SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

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

COST Action: CA15127
STSM reference number: 39242
STSM title: Assessing the robustness and critical nodes of real networks
STSM start and end date: 14/01/2018 – 20/01/2018
Grantee name: Hale Cetinay Iyicil

PURPOSE OF THE STSM:
(max 200 words)

The object of this STSM is to jointly work on the analyses of robustness and vulnerability of real-world networks. Three main objectives during the visit to the host are:

- Integrating the selected set of real world networks' data in the UdG simulator,

- Investigating the robustness of real world networks after a targeted-node-removal using both the traditional metrics (such as betweenness and degree centrality) and the recently proposed graph metrics (such as the ranked diagonal elements of the pseudoinverse of the Laplacian (zeta metric [1])),
- Comparing and ranking the node-removal strategies in the selected set of real world networks' data.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS
(max.500 words)

During the visit between 14 January and 20 January to the University of Girona, the STSM is carried out in the following steps:

(1) Determining the set of metrics to use as 'destructive strategies'

Centrality metrics can identify which elements in a network are important or central [2]. We investigate how fast the robustness (R-value) changes when we gradually remove a node in the network according to the traditional centrality metrics: (1) Nodal degree (2) Betweenness (3) Closeness (4) Principal adjacency eigenvector component, and recently proposed spreader metrics (5) Diagonal element of the pseudo-Laplacian (zeta vector)[1]. Additionally, we have included (6) random attack mechanism in order to compare the effects of targeted attacks and random attacks.

[1] [1] propose the zeta vector $\zeta = (Q_{11}^{\dagger},\ Q_{22}^{\dagger}, \dots ,\ Q_{NN}^{\dagger})$, which is the diagonal elements of the pseudo-inverse $Q^{\dagger}$ of the Laplacian matrix of a graph, as the nodal spreader list. The node with a minimum value of $Q_{ii}^{\dagger}$ is regarded as the best spreader node.

(2) Determining the set of metrics to assess the overall robustness R-value

With the expertise of the host university in the telecommunication networks and using the reference [2], which provides an overview about the robustness metrics in real-world networks, it is decided that the R-value includes the convex combination of the following structural robustness, centrality measures and functional robustness metrics:

- Average nodal degree: Networks with higher average nodal degree are considered better connected on average and are likely to be more robust.
- Effective graph resistance is related with the number of paths between two nodes and their length. The smaller the effectice graph resistance value is, the more robust the network
- Largest connected component and Fractional size largest component are the measures to compare the sizes of the largest connected component after the attacks to the original graph.
- Average two terminal reliability gives an indication of the probability of connectivity between a randomly chosen node pair. The higher the average two-terminal reliability is, the higher the robustness is.
- Degree of fragmentation is related with the total number of connected components when the network is partitioned by node removals.
- Algebraic connectivity measures how difficult it is to break the network. Higher values indicate better robustness.
- Node betweenness centrality, and Eigenvector centrality define the graph level centralization index, by calculating the sum of the deviation from the maximum centrality scores.

(3) Integrating the set of real networks to the UdG simulator

With the host university, we focused on 3 subset of real-world infrastructures that are vital for the society: telecommunication networks, power grids and metro networks:

- For telecommunication networks: Reference [2] is used and 10 different networks are included in the simulator. The network size varies from N=11 to N=754 (where N is the number of nodes in the underlying graph).
- For power grids networks: The public data for the power grids is limited. Therefore, in this part, first the real-world like test data topologies from IEEE [4] is used. In addition, the topologies of 3 European countries, as their form found online [5], is included into the simulator. Their sizes varies from N=35 to N=231.
- Finally, 33 metro network topologies are included to the UdG simulator. The networks are from different countries and in different sizes varying from N=5 to N=83. More details on the networks can be found in [6] and [7].

(4) Analyzing and comparing destructive strategies in telecommunication, electric power, and metro networks

After deciding on the destructive strategies, the robustness metrics to include in the computation of R value, and the real-world networks; the final steps are the analyses of the network robustness after attacking nodes sequentially and observing the effects on the robustness value. The results of this part will be discussed in detail in the following part of the report.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

(max.500 words)

By sequentially removing network nodes according to the selected strategies, we measure the impact of these removals on the final R-value (The R-value is normalized between 0 and 1: 0 indicates the 'worst' robustness, whereas the maximum value 1 means a 'fully' robust network.).

(1) The effect of destructive strategies on R-value in real-world networks

Each attack strategy is simulated and their effects on the R-value are observed in 3 real world infrastructures. Table 1 presents the final R-value of the network after attacking the 25% of the nodes in the underlying graphs of the telecommunication networks. We observe that the *Cesnet201006* network is particularly vulnerable to targeted attacks. The removal of the 25% of initial network nodes according to betweenness centrality nearly zeroes the R value at the end of the attacks. Out of those 10 networks, *Abilene* is the most robust network to the targeted attacks.

Table 1 . Final R-value after the random and targeted attacks in telecommunication networks

	Random	Betweenness centrality	Nodal degree	Closeness centrality	Eigenvector centrality	Zeta vector
Abilene	0.72	0.54	0.67	0.68	0.69	0.55
Cesnet201006	0.72	(0.00)	0.03	0.52	0.12	0.03
Cogentco	0.67	0.20	0.38	0.53	0.37	0.24
Deltacom	0.74	0.31	0.47	0.65	0.49	0.33
Garr201201	0.68	(0.02)	0.08	0.60	0.15	(0.01)
Geant2012	0.78	0.34	0.49	0.71	0.55	0.41
GpENI_L2	0.65	0.05	0.14	0.52	0.19	0.05
Kdl	0.59	0.26	0.33	0.47	0.45	0.33
Renater2010	0.77	0.25	0.39	0.61	0.35	0.29
UsCarrier	0.62	0.21	0.35	0.41	0.33	0.22

(2) Comparing destructive strategies in real-world networks

After observing the effect of the attacks in each network from different infrastructures, the next step is to compare the destructive strategies. To present our results, we group the networks according to their infrastructure (i.e., telecommunication, power grids and metro networks) and in Figure 1, Figure 2 and Figure 3 we present the comparison of the destructive strategies, respectively for telecommunication, power grids and metro networks. In those following figures, X axis represents ranking of the destructive strategy (from left (1: best ranked) to right (6worst ranked)) and Y axis represents the total number of times that each destructive strategy has that rank number.

From the attack strategies, betweenness centrality and zeta vector seem the most powerful ones to destroy the network. For instance, in Figure 1, Betweenness has been ranked as the 'best' destructive strategy in 9 networks out of 10 telecommunucation networks. Similarly, in Figure 3, we see Zeta vector has been ranked as the 'second best' destructive strategy in 27 out of 33 metro networks.

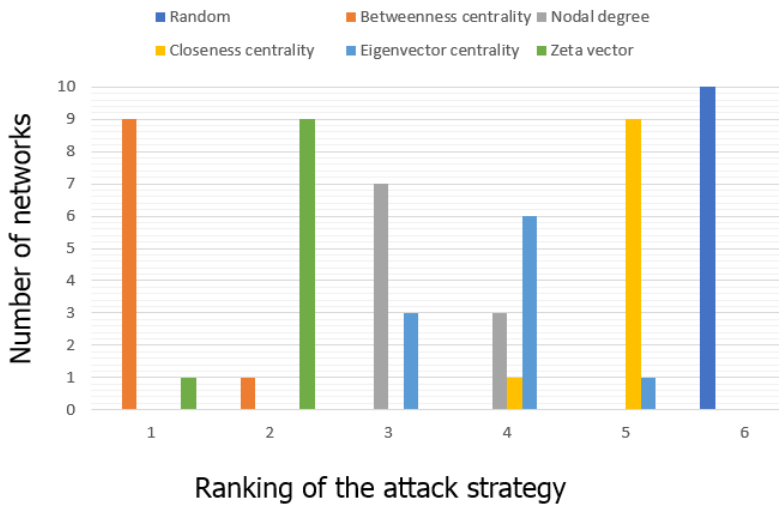

Figure 1. Histogram of the ranking of different attack strategies in telecommunication networks

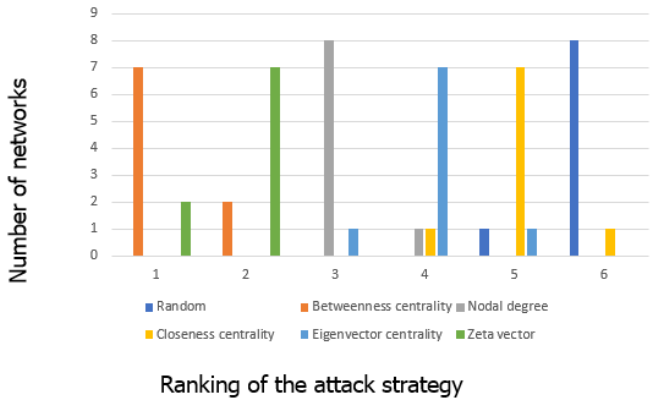

Figure 2 Histogram of the ranking of different attack strategies in power grids

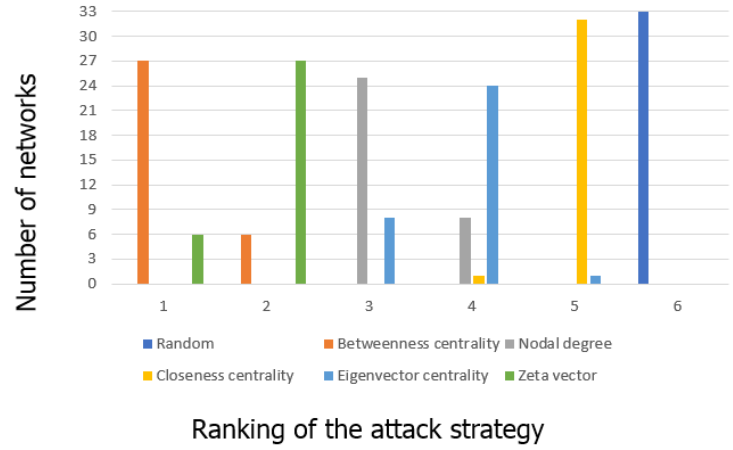

Figure 3 Histogram of the ranking of different attack strategies in metro networks

In nearly all of the tested networks from three different infrastructures, a node removal strategy according to the betweenness centrality value has been found the most effective. The betweenness is followed by the zeta vector, which seems also a powerful way to decrease the overall robustness value of the network. The worst method to destroy the networks is always the random attack, which is expected in the real-world network infrastructures.

FUTURE COLLABORATIONS (if applicable)

The UdG simulator can efficiently analyse different infrastructures and compare different attack scenarios. The future collaboration aims to integrate more accurate real-world infrastructures with also incorporating the geographical coordinates.

References:

1. Van Mieghem, P., K. Devriendt and H. Cetinay, 2017, "Pseudoinverse of the Laplacian and best spreader node in a network", Physical Review E, vol. 96, No. 3, p 032311.
2. Rueda, Diego F., Eusebi Calle, and Jose L. Marzo. "Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements." *Journal of Network and Systems Management* 25.2 (2017): 269-289.
3. UdG simulator: http://songohan.udg.edu
4. Power Systems Test Case Archive: https://www2.ee.washington.edu/research/pstca/
5. Power grids data set. https://wiki.openmod-initiative.org/wiki/Transmission_network_datasets#Europe
6. Wang, Xiangrong, et al. "Multi-criteria robustness analysis of metro networks." Physica A: Statistical Mechanics and its Applications 474 (2017): 19-31.
7. Derrible, Sybil, and Christopher Kennedy. "The complexity and robustness of metro networks." Physica A: Statistical Mechanics and its Applications 389.17 (2010): 3678-3691.