# SHORT TERM SCIENTIFIC MISSION (STSM) SCIENTIFIC REPORT

**This report is submitted for approval by the STSM applicant to the STSM coordinator**

**Action number: 38866**
**STSM title: Adding effective resistance as attack generation mechanism**
**STSM start and end date: 30/10/2017 to 06/11/2017**
**Grantee name: Sergio Gómez Cosgaya**

## PURPOSE OF THE STSM:
## (max 200 words)

The object of this STSM is to jointly work on robustness quantifications and vulnerability identifications of real-world communication networks. The two main objectives during the visit are:

- Continue with finding of the related STSM performed previously by a researcher from TUDelft visiting UdG hosted by Jose Marzo, integrating theoretical robustness measures from TUDelft in the UdG simulator.

- Adding effective resistance metric from TUDelft as a mechanism to generate targeted attacks to networks selecting the most important nodes depending on their effective resistance, i.e. by computing each metric on every node and selecting those with a larger effective resistance value, generating the desired failure sequence (from most important nodes to less).

During the STSM, possible remaining work from previous STSM by TUDelft researcher would be finished. Therefore, the new attack generation mechanism will be implemented in the UdG simulator and an analysis using real networks is going to be carried out. To accomplish this task, Sergio Gómez (computer engineering master student and researcher in Broadband Communications and Distributed Systems at UdG) would visit TUDelft, hosted by Prof. Piet Van Mieghem.

An analysis of implemented attack generation mechanism compared with other mechanisms as random, targeted or epidemical attack generation is planned.

## DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

(max.500 words)
During the visit in Technical University of Delft from 30 Oct to 11 Nov, the STSM is carried out in the following steps:

- **Meeting for redefining working plan during STSM:**
  In this meeting with the host institution senior member and researchers it was decided to slightly modify workplan because of these reasons:
  1. Effective resistance metric (zeta vector attack mechanism) was integrated in previous STSM (action number 38792) carried by TUDelft researcher. Instead, other type of targeted attack strategies were planned to be introduced.
  2. TUDelft senior member proposed focusing on performing modifications in the UdG simulator to get a set of final experiment results.

Funded by the Horizon 2020 Framework Programme

- **UdG simulator introduction:**
  A brief explanation about UdG features has been done to TUDelft researches in order to make them capable to use it. Also access was given to them and a joinly *workspace* was created for computing shared experiments between both research goups.

- **UdG simulator modifications:**
  1. Adding other attack generation mechanisms:
     The first step was to add attack mechanisms based on nodal degree, closeness centrality and eigenvector centrality to the previous existing mechanisms in simulator (e.g. random, epidemic, betweenness based, etc.).
  2. Adding the deterministic set of *best attack sequence* (i.e. targeted attackts according to the best metric value (e.g. with higher nodal degree)) instead of using different attack sequences [1] generated using a probabilistic function depending on metric values to select elements.
  3. Adding the feature to upload multiple networks at once to the simulator. This feature is needed for the future STSM carried by another TUDelft researcher in Girona in which several real networks will be used.
  4. Experiment summary creation:
     An experiment is defined as a set of simulations using multiple networks, attack mechanisms and metrics. All combinations of networks and attack mechanisms will result in a single simulation. Therefore using 10 networks and 5 different attack mechanisms will result in a experiment with 50 simulations. Before this STSM, there was only an Excel file for each simulation, hence it was decided to generate an another Excel file as a summary for the whole experiment, where all attack mechanisms are compared and ranked from better to worst using an histogram. The histogram shows, for example, which mechanisms appears more times as the best ranked (i.e. it is the best strategy).

- **Final meeting:**
  During last STSM day, we meet again in order to show resulting work done and to identify next steps and future collaborations.

## DESCRIPTION OF THE MAIN RESULTS OBTAINED

(max.500 words)

In order to show resulting work done during the STSM, different kind of results output is provided:

- Adding networks:
  Simulator is now able to upload multiple networks. A visualization of a network can be seen in figure 1. The network visualized is *cost266*, which is a network available in SNDLib[1] and it is the nework used in next point.

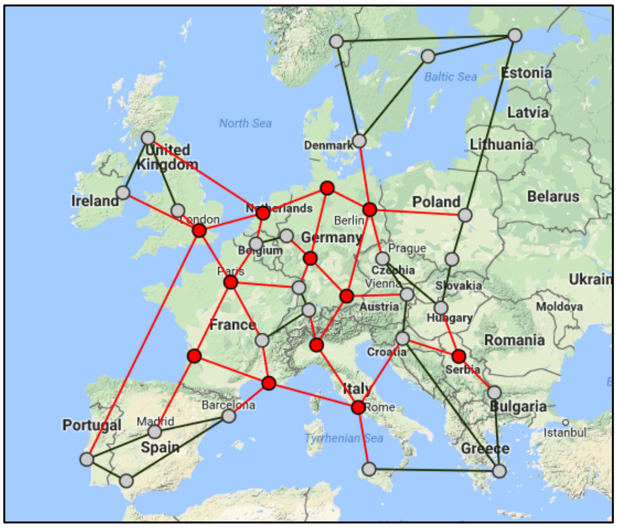


Figure 1: *Cost266 network visualization over a map.*
*Red nodes represent removed nodes (in this case the 30% of nodes).*

[1] SNDLib webpage: http://sndlib.zib.de/home.action

- Computing added attack mechanisms:
  Figure 2 shows the robustness surface[2] when using two different mechanisms against *cost266* network. At left random attack mechanisms and at right a betwenness-based targeted mechanism is used. It can be seen that betweenness targeted mechanism is more powerfull than random attacks (i.e. network is more damaged).

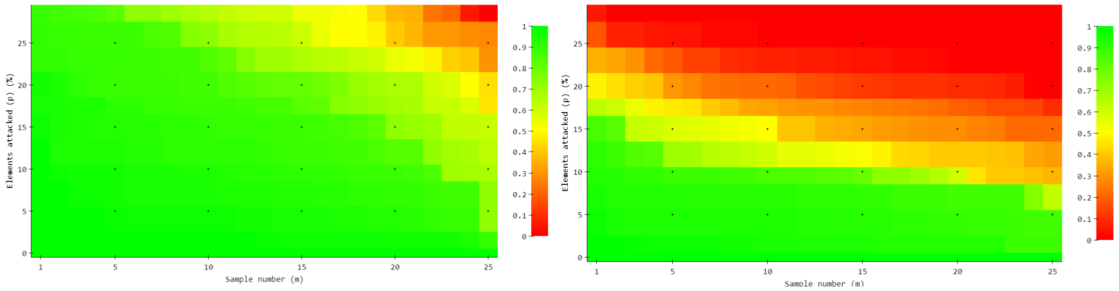


Figure 2: *Random (left) and betweennes based (right) mechanisms robustness surface against cost266 network from 0% to 30% of elements attacked.*

Figure 3 shows a comparison between all available attack mechanisms in simulator (random, epidemic, betweenness based targeted, nodal degree based targeted, closeness based targeted, eigenvector centrality based targeted and zeta vector based targeted) behavior in *cost266* network. X axis represents the number of elements attacked from left (0 elements) to right (30% of elements) and Y axis represents robustness value from bottom (0, not robust) to top (1, robust and not damaged).

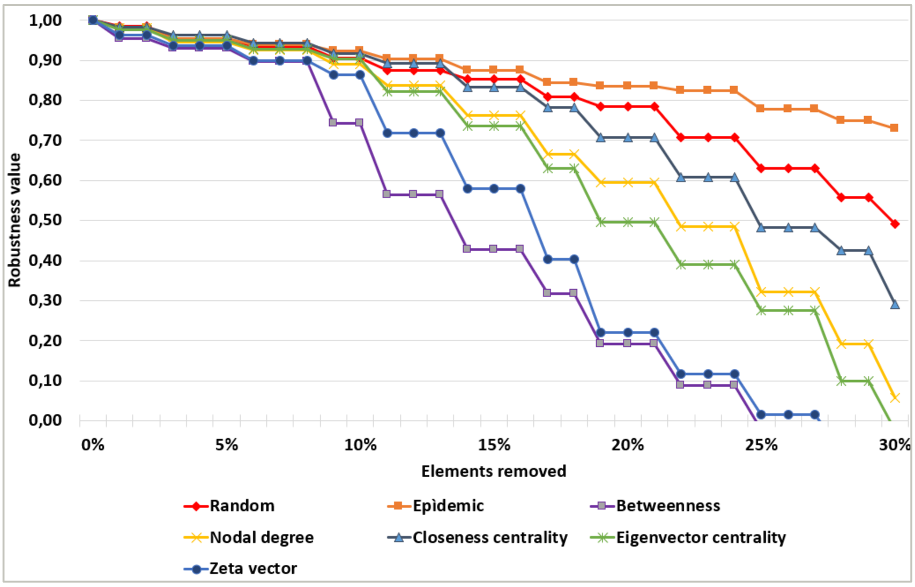
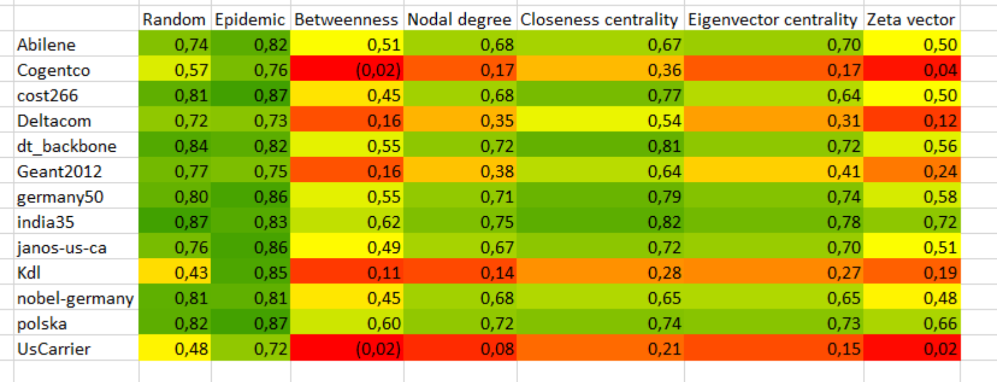


Figure 3: *Attack mechanisms comparison against cost266 network.*

It can be observed that in this case betweenness and zeta vector based targeted attacks are the most damage attack mechanisms and that, for instance, epidemic mechanisms damage the network less.

- Generating whole experiment summary:
  In order to show an example of an experiment summary, 13 different networks and all available attack mechanisms has been computed removing up to 30% of network elements. Figure 4 shows an screenshot of the summary first Excel page where the final robustness value for each simulation is written. In the table can be seen how each network is affected by the different attack mechanisms (e.g. *UsCarrier* is less robust than *germany50* againts these attacks) and how each strategy affectsnetworks similar to figure 3 but also comparing with all simulations (figure 3 only shows comparison in a unique simulation or network). Again, epidemic strategy makes the less damage and betweenness and zeta vector based strategies seems like to be the most powerful ones.

[2] Robustness surface is a heatmap where X axis represents different kind of generated attack sequences and Y axis represents the amount of elements removed (from bottom as no elements removed to top as a percentage of elementes removed). Green color represents network is not damaged and red color represents network is very damage.



| | Random | Epidemic | Betweenness | Nodal degree | Closeness centrality | Eigenvector centrality | Zeta vector |
|---|---|---|---|---|---|---|---|
| Abilene | 0,74 | 0,82 | 0,51 | 0,68 | 0,67 | 0,70 | 0,50 |
| Cogentco | 0,57 | 0,76 | (0,02) | 0,17 | 0,36 | 0,17 | 0,04 |
| cost266 | 0,81 | 0,87 | 0,45 | 0,68 | 0,77 | 0,64 | 0,50 |
| Deltacom | 0,72 | 0,73 | 0,16 | 0,35 | 0,54 | 0,31 | 0,12 |
| dt_backbone | 0,84 | 0,82 | 0,55 | 0,72 | 0,81 | 0,72 | 0,56 |
| Geant2012 | 0,77 | 0,75 | 0,16 | 0,38 | 0,64 | 0,41 | 0,24 |
| germany50 | 0,80 | 0,86 | 0,55 | 0,71 | 0,79 | 0,74 | 0,58 |
| india35 | 0,87 | 0,83 | 0,62 | 0,75 | 0,82 | 0,78 | 0,72 |
| janos-us-ca | 0,76 | 0,86 | 0,49 | 0,67 | 0,72 | 0,70 | 0,51 |
| Kdl | 0,43 | 0,85 | 0,11 | 0,14 | 0,28 | 0,27 | 0,19 |
| nobel-germany | 0,81 | 0,81 | 0,45 | 0,68 | 0,65 | 0,65 | 0,48 |
| polska | 0,82 | 0,87 | 0,60 | 0,72 | 0,74 | 0,73 | 0,66 |
| UsCarrier | 0,48 | 0,72 | (0,02) | 0,08 | 0,21 | 0,15 | 0,02 |

Figure 4: *First page of experiment summary example.*

Finally, figure 5 shows the histogram created in the second page of the Excel summary where X axis represents the mechanism rank (from left (best ranked) to right (worst ranked)) and Y axis represents the number of times that each attack mechanism has that rank number. It can be seen that betweenness is the mechanism that appear as best ranked the most.

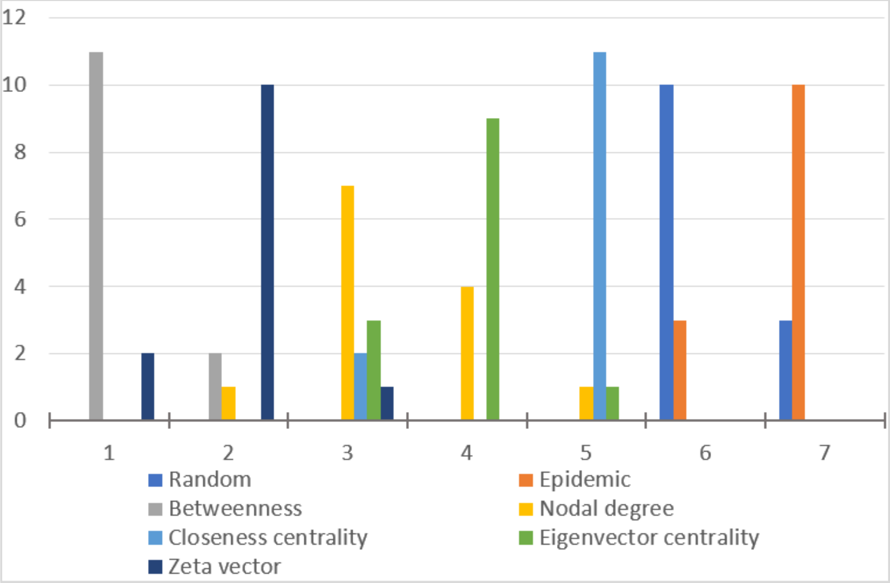


Figure 5: *Experiment summary histogram.*

## FUTURE COLLABORATIONS

Next step in collaboration between UdG and TUDelft is to add a huge number of real networks in the simulator. These networks should be grouped by their meaning (i.e. grouping metro networks, internet networks, etc.). This step is going to be done in a STSM in January 2018 performed by a TUDelft researcher in Girona.

References:

1. Marzo, J. L., Cosgaya, S. G., & Scoglio, C. (2017, September). Network robustness simulator: A case study on epidemic models. In Resilient Networks Design and Modeling (RNDM), 2017 9th International Workshop on (pp. 1-6). IEEE.
2. Klein, Douglas J., and Milan Randić, 1993, "Resistance distance." Journal of mathematical chemistry 12.1: 81-95.
3. Latora, Vito, and Massimo Marchiori, 2007, "A measure of centrality based on network efficiency." New Journal of Physics 9.6:188.
4. Van Mieghem, P., K. Devriendt and H. Cetinay, 2017, "Pseudo-inverse of the Laplacian and best spreader node in a network", Physical Review E, vol. 96, No. 3, p 032311.
5. Wang, X. , J. L. A. Dubbeldam and P. Van Mieghem, 2017, "Kemeny's constant and the effective graph resistance", Linear Algebra and its Applications, vol. 535, pp 231-244.
6. UdG simulator: http://infraiiia01.udg.edu