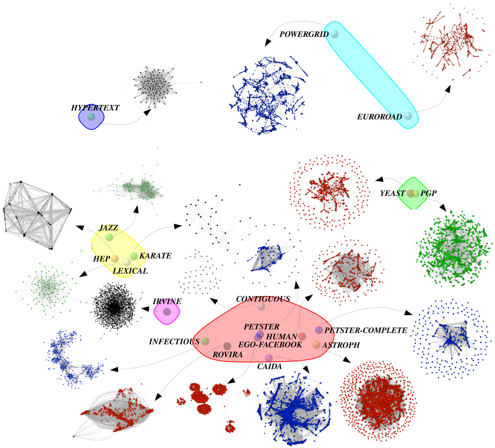
Network Robustness and Network Similarity - An Information Theory Perspective

- Network evolution in time



Network Robustness and Network Similarity - An Information Theory Perspective

- D between pairs of real networks networks



Reference

T. Schieber, L. Carpi, A. Diaz-Guilera, **P. M. Pardalos**, C. Massoler and M. Ravetti
Networks dissimilarities measure based on Information Theory quantifiers, ARXIV FILE

Concluding remarks

ΧΡΥΣΟΝ ΓΑΡ ΟΙ ΔΙΖΗΜΕΝΟΙ ΓΗΝ ΠΟΛΛΗΝ ΟΡΥΣΣΟΥΣΙ ΚΑΙ ΕΥΡΙΣΚΟΥΣΙΝ ΟΛΙΓΟΝ

”Seekers after gold dig up much earth and find little”

”The lord whose oracle is at Delphi neither speaks nor conceals, but gives signs”

- Heraclitus

I shall be telling this with a sigh
Somewhere ages and ages hence:
Two roads diverged in a wood, and I,
I took the one less traveled by,
And that has made all the difference.

- Robert Frost