CRITIS 2017

Network robustness under massive failures: relevant metrics analysis and simulation

Jose L Marzo
Universitat de Girona
Kansas State University

UdG

Lucca, October, 9th, 2017

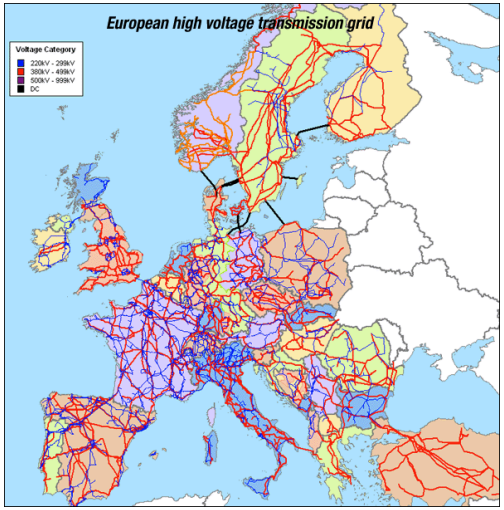
KANSAS STATE UNIVERSITY

Contents

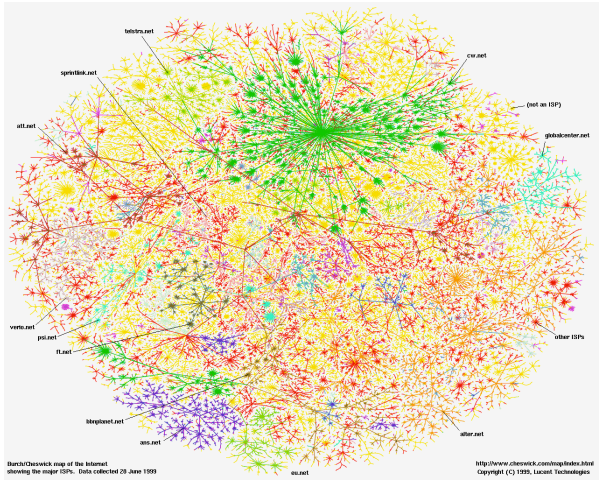
- Motivation
- The robustness concept and metrics
- Modelling multiple failures
- Robustness Computation mechanism
- Simulation scenario and some results
- Conclusions & future work

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

Robustness concept

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 computation relies on graph theory, it is mainly centered on graph connectivity

Robustness metrics

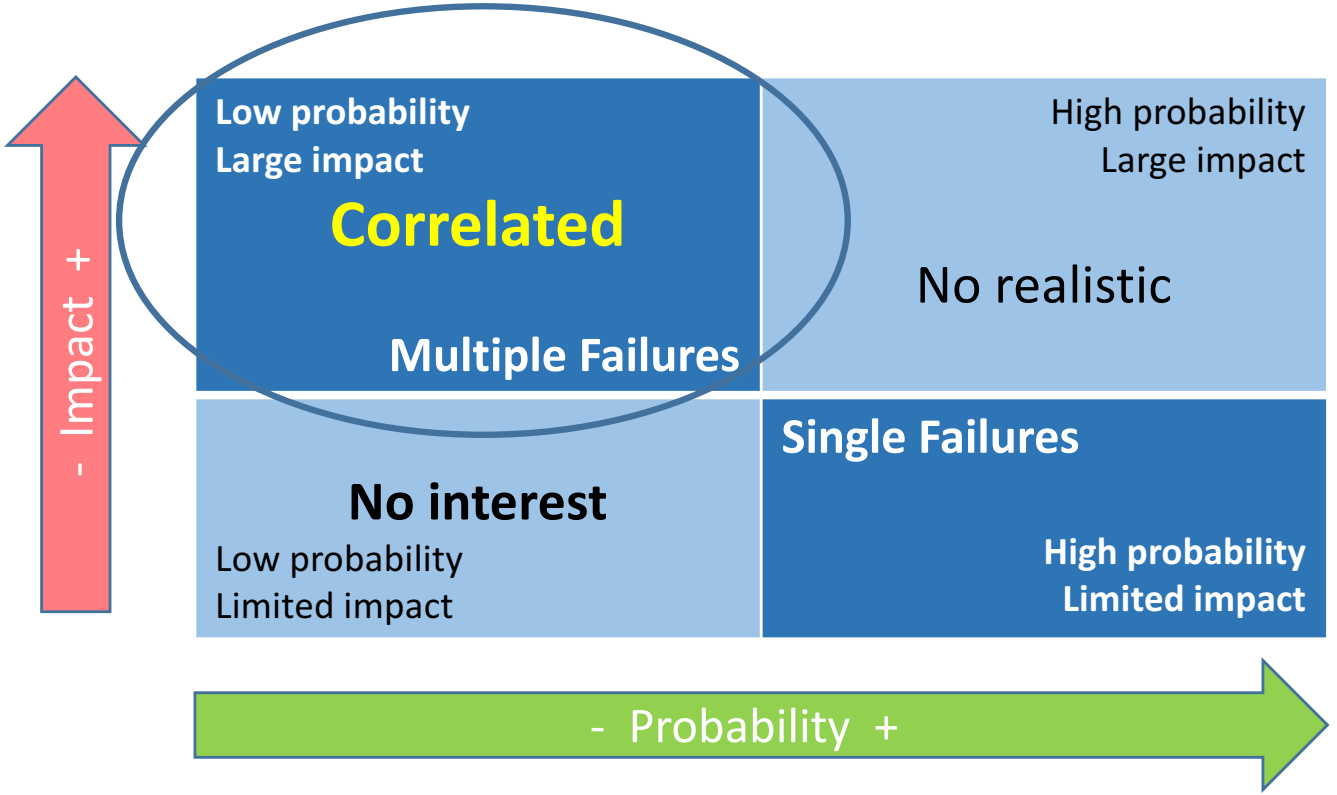
CRITIS 2017

- **Structural**
  (based on classic graph properties)
  - Average nodal degree, Finding paths
  - Connectivity & fragmentation
- **Centrality**
  (it locates the most “important” nodes/links)
  - Degree, Betweenness, Spectral properties, Eigenvectors, …
- **Dynamic/Functional**
  (Considering the expected performance of existing services)
  - Throughput, link occupancy, …

UdG

Kansas State University

Single vs. Multiple failures



Multiple failures happen rarely **but their consequences are too costly**

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

Resilient communication services protecting end-user applications from disaster-based failures (RECODIS)
COST Action **CA15127**

WG4 Malicious human activities

1. **Measures** to evaluate vulnerability of communication networks to malicious human activities
2. Techniques of **network design** / update of characteristics of existing network architectures to improve their resilience against malicious human activities
3. **Algorithms of resilient routing** (and routing metrics) to assure resilience of communication paths to malicious human activities Robustness metrics
4. **Advanced topics** in communication networks resilience under malicious human activities

Modelling multiple failures

Dynamic failures *occur along of time*

- *There is a **cause** that triggers the **propagation** (**correlated** failures)*
- On top of random, there are other **type of "attacks":**
  - *Targeted*
  - *Epidemics*
  - *Cascading*
  - *Others*

Dynamic scenarios: **targeted**

They are normally provoked by malicious attacks (human driven)

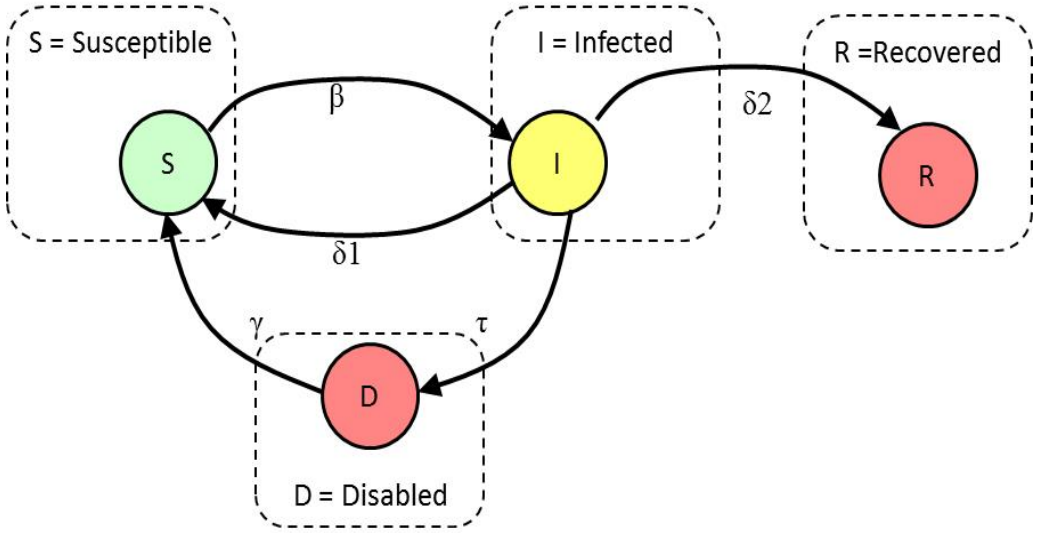
There is a strategy to maximize the impact

Most important nodes/links are attacked first, examples:

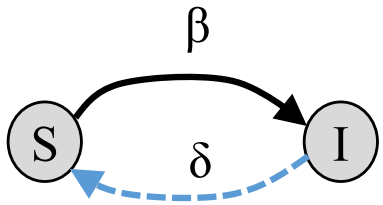
- Nodal degree
- Betweeness
- Other

Dynamic scenarios: **epidemics**

Classical models of contagion define some state (or compartment) for the individuals such as susceptible, infected and infectious (and many more!).

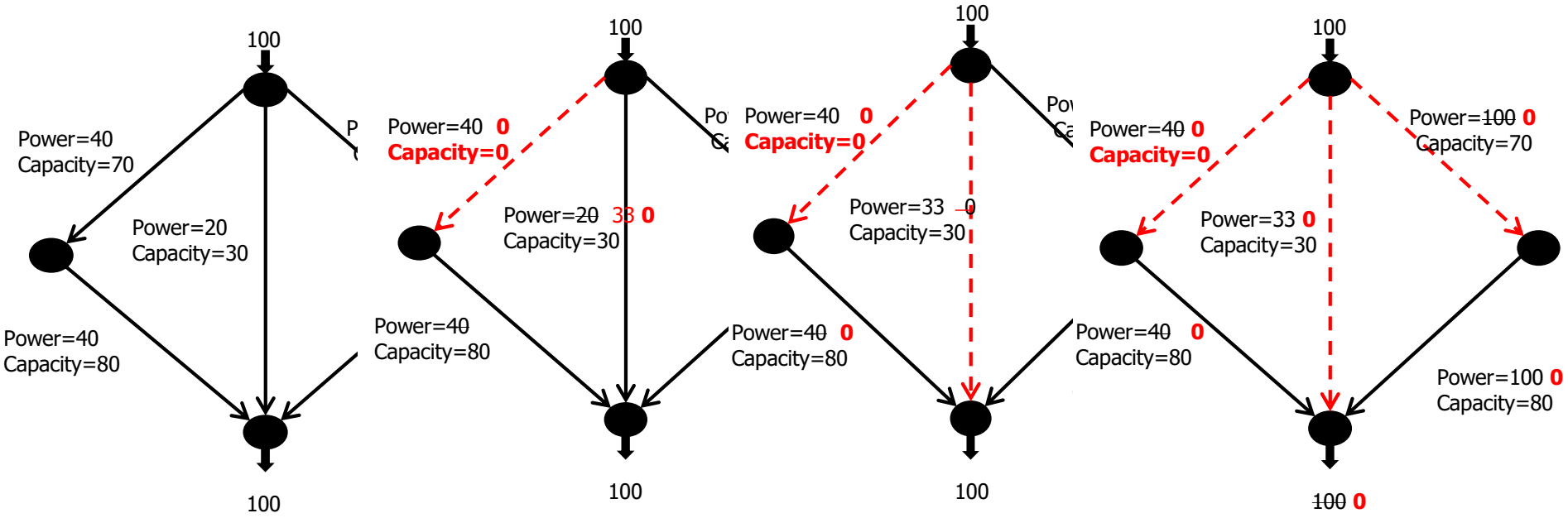


A simplified model is used in our simulator:



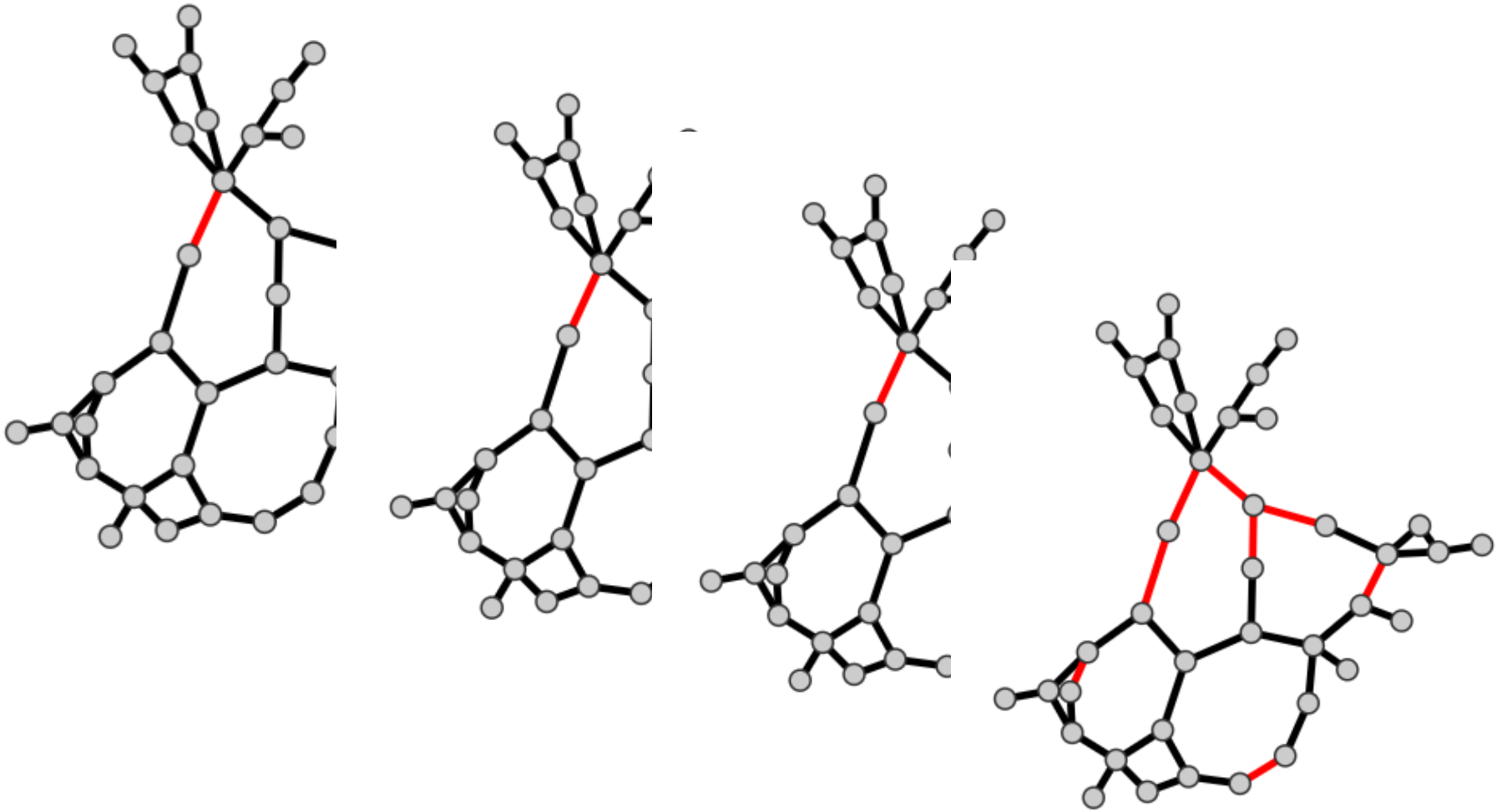
Dynamic scenarios: **cascading**

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



Extra information is needed:
the capacity of the links and the power demands

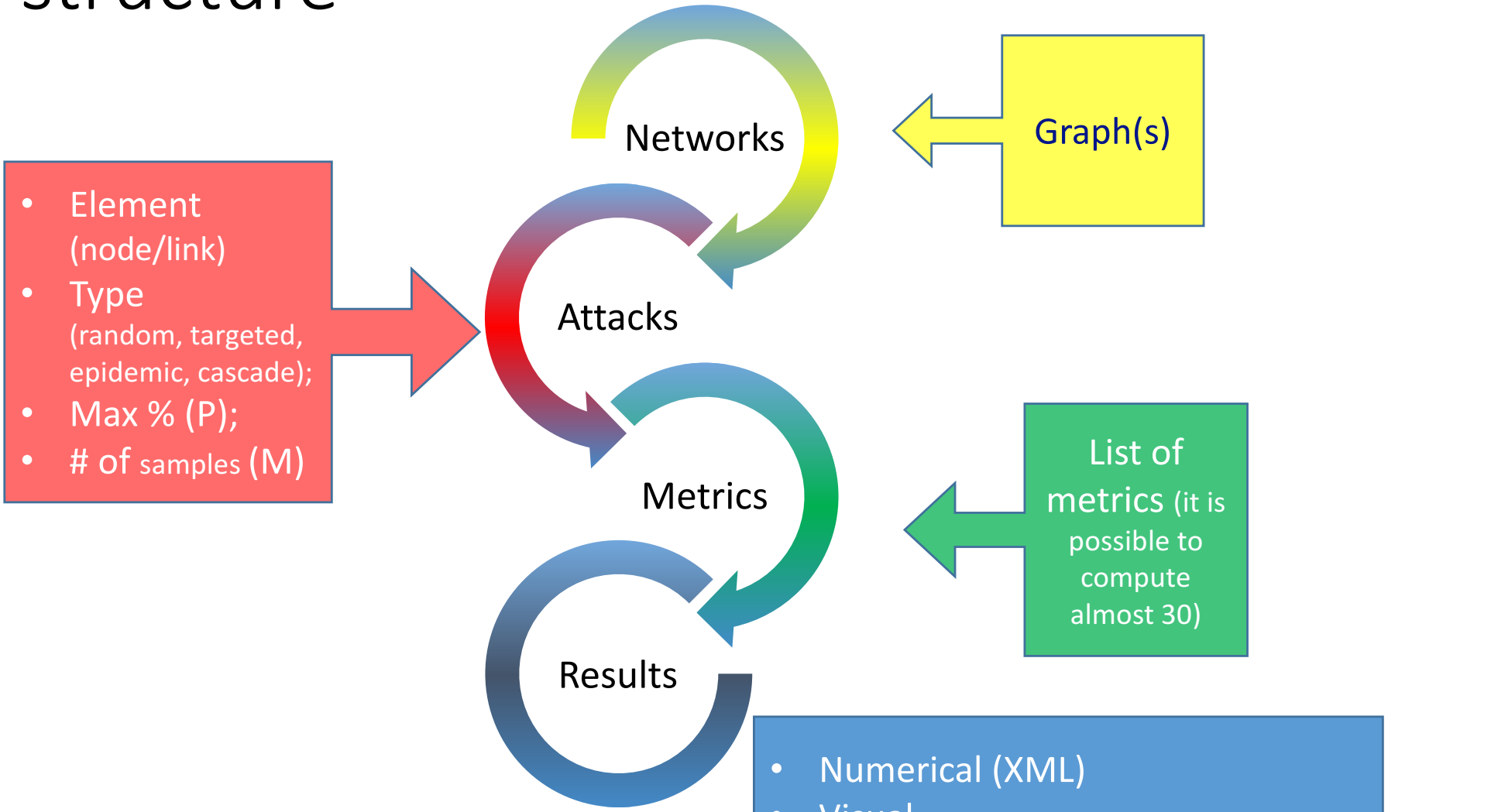
Dynamic scenarios: **cascading**



Contents

- Motivation
- The robustness concept and metrics
- Modelling massive failures
- **Robustness Computation mechanism**
  - **The Network Robustness Simulator (NRS)**
  - **Robustness surface and PCA**
- Simulation Scenario and Results
- Conclusions and future work

Network Robustness Simulator
structure

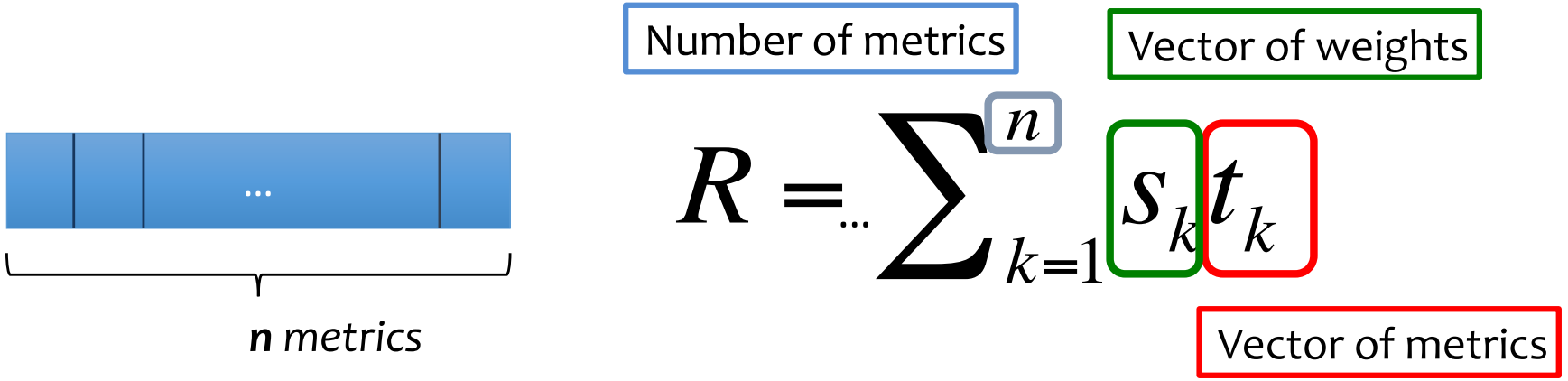


Previous work. The R value

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

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:



where $\boldsymbol{s}$ and $\boldsymbol{t}$ 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,

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

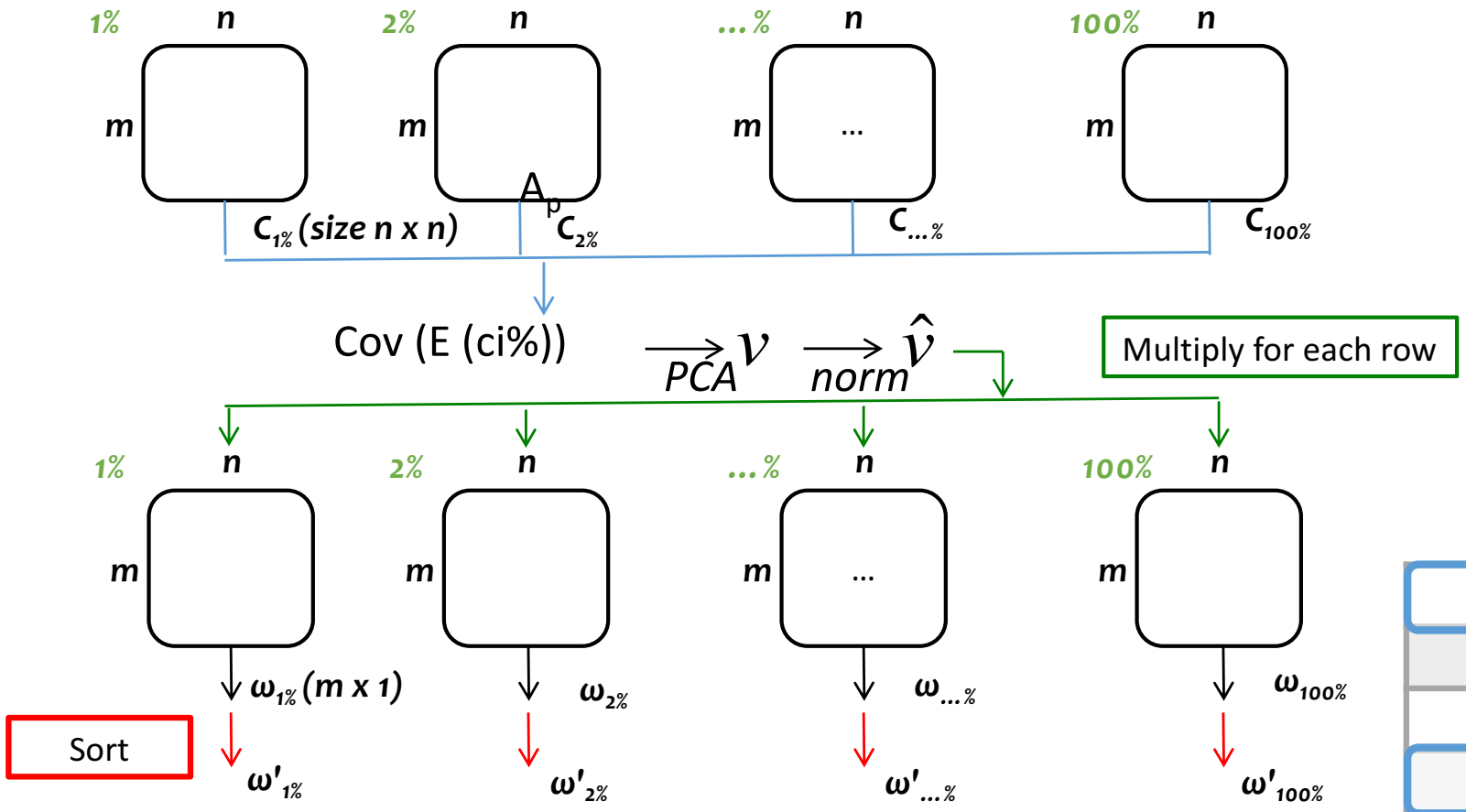
for a **dynamic** scenario we proposed the **R*-value** obtained by extracting the most informative robustness metric from the **n** computed metrics **and normalised**

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

a normalized eigenvector

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

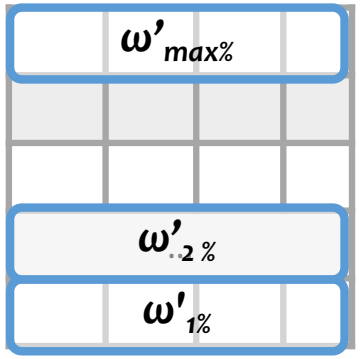
Dynamic approach
0 % to p % , m samples, n metrics



where $\omega_{1\%}=\{R^*_{1\%}, R^*_{1\%,...}, R^*_{1\%}\}$ ...

$\Omega = \{\omega'_{1\%}, \omega'_{2\%,...}, \omega'_{max\%}\}$

Ω matrix

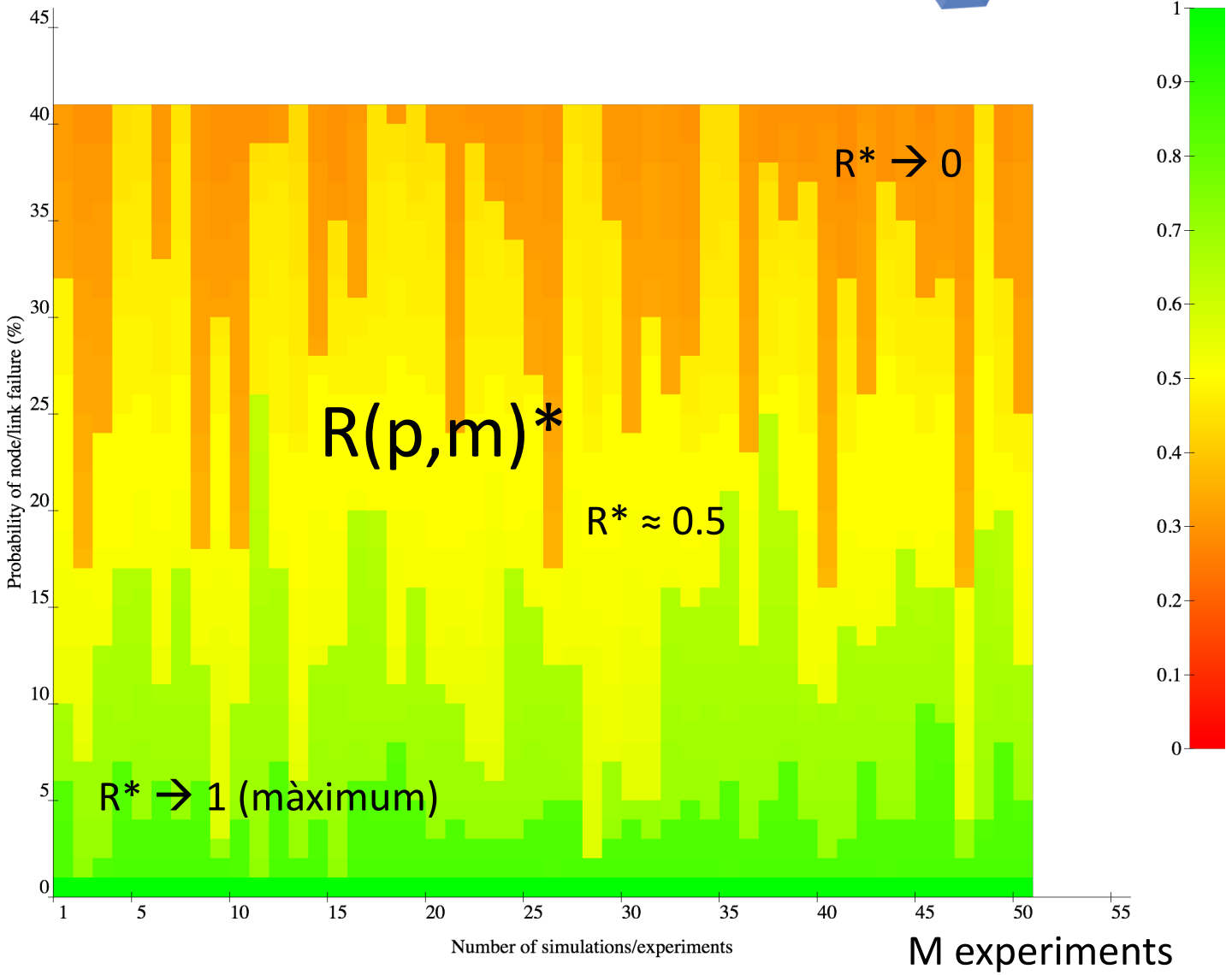


Robustness Surfaces: initial

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

P %

p

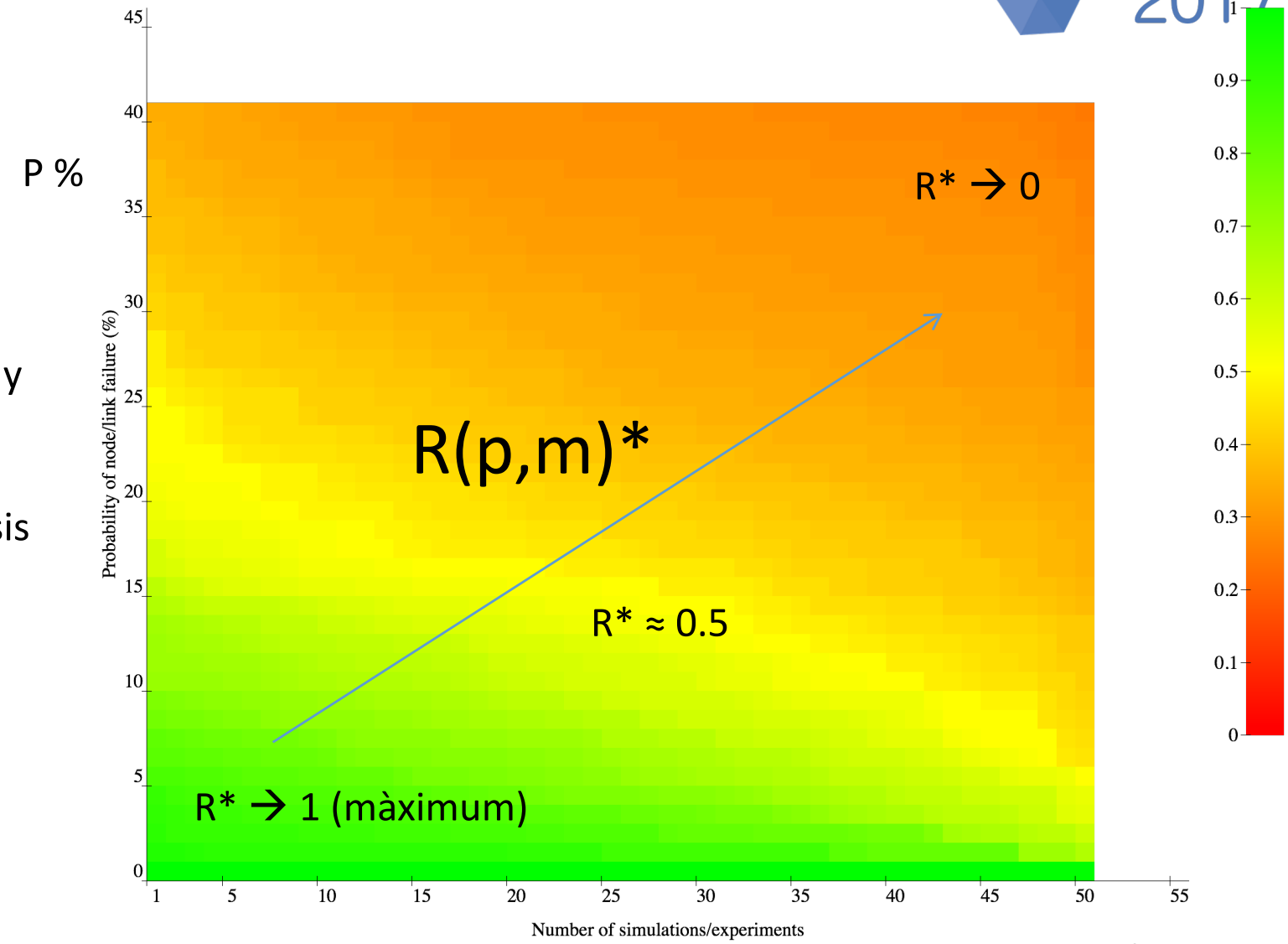


M experiments

m

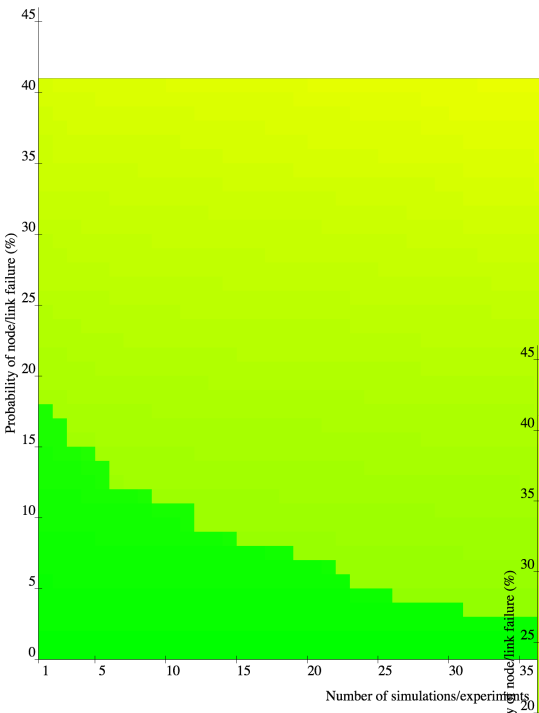
Robustness Surfaces: sorted

- As the results in columns are actually independent rows are sorted for a better **visual** analysis
- Then a Robustness surface is obtained

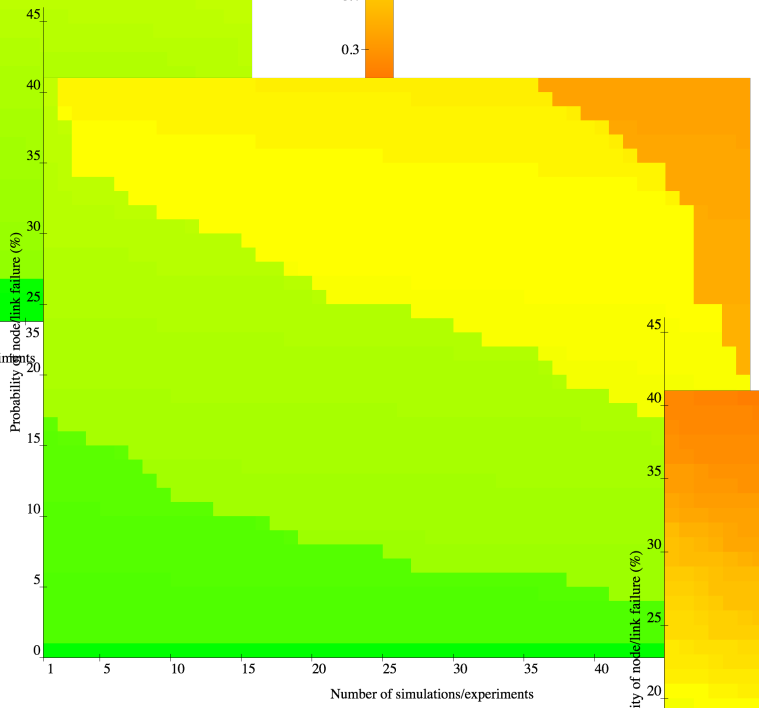


"Robustness surfaces of complex networks", *Manzano, M., Sahneh, F., Scoglio, C., Calle, E., & Marzo, J. L.* Scientific Reports, Nature. September 2014

Some results
Robustness surfaces

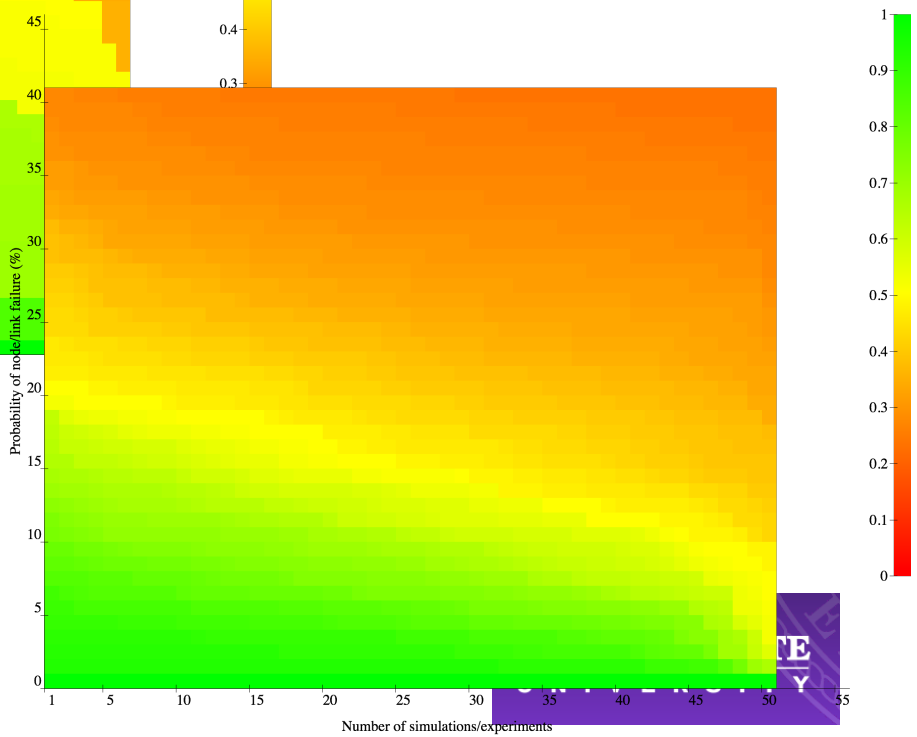


Exponencial



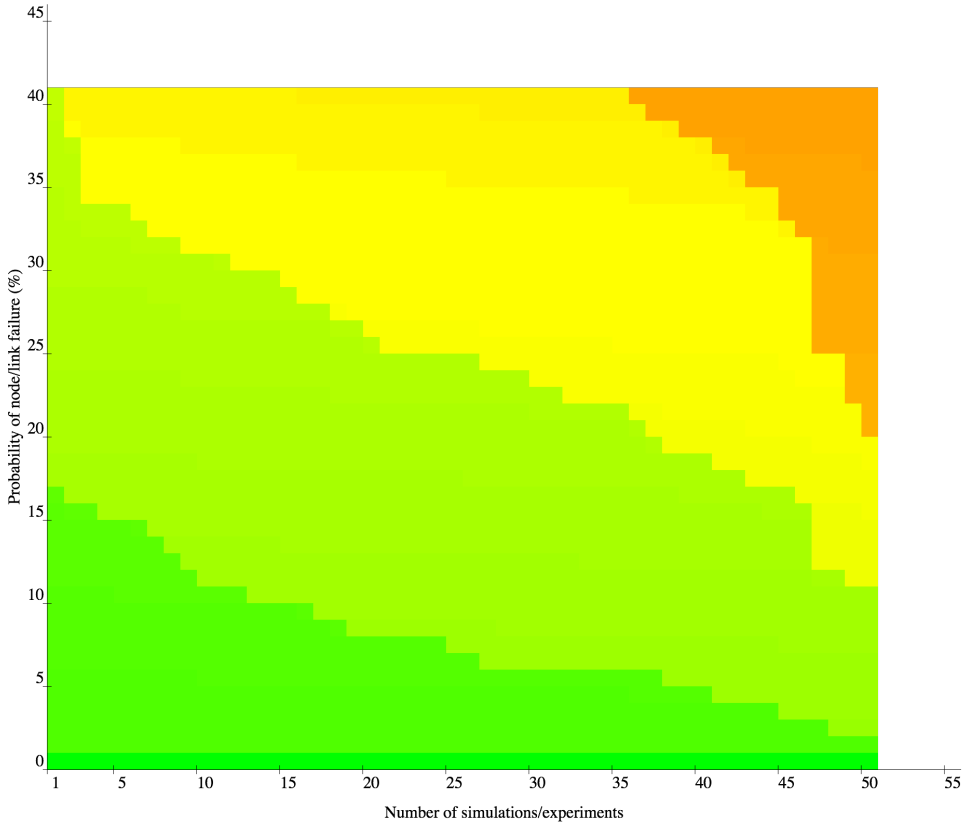
Grid

Random

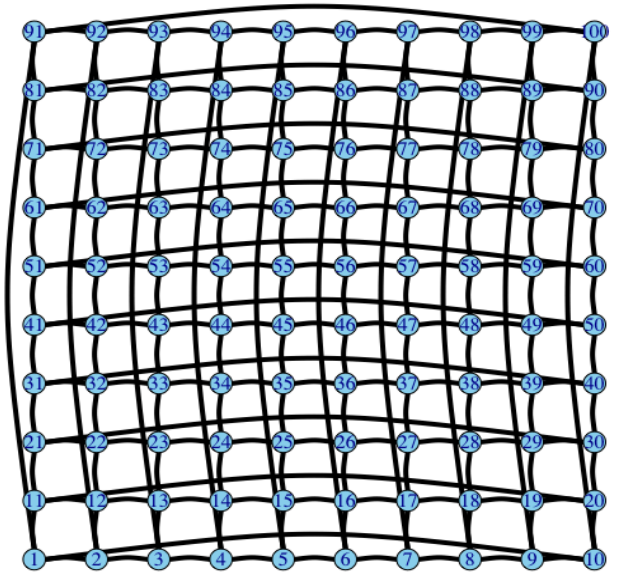


Tree

Random



Grid



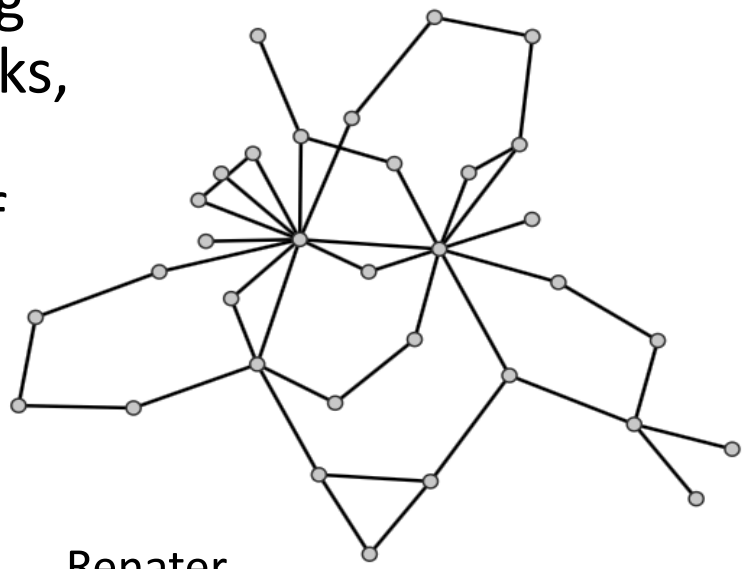
Targeted

Contents

- Motivation
- The robustness concept and metrics
- Modelling massive failures
  - Introducing Epidemic models
- Robustness Computation mechanism
  - The Network Robustness Simulator (NRS)
  - Robustness surface and PCA
- **Simulation Scenario and Results**
- Conclusions

Simulation Scenario

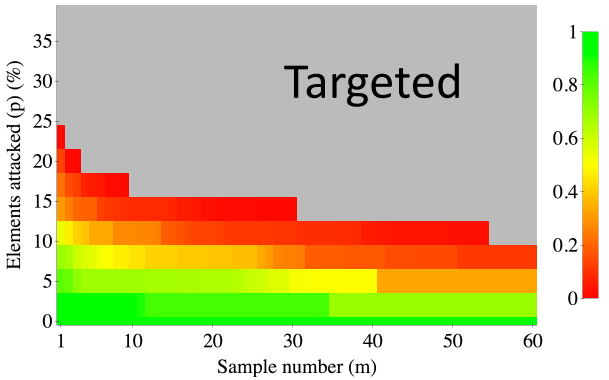
- In general, **targeted** attacks damage the most the networks, followed by random and epidemics (which damage the less).
- Explanation: epidemics always remove a node linked to the previously removed, i.e. epidemics enlarge a single “hole” meanwhile random (and indeed targeted) make independent “holes” (being the impact to the networks more severe).
- When looking for topologies showing better robustness to epidemic attacks, we found out that it was always the case where the topology has a set of connected “hubs”.

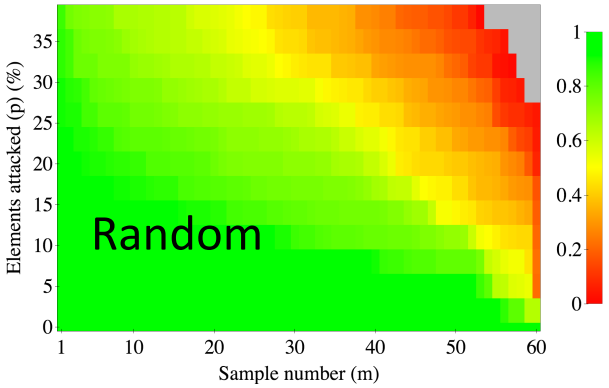


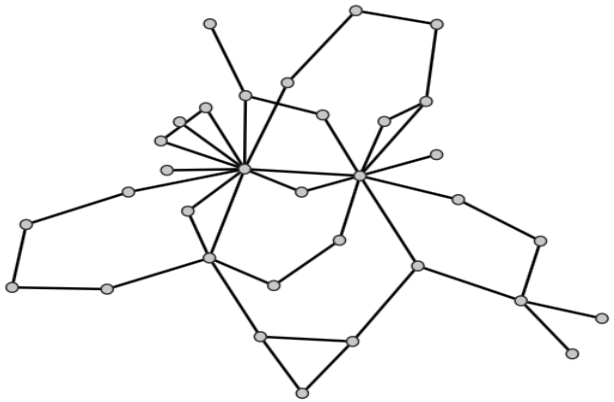
Renater

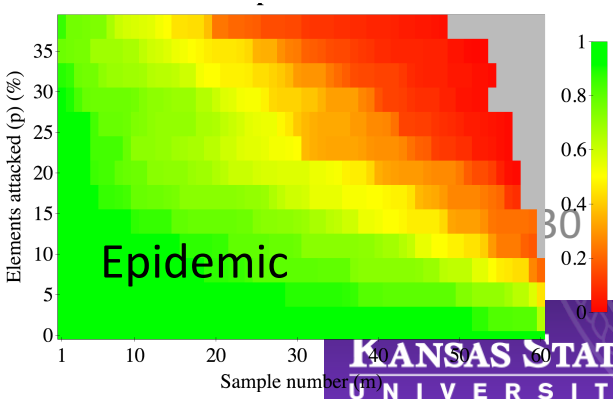
Different attacks to Renater

- The Renater network is selected.
  - It is clearly appreciated two closely interconnected hubs.
  - This structure facilitates de expansion of the epidemic model.
- For **targeted** attacks, the robustness is shaply reduced
  - Above 15% of removed elements gives values of Robustness (R^*) very close to zero
- **Epidemic** gives **smaller** robustness (more red/grey area) average of R^* is 0.55 (0,66 in the case of random)
- The robustness surface of **epidemic** shows **sharper** behavior (clear transitions) due to the fact that when reaching a hub, the damage is higher.



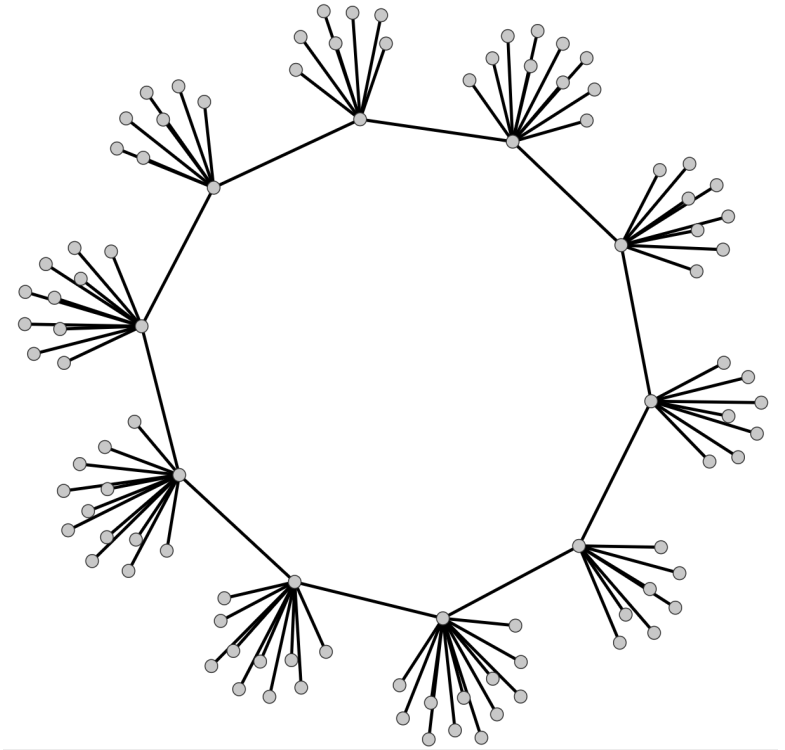






Simulation Scenario (ii)

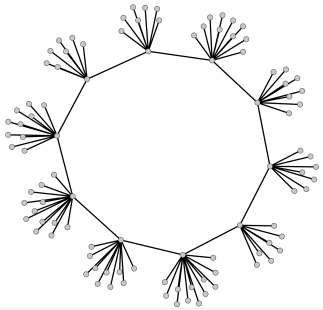
- It was studied the optimal robustness characteristic to random breakdowns for networks.
- These topologies are formed by a small group (proportional to $\sqrt{N}$)
  of well-connected hubs while the remaining nodes ($N-\sqrt{N}$) have degree equal to one (“leafs”)
  - where N is the total number of nodes.

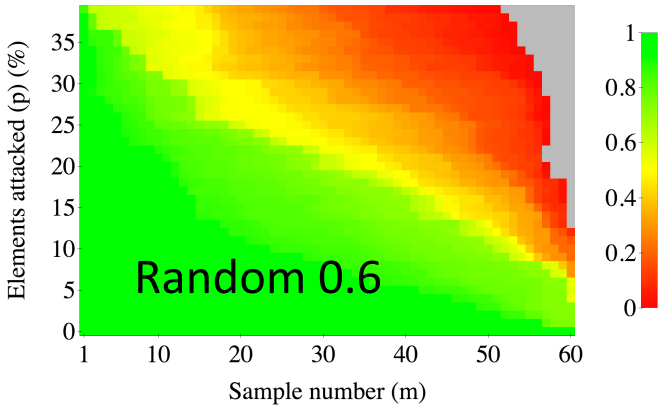


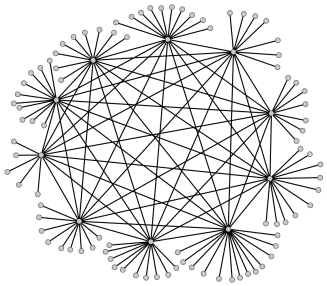
Gerald P, Sameet S, Shlomo ,H. Eugene S. “Optimization of network robustness to random breakdowns”. Physica A: Statistical Mechanics and its Applications, Volume 370, Issue 2. Elsevier. 2006.

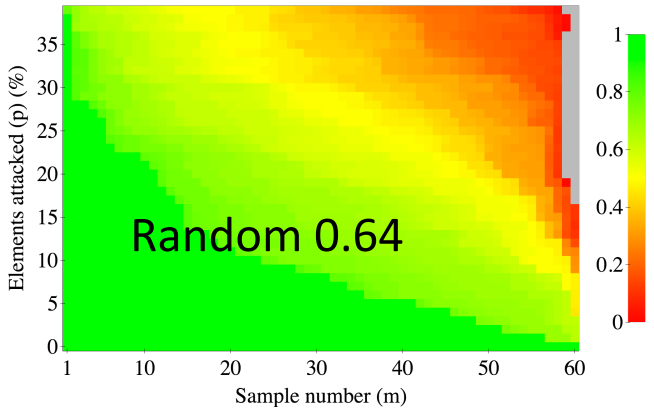
Simulation Scenario

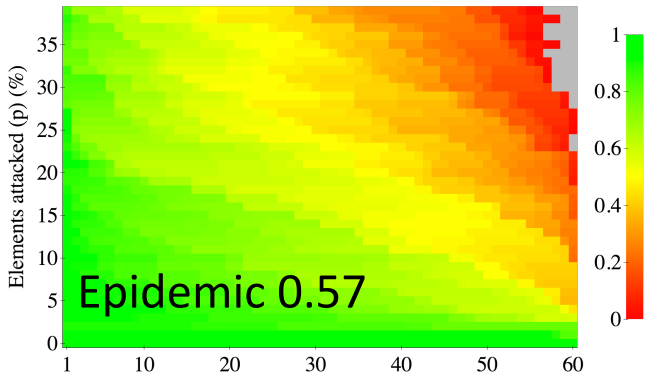
- csadvcsvs

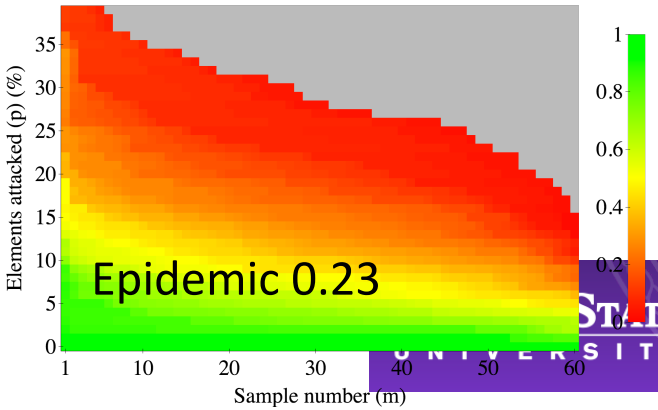












Conclusions

- A complete set of metrics are computed by extending the calculation to different percentage of failures and failure configurations (dynamic scenario)
- Principal Component Analysis (PCA) is used to extract the most significant information of a set of robustness metrics which is used to normalize R-value (obtaining R*-values) therefore the robustness of different networks can be easily analized and compared
- Drawing the robustness surface, a novel framework is provided to visually assess the network robustness variability

Future work

- Expanding the simulator:
  - Adding new metrics, in particular functional ones
  - New attack strategies/models
- Interdependent networks
  - New interdependency models
  - Expanding visualization tool to cope with (at the moment just two networks)
- Working in a new responsive interface for the Network Robustness Simulator
- Current version allows a basic parallelization. As computations are in essence quite independent each other, we think that an study of this factor would increase the speed of calculations increasing scalability.

CRITIS 2017

Thank you!

Acknowledgements:

Dr Eusebi Calle
Dr Caterina Scoglio
Carmen Mas-Machuca
Petra Stojsavljevic
Diego Rueda
Sergio Gómez
Antonio Bueno

EU ACTION COST RECODIS

RECODIS
Resilient communication services protecting end-user applications from disaster-based failures

UdG

KANSAS STATE UNIVERSITY