Robustness Against Large-Scale Failures in Communications Networks: a Simulation Approach

ONDM, Budapest, 2017

Jose L Marzo
<joseluis.marzo@udg.edu>

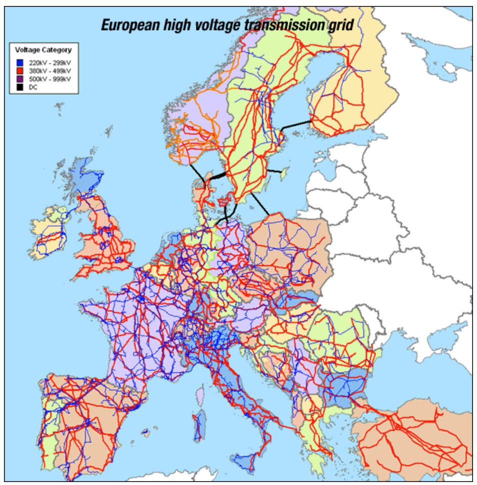
Eusebi Calle
<eusebi.calle@udg.edu>

Contents

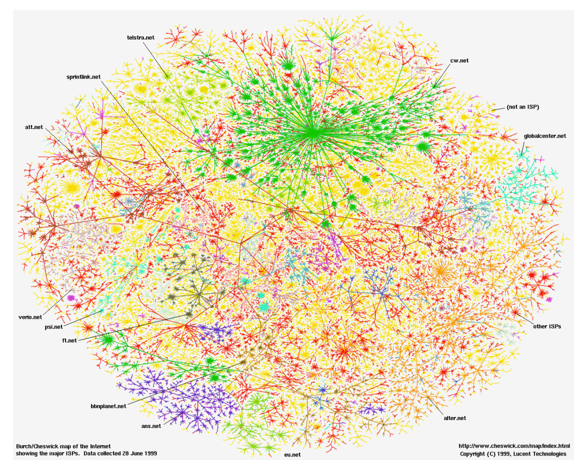
- Motivation
- Network Robustness Simulator
  - Single vs. Multiple failures
  - Dynamic scenarios
  - Robustness metric
  - Results visialization
  - Demo
- Conclusions

Motivation

London's
underground



European power grid



The Internet

http://visualign.wordpress.com/2012/07/11/london-tube-map-and-graph-visualizations/
www.geni.org
www.cheswick.com

Network Robustness Simulator

- **Multiple failures**
  - Single vs multiple
  - Correlated
- Dynamic scenarios (“attacks”)
- Robustness metric
- Results visualization

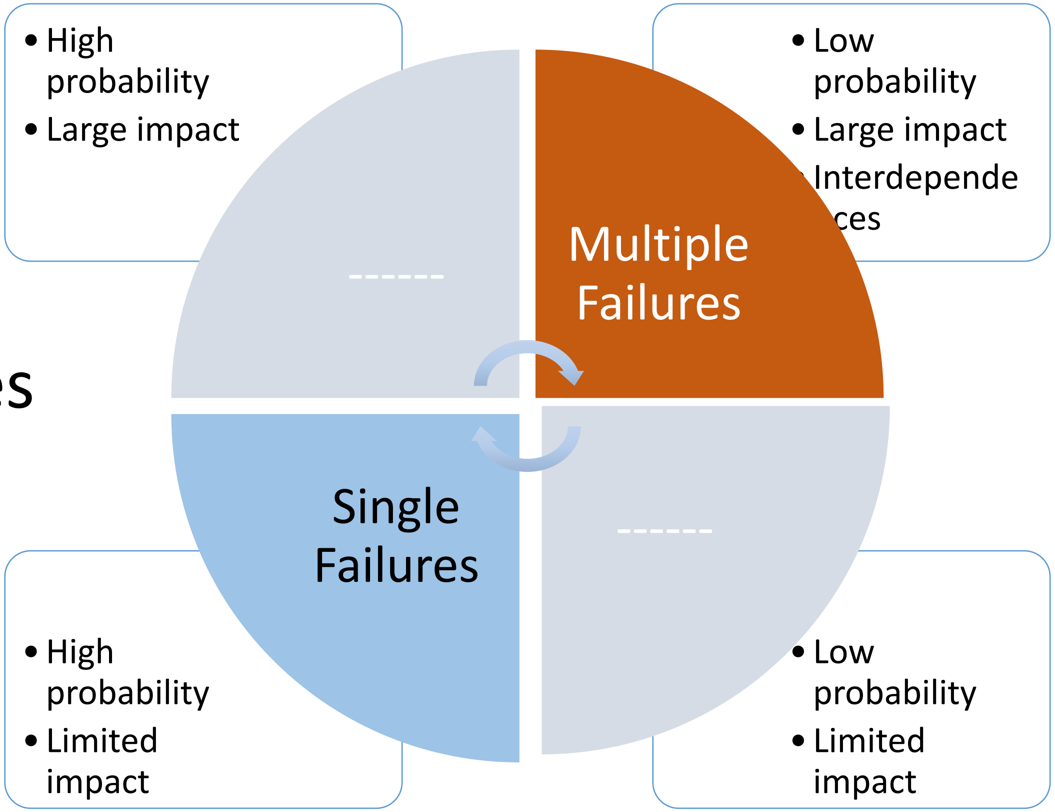
Single vs. Multiple failures

Because multiple failures happen rarely…

- there is less incentive to tackle them

- but that is changing: **their consequences are too costly**

Link / Nodes



Large-scale failure: a multiple failure in which a significant portion of network elements are affected by failures, all related to a single cause.

Network Robustness Simulator

- Multiple failures
- **Dynamic scenarios** (“attacks”)
- Robustness metric
- Results visualization

Dynamic scenarios

Static scenarios are simulated as one-off attacks or failures.

However…

Dynamic failures are more complicated because:

- *They occur along a **period** of time*
- *There is a **cause** that triggers the **propagation***

- On top of random, there are other **interesting cases:**
  - *Targeted*
  - *Epidemics*
  - *Cascading*

Dynamic scenarios: targeted

They are normally provoked by malicious attacks (human driven)

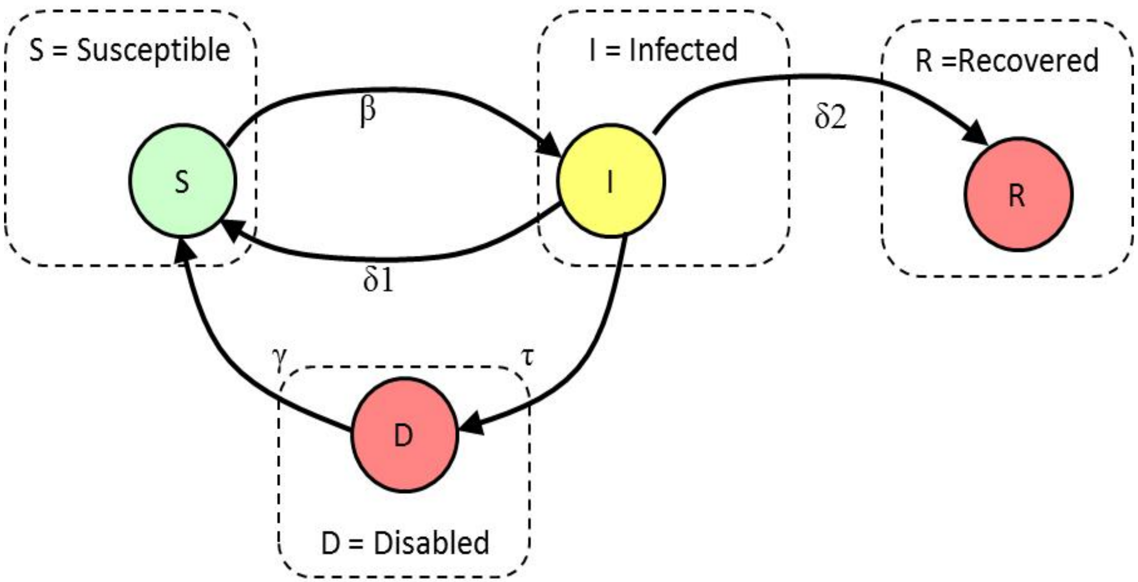
There is a strategy to maximize the impact

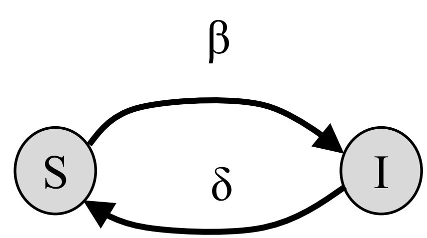
Most important nodes/links are attacked first:

- Hubs (i.e. elements with the highest nodal degree, betweeneness, etc.
- Central links (based on betweeneness)

Dynamic scenarios: epidemics

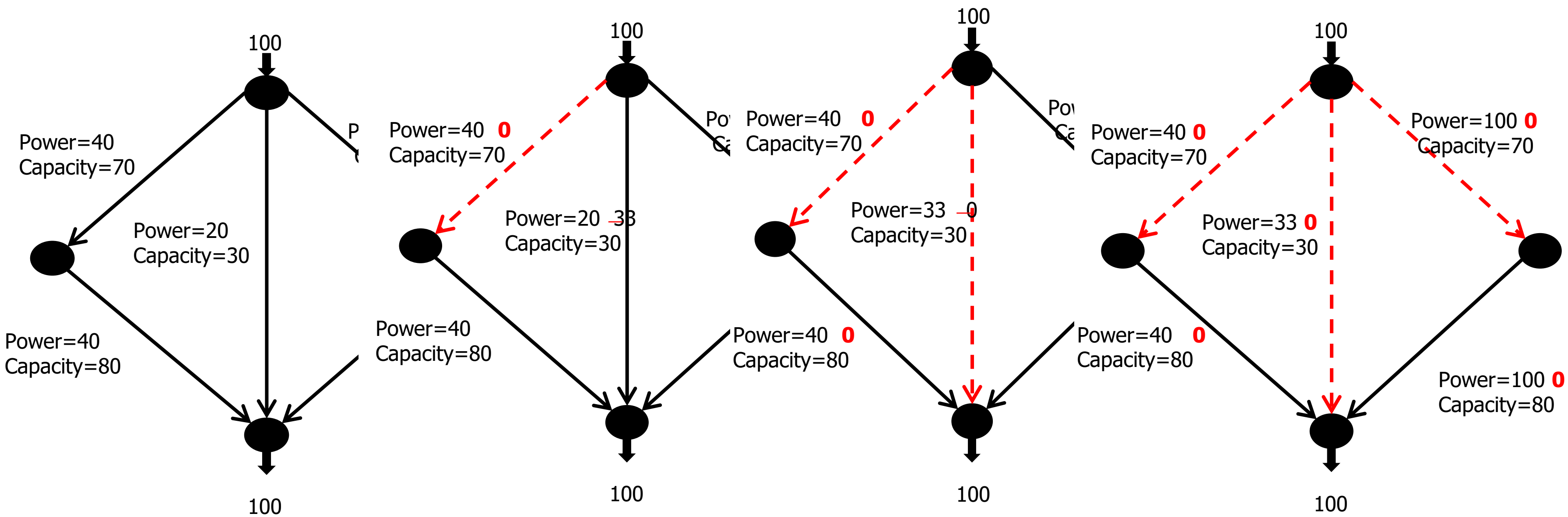
A failure that propagates in the network can be modelled using an **epidemic** model.





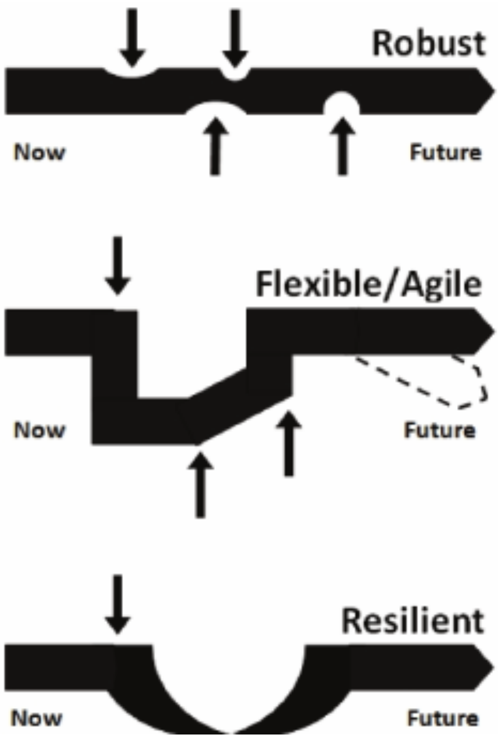
Dynamic scenarios: cascading

A failure that propagates in the network can be modelled using an **cascading** model.



Network Robustness Simulator

- Multiple failures
- Dynamic scenarios (“attacks”)
- **Robustness metric**
  - Structural
  - Centrality
  - Functional
- Results visualization



Robustness metrics

Robustness (robustus / robur), means “oak” in Latin, being the symbol of strength and longevity in the ancient world.

“Robustness is the ability of a network to continue performing well even when it is subject to failures or attacks.”

Robustness metrics

- **Structural**

(based on classic graph properties)

  - Average nodal degree, Finding paths
  - Connectivity & fragmentation

- **Centrality**
(it locates the most “important” nodes/links)

  - Degree, Betweenness, Spectral propierties, Eigenvector, …

- **Dynamic/Functional**

(based on the expected performance of existing **services** on the network)

  - Throughput, Link occupancy, …

Unconnected graphs metric relaxation

After removing some elements, the graph could easily become disconnected and some metrics are useless as they are just defined for connected networks.

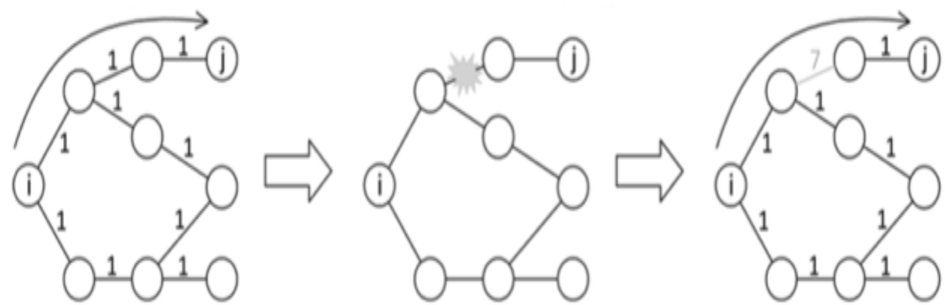
The shortest path between nodes i and j (they are not connected) according the graph theory is ∞.

- In our approach, it becomes useless.

Relaxation: the weight of a missing link is set to the diameter of the full network.

Paths using missing links are artificially long but not infinite.

As all links are equally treated the comparisons among different networks is therefore fair.



“Can we get an unified value of robustness considering “all” metrics?”

Previous work. The R value

Trajanovski et. al have proposed a framework to evaluate the robustness of complex networks, which is based on the generic metric R-value.

The R-value is denoted by:

Number of metrics

Vector of weights

n *metrics*

$$R = \dots \sum_{k=1}^{\boxed{n}} \boxed{s_k}\,\boxed{t_k}$$

Vector of metrics

where ***s*** and ***t*** are n × 1 weight and graph metric vectors, respectively

The R-value includes several graph metrics characterizing the network robustness.

Stojan Trajanovski, Javier Martín-Hernández, Wynand Winterbach, and Piet Van Mieghem. Robustness envelopes of networks. Journal of Complex Networks, 2013.

Robustness Surfaces. R* value

Based on R-value,

$$R = \sum_{k=1}^{n} \boxed{s_k} t_k$$

for a **dynamic** scenario we proposed the **R*-value** obtained by extracting the most informative robustness metric from the **n** computed metrics **and normalised**

$$R^*_{p,m} = \sum_{k=1}^{n} \boxed{\hat{v}_k} t_k$$

a normalized eigenvector

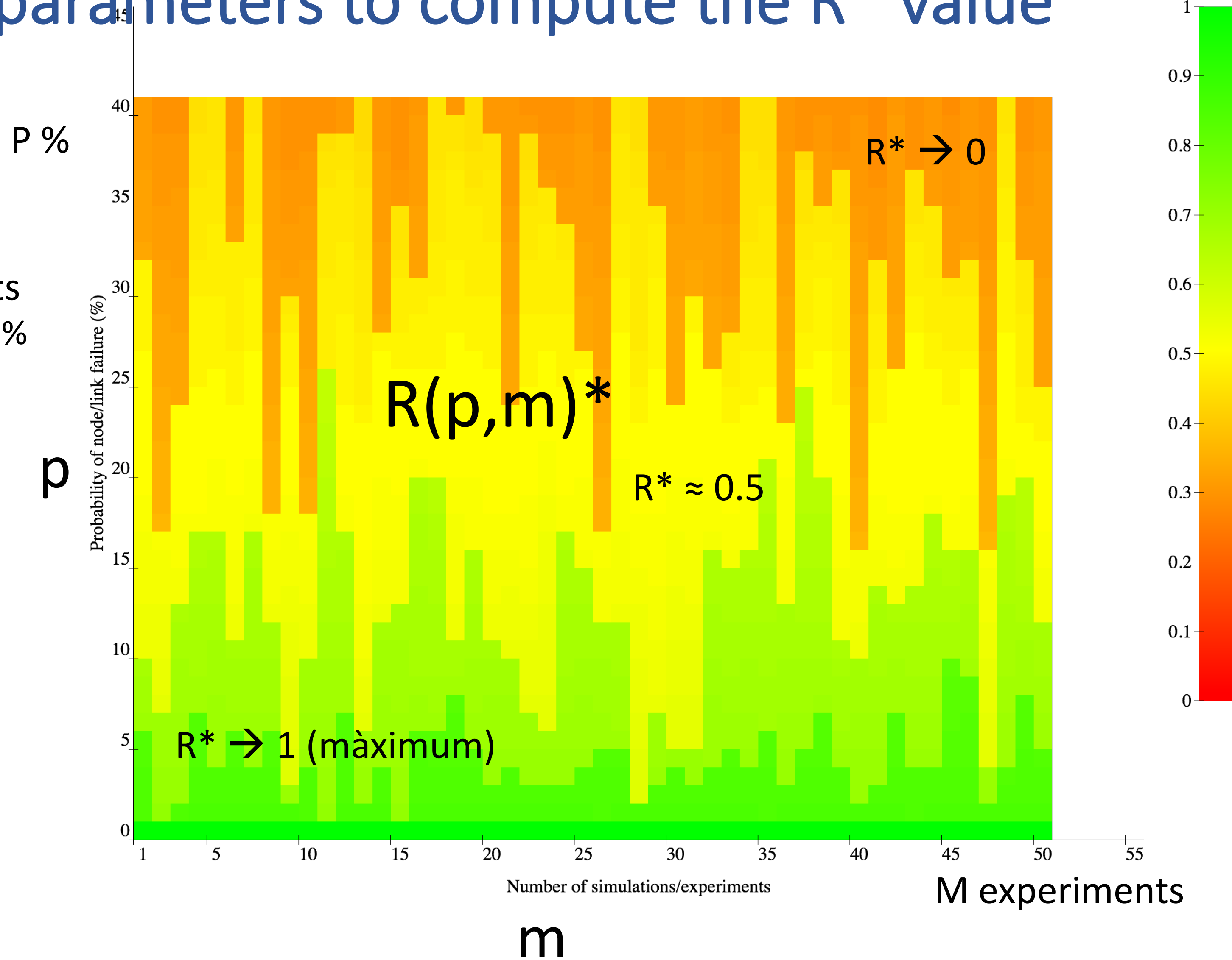
Instead of weights (s_k as for R value) a normalised eigen vector $\hat{v}_k$ is used.

Network Robustness Simulator

- Multiple failures
- Dynamic scenarios ("attacks")
- Robustness metric
- **Results visualization**
  - All numerical results (in a XML file)
  - Robustness surfaces
  - Interactive "attack" visualization

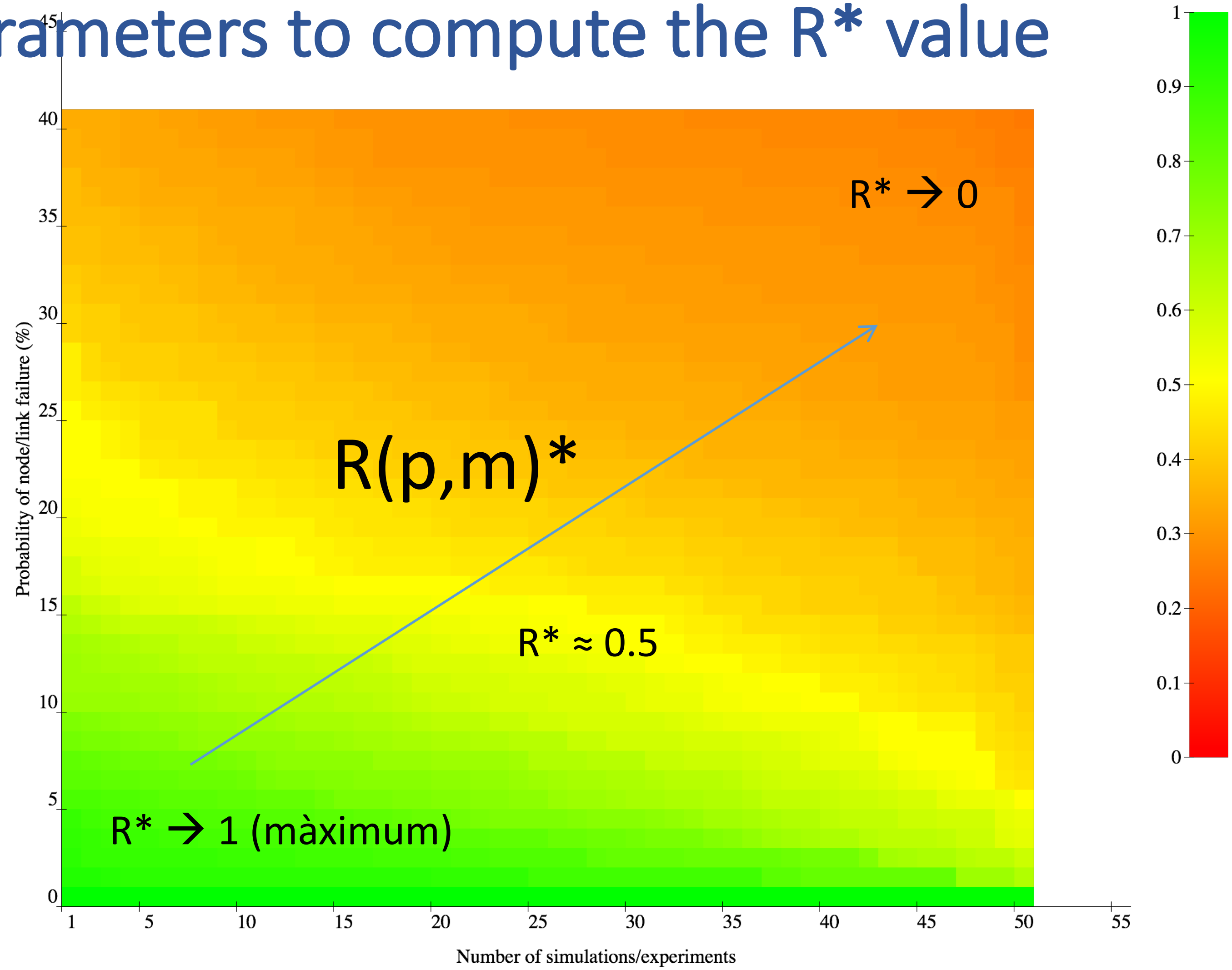
Robustness Surfaces:
p & m parameters to compute the R* value

- In the example a network is "stressesed" by removing **P** elements
  - P varies 0% to 40%
  - P rows are obtained.
- For a given P, **M** independent experiments are performed.
  - M varies 1 to 50
  - M columns are obtanined.



Robustness Surfaces:
p & m parameters to compute the R* value

- In the example a P % network is “stressesed” by removing **P** elements
  - P varies 0% to 40%
  - P rows are obtained.
- For a given P, **M** independent experiments are performed.
  - M varies 1 to 50
  - M columns are obtained.



M experiments

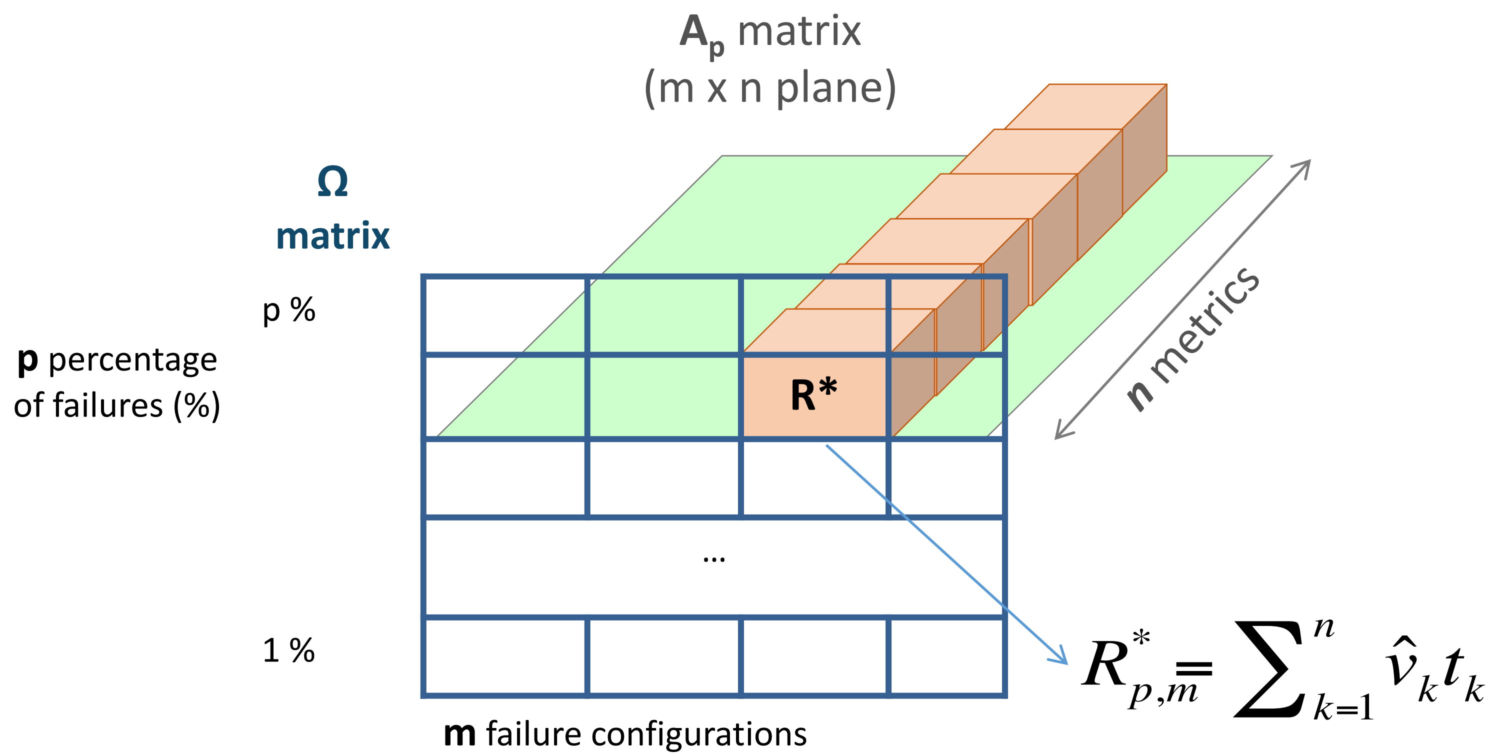
"Robustness surfaces of complex networks", *Manzano, M., Sahneh, F., Scoglio, C., Calle, E., & Marzo, J. L.* Scientific Reports, Nature. September 2014

Robustness Surfaces. Ω matrix

Ω is a matrix where:

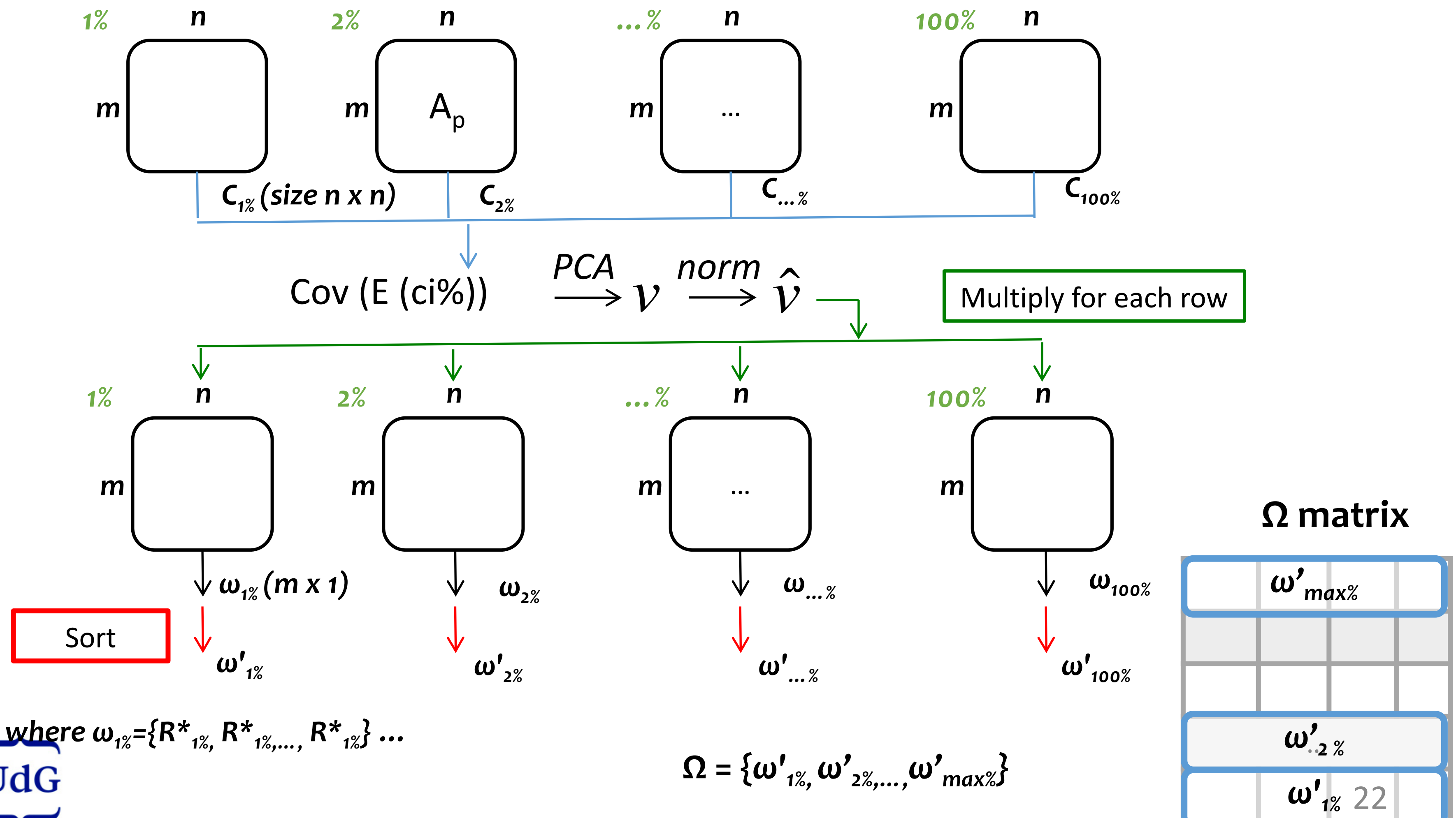
the **rows** are the percentage of failures (p) and

the **columns** are the failure configurations (m) for a giving p

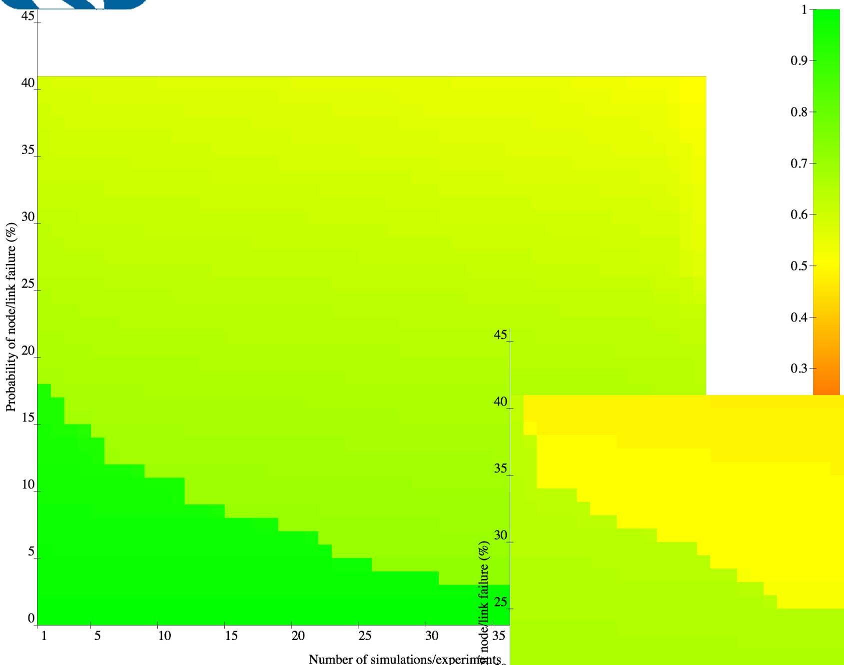


Robustness Surfaces : R* value

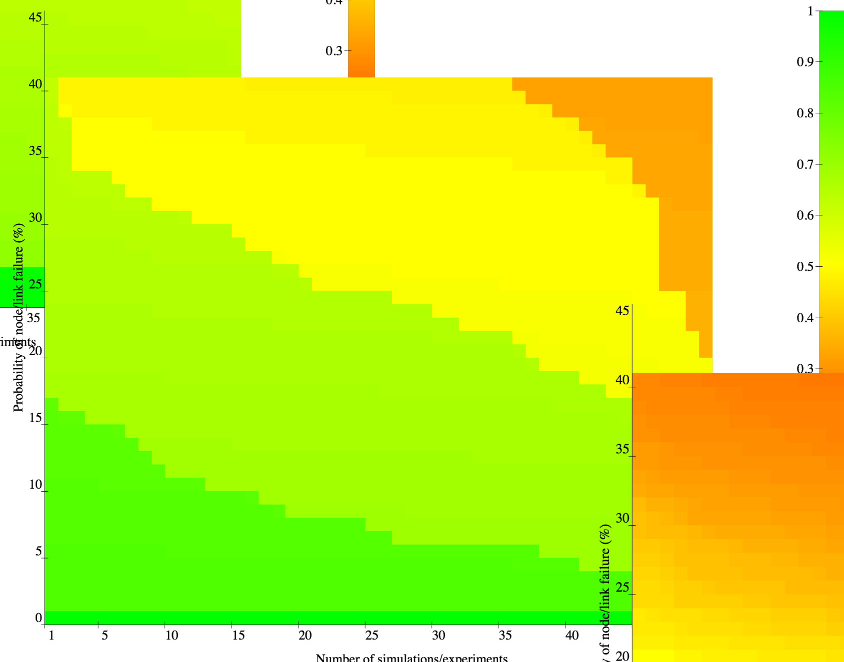
Ω matrix calculation summary



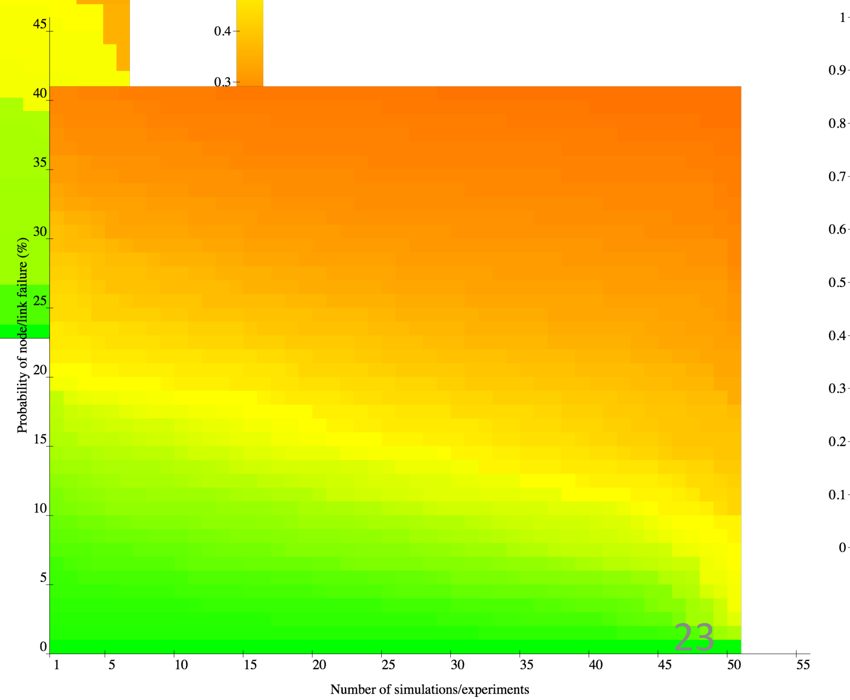
Some results
Robustness surfaces



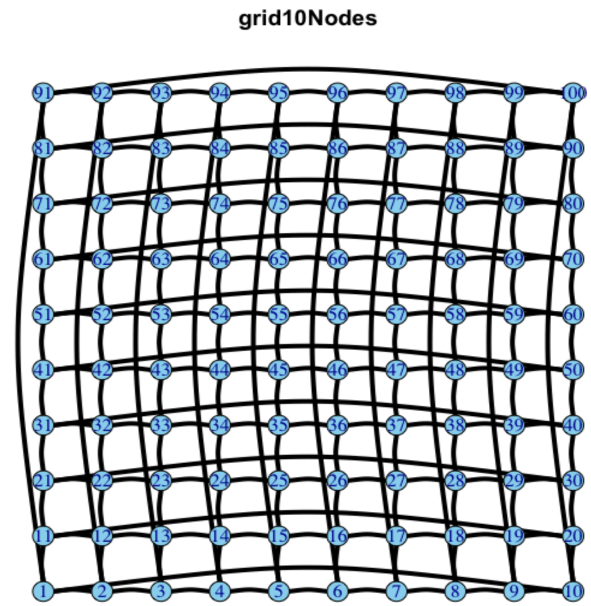
Exponencial



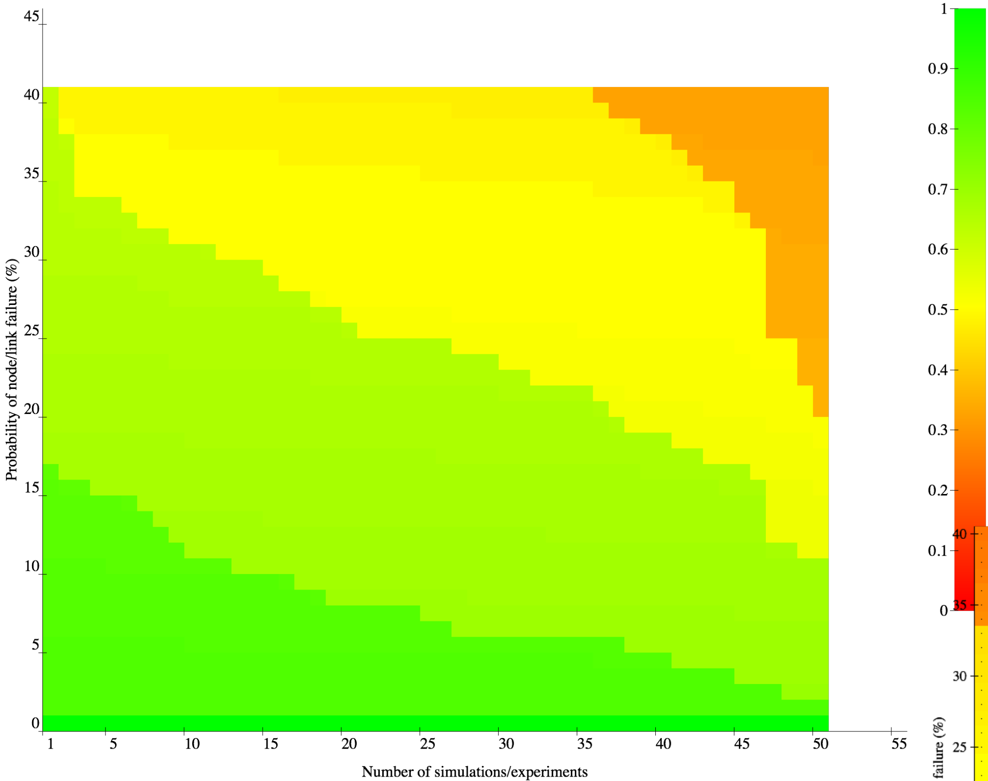
Grid



Tree

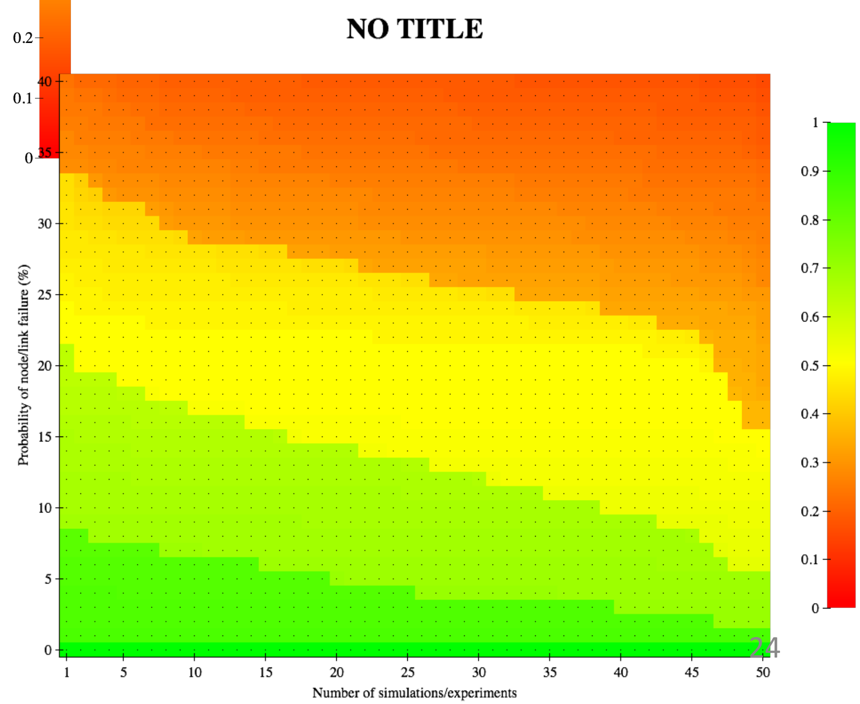


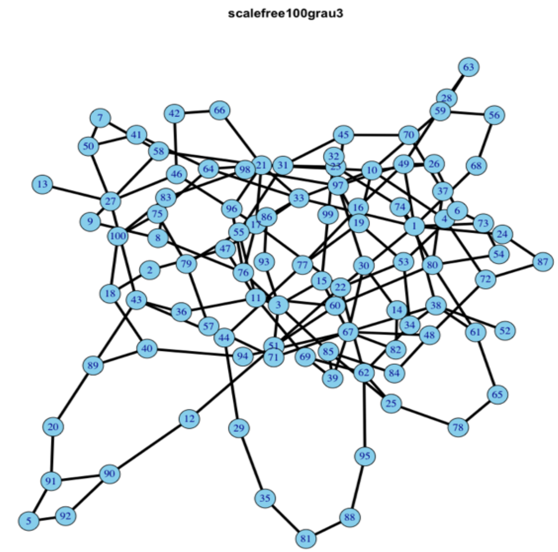
Grid

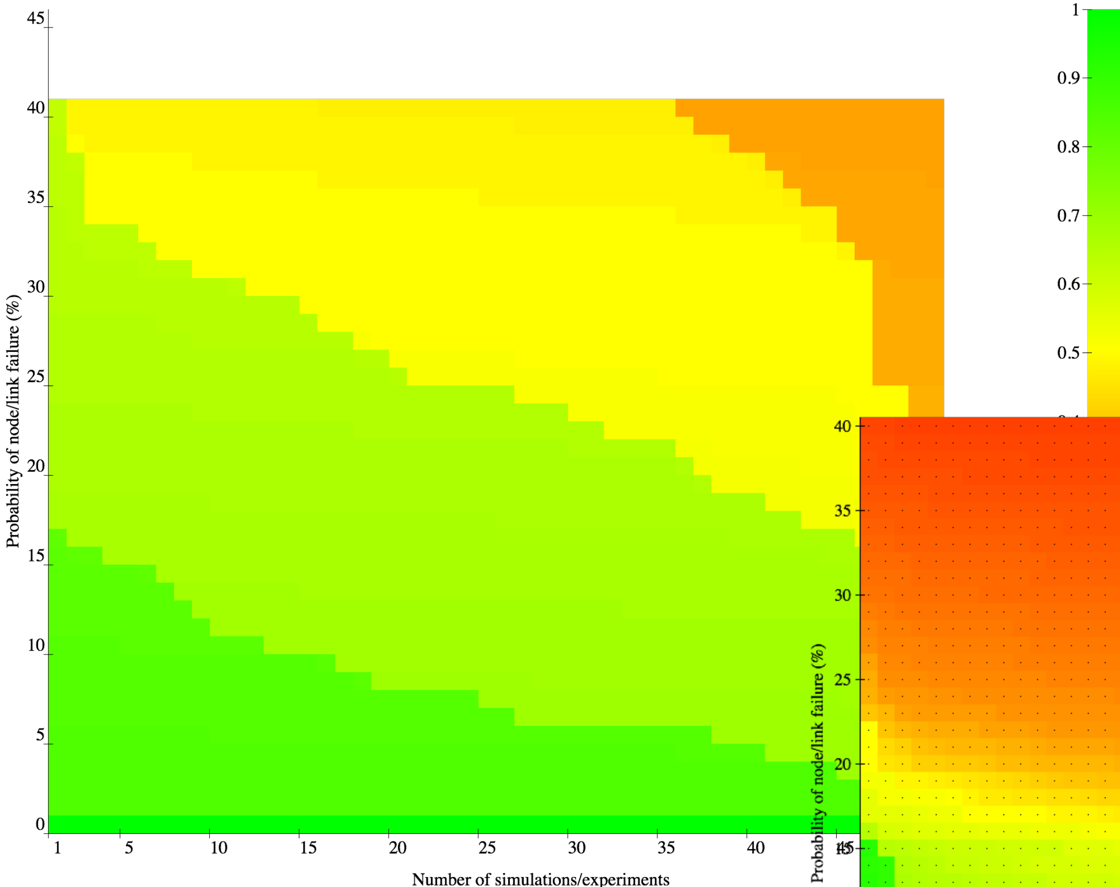


Random

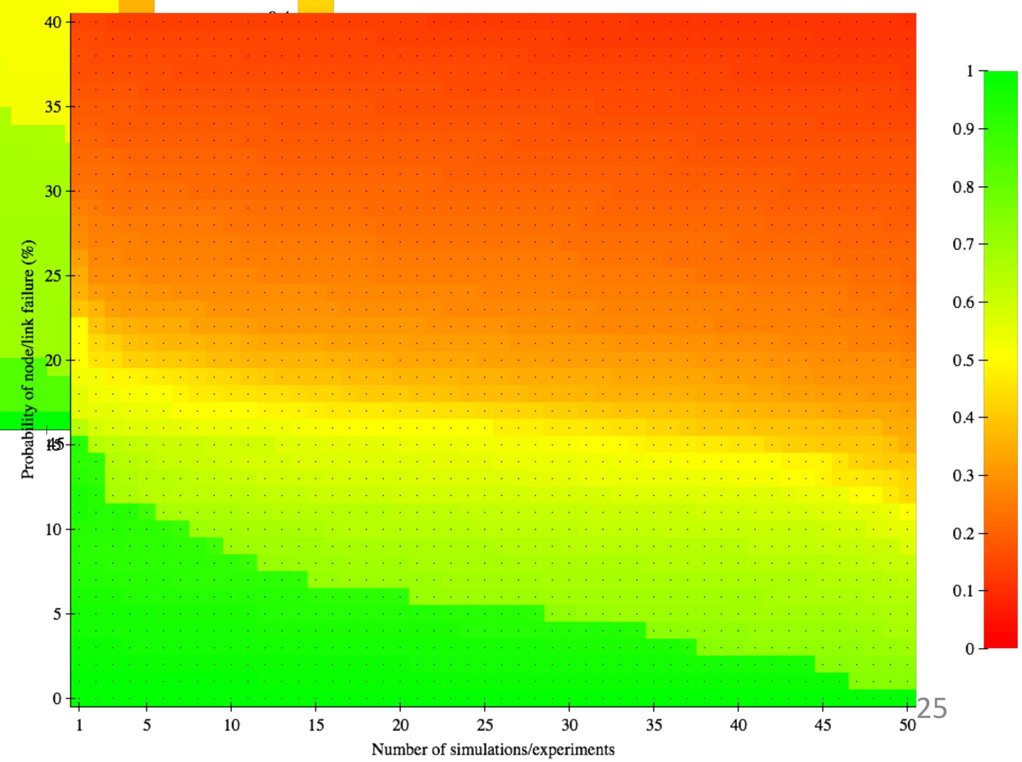
Targeted





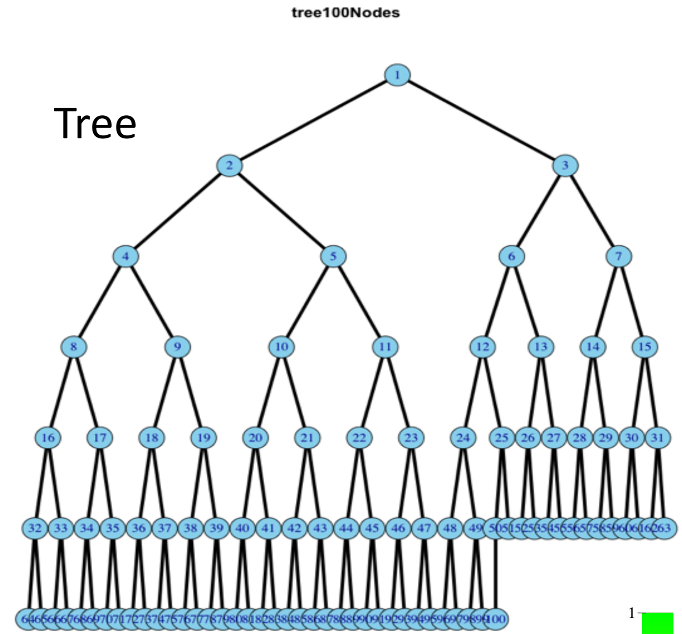


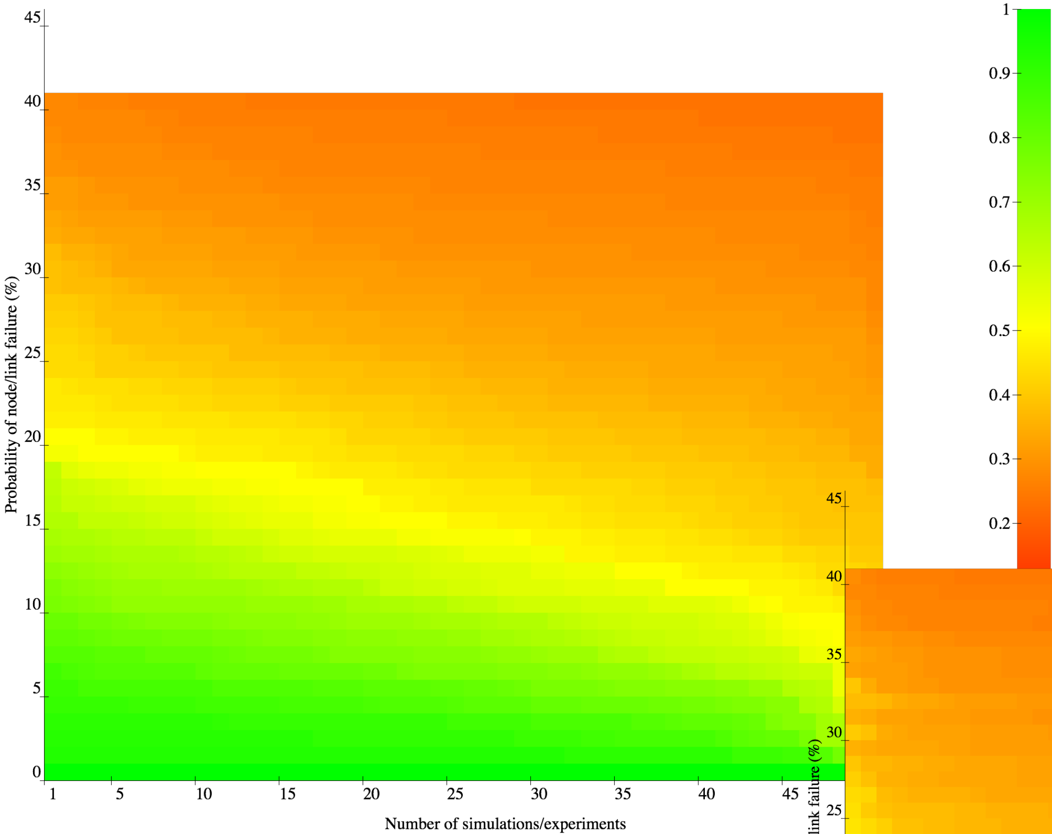
Random



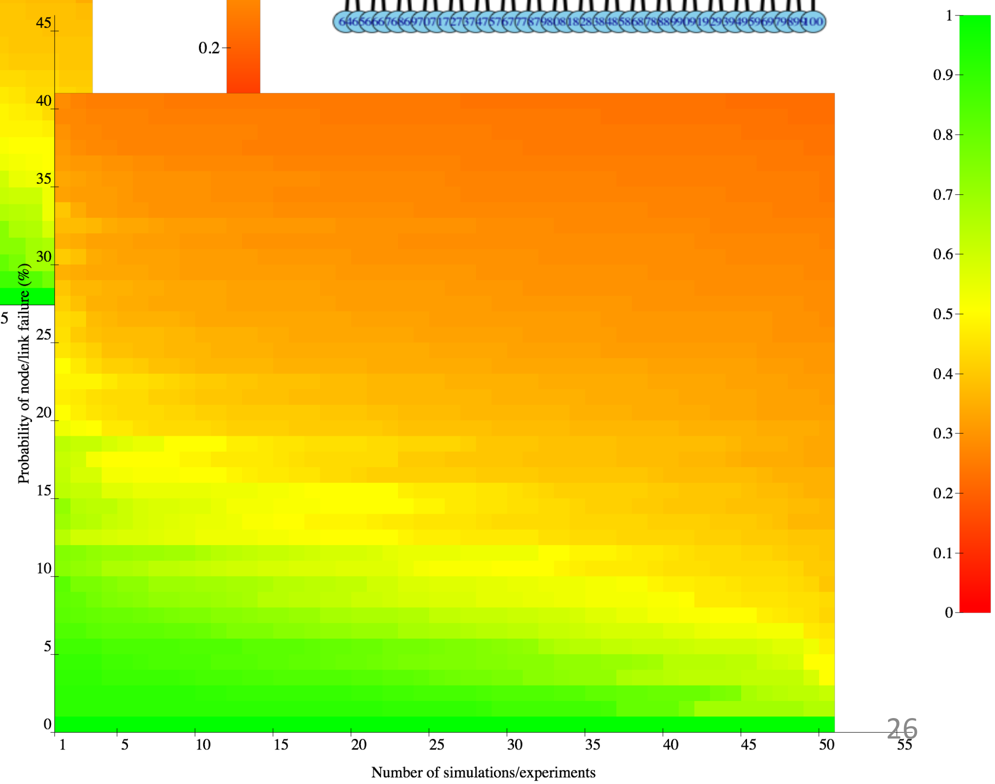
Targeted

Tree





Random



Targeted

video

Conclusions

- A complet set of A_p matrixes are obtained by extending the calculation to diferent percentage of failures and failure configurations.
- Principal Component Analysis (PCA) is used to extract the most significant information of a set of robustness metrics which is used to normalise R-value (obtaining R*-values)
- Drawing the robustness surface, a novel framework is provided to visually assess the network robustness variability

Future work

- To allow automatic comparison between surfaces (on top of visual inspection)
- Backtracking to identify particular failure scenarios with sharp transicions in the surface image
- Increasing the performance of the calculations
    - Most of the calculations can be simultaneously computed
- Adding network interdependences

Thank you!

Acknowledgements:
Diego Rueda
Jordi Capdevila
Sergio Gomez
Antonio Bueno

Broadband Communications and
Distributed Systems Group