

A Computational Framework for Network Robustness.

J. Martín Hernández, C. Doerr, P. Van Mieghem¹; Network Architectures and Services (NAS)

Why Network Robustness?

Society depends more strongly than ever on large networks. Can you think of how many networks did you use today? The telephone network, a transportation network to get to this very building, social networks, and certainly the Internet to check your email. Complex types of vulnerability appear in such evolving and decentralized systems that can threaten our daily quality of life. To date, there is not a general framework to evaluate the robustness of all these networks.

Failure classification

Any network perturbation can be classified in one of the following categories:

- 1. Intentional attacks:** *maximum impact*, attacks targeting the most vulnerable part of the network. Or *minimum impact*, attacks targeting secured areas of the network.
- 2. Random failures:** average damage due to equipment dying from aging, operational mistakes, production faults, etc.
- 3. Natural disasters:** correlated attacks confined to a disaster area.

TU Delft has built a computational framework that allows a study of the full spectrum of attacks for any metric used in the field of robustness analysis. The right hand figure shows a case study for the European research network *GEANT* under random failures (red curve) and natural disasters (blue curve). The figure shows the best, worst and average case effect on the network. The size of the colored area quantifies the total amount of different responses possible for the network, thereby giving some measure of uncertainty.

Which links are most vulnerable?

The figure on the right shows the effect of a natural disaster on the *hopcount* of the *GEANT* network. Failures of red coloured links will have the largest impact on the overall network.

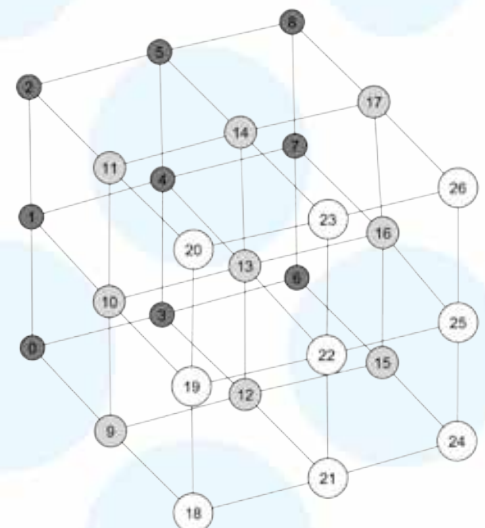
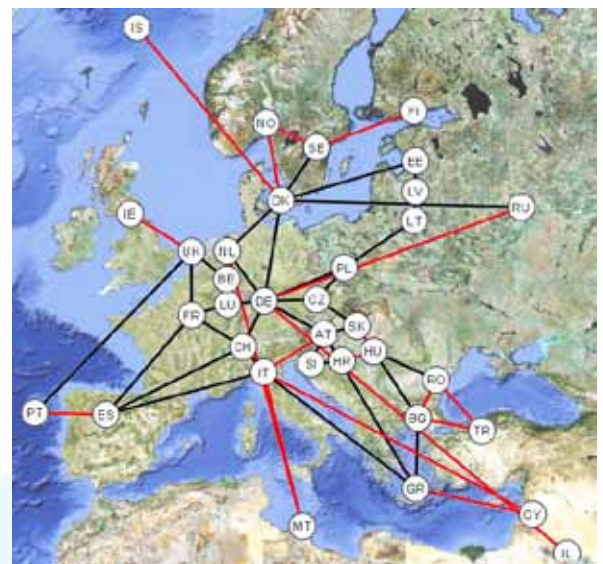
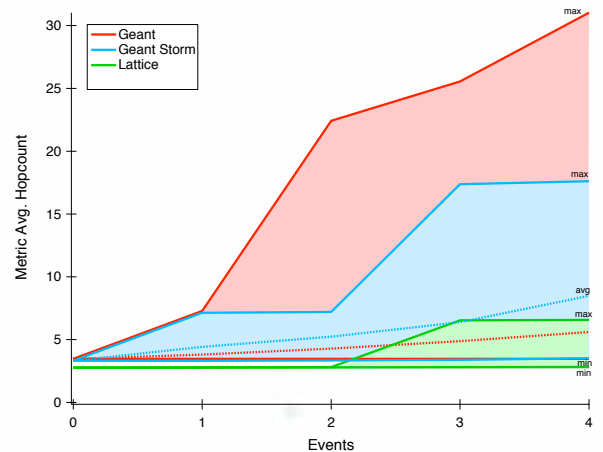
The links in the *GEANT* network have different importance. A network can be highly protected against random failures, but be very vulnerable to natural disasters (or vice versa).

Improving Robustness

The topology of real world networks is subject to several constraints (such as monetary, political and/or geographical), to which network design needs to conform.

The computational framework allows network designers and researchers to explore and optimize the robustness of networks by

- Simulating the network's robustness to a series of "what-if" scenarios and incremental modifications, thereby allowing the weak spots in the network to be consecutively improved,
- Exploring new, alternative topologies that are generally less vulnerable to failures. The generated lattice topology on the right contains a comparable number of links as the *GEANT* network, yet will function much more stable (top figure, green curve) and with less uncertainty than the original topology.



¹Contact us! J. MartinHernandez@tudelft.nl, C.Doerr@tudelft.nl, P.F.A.VanMieghem@tudelft.nl