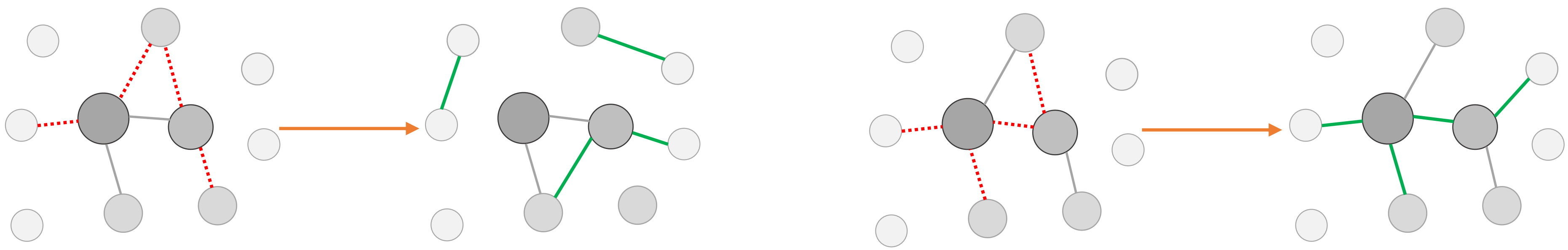
Topological **Fragility** versus **Antifragility**: Understanding the Impact of Real-time Repairs in Networks Under Targeted Attacks



Alexandru Topîrceanu and Mihai Udrescu

ACSA Research Lab
Department of Computer and Information Technology
Politehnica University Timisoara

Barcelona, August 2018

Agenda

Motivation of study, considering literature on:

- Robustness of complex networks
- Node & edge attacks
- Node & edge repairs

➢ Our proposed edge attack-repair mechanism

➢ Strategies for attack & repair

➢ Quantifying network fragility

➢ Analysis of attack-repair rates

➢ Topological antifragility

Motivation

Fragility = inability to withstand damage without loosing functionality [Albert, 2000] (represented by removed nodes or destroyed links)

Antifragility = gain strength under stress (*i.e.*, more than robustness) [Taleb, 2012].

Fragility is an important concept because [Albert, Barabasi, Newman, Vespignani]:

- Network dynamics are highly dependent on the topological structure (interactions between nodes): *e.g.*, spreading of opinion, disease outbreaks, cybernetic attacks, gene interactions, or trade patterns.
- Topology is dynamic, being influenced by natural growth, external attacks, and by the responses to such attacks.

State of the Art

Network repairing strategies are a relatively new research topic.

Node repairs:

- Global (Deg, Btw, KShell) versus local (Btw, Cls) repairs in the context of transportation optimizations [Sun, 2017].
- Shell repair strategy for node failures in energy transfer networks [Fu, 2017].
- Random versus preferential repairs on localized attacks [Hu, 2016].

Edge repairs:

- Edge deletion/addition based on optimizing the leading eigenvalue that controls the information dissemination [Tong, 2012].

Motivation of this study

1. Few studies on network repair strategies
2. Few studies on edge manipulation

➔ We propose an edge attack-repair mechanism and offer insights regarding:

- Study impact of centralities in attack efficiency
- Study 3 different repair strategies
- Compare synthetic and real-world topologies

The edge **attack** mechanism

We run 100 attack-repair iterations / simulation on $G = (N, E)$.

- Each iteration consists of removing **α** (%) edges – attack rate.
- Study impact of α={1%, 2%, 5%, 10%} *E*.
- Attack strategies [Vespignani, 2010; Wang, 2002]:
  1. Random edge $e_{ij} \in E$.
  2. Targeted edge e_{ij} with probability p_{ij} based on fitness of n_i and n_j

$$f(e_{ij}) = \frac{f(n_i)+f(n_j)}{2} \text{ and } p_{ij} = \frac{f(e_{ij})}{\sum_{e \in E} f(e)}$$

f={degree *Deg*, betweenness *Btw*, eigenvector *Eig*, clustering coefficient *CC*}

The edge **repair** mechanism

Repair rate (ρ) = fraction of new edges to be added back to G.

We remove αE edges, and add back $\rho\alpha E$ edges, $\rho = \{0,10,25,50,100\}\%$.

- We do not restore more edges than removed / iteration!

Repair strategy = selecting a subset of affected nodes to receive new edges.

1. No repair – reference scenario without repairs (most destructive)
2. Random nodes (adjacent to removed edges)
3. High degree first – probability is d.p. ~ $k_i / \sum k_i$
4. Low degree first – probability is i.p. ~ $k_i / \sum k_i$

Other strategies: other node centrality, intra-community-first, redundant-first, cost-optimal-first etc.

Quantifying network fragility

1. Largest component size (LCS)
2. Number of connected components (NCC)
3. *Other: APL, diameter, total connectedness, avg. geodesic length etc.*

A network is more fragile if LCS decreases ***sooner*** and/or to a ***lower*** value.

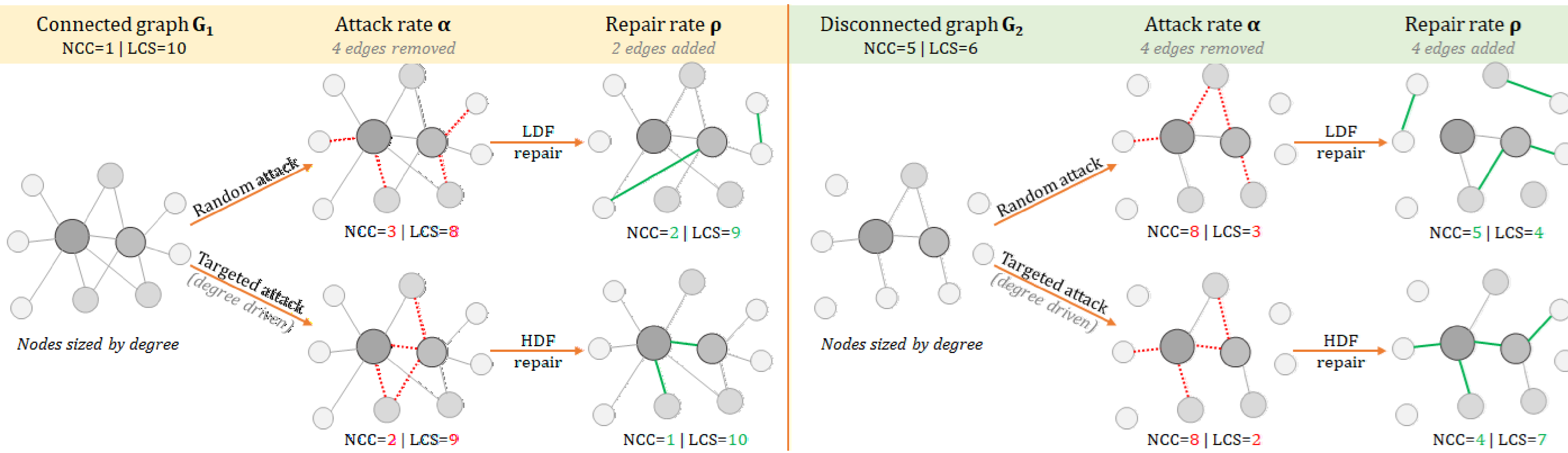
A network is more fragile if NCC increases ***sooner*** and/or to a ***higher*** value.

Network destruction threshold θ_S : when LCS drops below 10%N.

Network destruction time θ_T : time required to reach θ_S

$$0 < \theta_T \leq 100$$

Example of attack-repair mechanism



Random attack > targeted attack

Targeted repair > random repair

Targeted repair reduces NCC, increases LCS → antifragility!

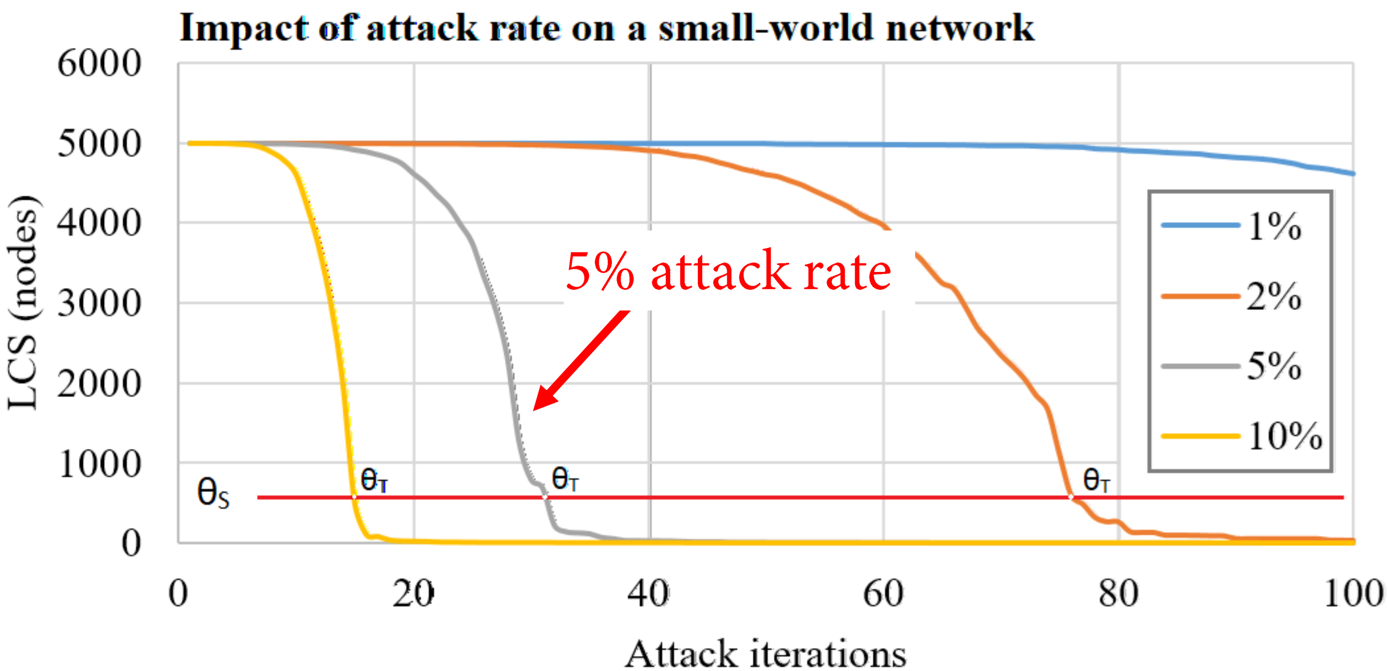
Datasets used for validation

Network	N	E	APL	ACC	Dmt	LCS	NCC
Rand	5000	25061	3.944	0.002	7	5000	1
Mesh	5000	26948	11.51	0.148	30	4989	12
SW	5000	19999	6.738	0.298	12	5000	1
SF	5000	15672	5.378	0.007	13	4999	2
FB	558	6829	2.829	0.469	8	558	1
CoAu	1589	2742	5.823	0.878	17	379	396
OSN	1899	20296	3.055	0.138	8	1893	4
Geom	3621	9461	5.316	0.679	14	3621	1

CoAu – initial LCS is about 24% of N.

Results. Impact of attack rate.

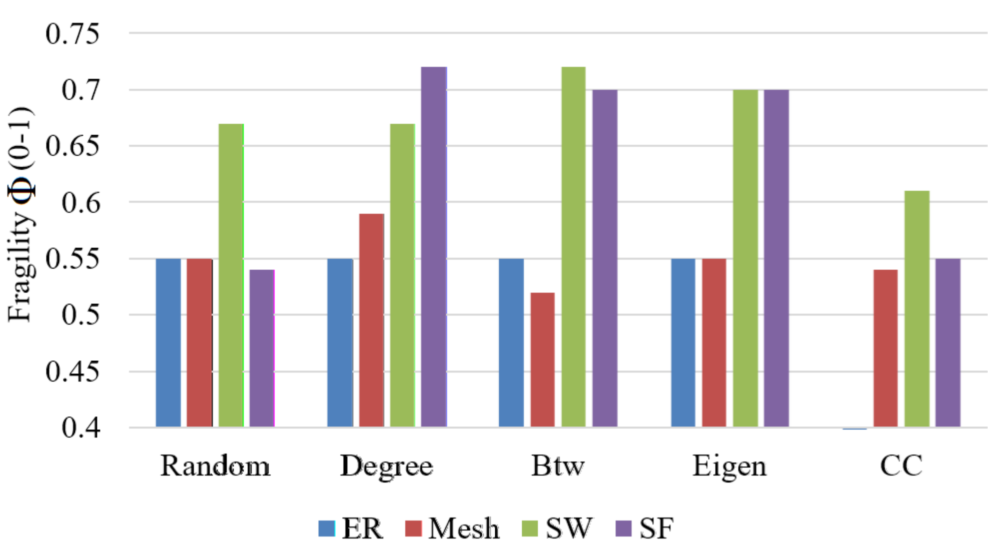
Study of α={1%, 2%, 5%, 10%} on SW (all other nets yield similar results).

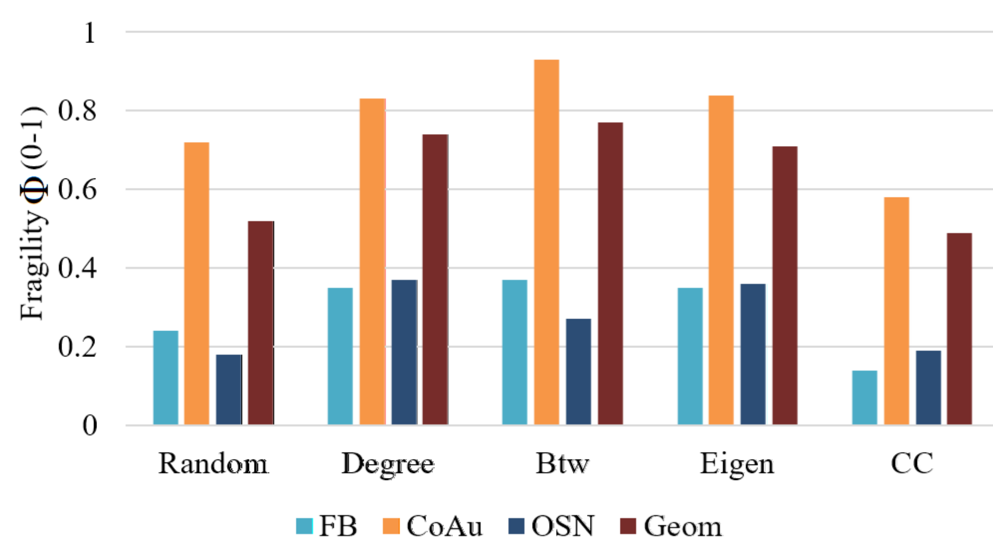


Network	1%	2%	5%	10%
Rand	-	-	45	23
Mesh	-	-	45	23
SW	-	78	33	17
SF	-	-	46	24
FB	-	-	76	34
CoAu	84	54	15	11
OSN	-	-	82	40
Geom	-	-	48	24

Results. Attack strategy analysis.

Estimation of fragility based on destruction time: $\phi = \frac{100-\theta_T}{100}$





SW 22-31% more fragile overall (hint: long-range links are weak spots)

SF more fragile only when using centrality targeted attacks

Meshes are as robust as random networks!

Results. Repair strategy analysis.

Study of ρ={0%, 10%, 25%, 50%} → ρ=25% sweet spot

Strategies: no repair, random, HDF, and LDF.

Results: HDF > LDF > random

Network	None	Random	HDF	LDF
Rand	45	59	79	68
Mesh	45	63	83	65
SW	33	54	69	63
SF	46	59	75	55
FB	76	82	100	92
CoAu	15	40	60	24
OSN	82	92	100	90
Geom	48	57	70	53

Interpretation:

- HDF consolidates a strong core of the network
- LDF immediately reconnects disconnected nodes

Results. Combined results.

θ_T obtained for random – HDF with α=5%, ρ=25%.

Avg synth random θ_T: 56.68

Avg synth HDF θ_T: 65.37 (+15%)

Avg real random θ_T: 63.95

Avg real HDF θ_T: 67.90 (+6%)

Network	*Rand*	*Deg*	*Btw*	*Eig*	*CC*
Rand	59-79	58-71	60-64	57-69	N/A
Mesh	63-83	61-72	75-71	69-70	67-75
SW	54-69	53-69	46-45	51-60	53-67
SF	59-75	44-47	44-41	43-45	61-70
FB	82-100	85-84	90-91	91-87	99-100
CoAu	40-60	29-36	7-7	20-19	45-48
OSN	92-100	82-85	98-100	83-89	98-100
Geom	57-70	41-40	34-35	37-38	69-69

Friendship nets (FB, OSN) less fragile than collaboration nets (CoAu, Geom).

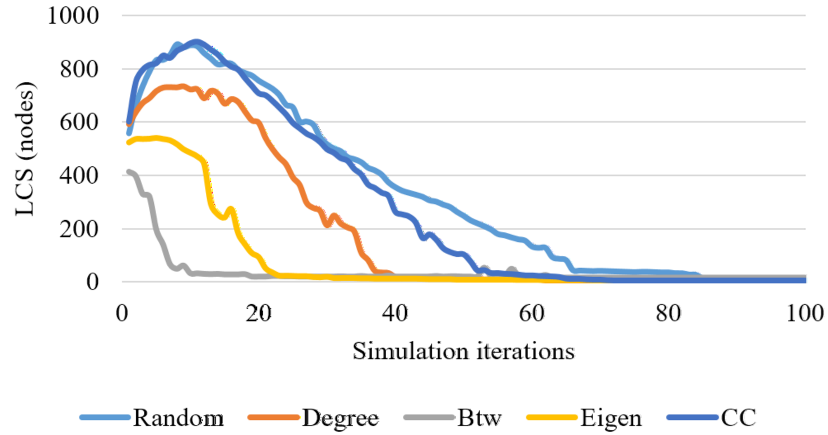
"Friendships" most vulnerable to Deg (ϕ=0.16), Eig (0.12), Btw (0.05).

"Collaborations" most vulnerable to Btw(ϕ=0.79), Eig (0.71), Deg (0.62).

Topological **antifragility**

Topological antifragility expresses the possibility of increasing the largest component while being under the attack-repair mechanism.

- Exemplified on the CoAu network.
- N = 1589 nodes, initial LCS = 379 (23.8% of N).
- LCS_{max}=902 (+138% and 56.7% of N)



Particularly on this topology, Btw & Eig prove much more aggressive and do not allow for any antifragile response.

Discussion

Real-world nets are **less fragile** than synthetic ones (40-130%).

Repairs have bigger impact on real nets (75-109%) than synth nets (22-46%).

Best **targeting** strategies for real nets: Btw, Deg (22% better than random)

Best **aiding** strategy is high degree nodes first.

- HDF is 16-36% better than LDF repairs.
- LDF is 3-15% better than random repairs.
- LDF = random on SF networks.

Conclusions

→The idea of counter-balancing attacks with a repair mechanism.

→Need for balance between attack rate and repair rate.

→Social systems rely on dynamical weighted ties which can change rapidly.

If a social agent does not keep his ties "alive", they may fade away, being replaced by new ones (connecting to other agents).

→Increase of largest component due to edge repairs.

Strengthening of the network while under attack: topological antifragility.

"You are what you share."

— *Charles Leadbeater* —

Free datasets available on ACSANet:

`cs.upt.ro/~alext/acsanet`

Authors A.T. and M.U. are partly supported by the Romanian National Authority for Scientific Research and Innovation (UEFISCDI), project numbers PN-III-P2-2.1-PED-2016-1145 (M.U.) and PN-III-P1-1.1-PD-2016-0193 (A.T.).