Using Community Structure Information to Improve Complex Networks Robustness

Cinara G. Ghedini* and Carlos H. C. Ribeiro*
*Aeronautics Institute of Technology
Computer Science Division
São José dos Campos – SP – Brazil
Email: cinara,carlos@ita.br

***Abstract*—This paper discusses the relation between two emergent features of most complex networks: community structure and high sensitivity to attacks. More specifically, we consider how the former can support mechanisms to mitigate the latter. The main point stressed here is that information about the community structure can be useful to detect and mitigate vulnerable topological configurations w.r.t network connectivity. We demonstrate this through an attack and failure protocol that considers the importance of central nodes regarding their roles connecting nodes, either inside or outside communities. We also propose local mechanisms for evaluating topological configurations based on community information. The strategy for minimizing the impact of central node failures to network connectivity relies on the creation of redundant paths between communities. The networks evaluated exhibited a significant improvement in their robustness regarding connectivity maintenance, being almost unaffected by failures of central nodes. The experimental benchmark encompasses both real complex network datasets and networks generated by well-established construction methods.**

Keywords–attacks and failures tolerance; community structure; adaptive mechanisms

I. INTRODUCTION

Complex networks exhibit unique characteristics that are often discussed in the literature, as the small-world effect, the clustering coefficient and the degree distribution [1]–[4]. Beside them, community structure is one of the main properties of real complex networks undergoing studies. Its features can support the understanding of the network formation and evolution processes, the collective and individual behavior, the information dissemination, among others, thus, being useful for a broad range of applications, from disease spreading to marketing.

Despite some nuances deriving from topological characteristics of each network, it is known that some property values combinations, which occur in several real networks, can produce robust networks regarding failures. On the other hand, when the most central nodes fail, the topology of complex networks is fairly affected, compromising the network operation [5]–[11]. Despite this eminent feature being well stated, mechanisms to evaluate and mitigate such states are mostly neglected. Analytical approaches for global robustness estimation are presented in [12][13]. Wang *et al.* [14] propose a global approach for supporting the design of networks through mechanism for detecting and protecting those links which are crucial for the network robustness.

Based on this, our approach explores community structure information for detection and mitigation of vulnerable topological configurations. For that, we evaluate the impact that links connecting elements in the same community (inside links), different communities (outside links) or both, have on the network topology when they fail. The results demonstrate that nodes connecting different communities indeed play a central role regarding the communication among network elements. Taking advantage of this information, mechanisms to identify possible harmful topological configuration and to promote adjustments on the network are proposed. Such mechanisms are based on previous work presented in [15], which considers a node as the main agent for detecting vulnerability and local efficiency as the measure for representing the state of vulnerability. Here, we propose using the community local efficiency for both goals. Differently, Yang *et al.*, in a very recent paper [16], use community information for supporting a global link rearrangement procedure, as a possible way to improve the network robustness, without taking into account the detection of harmful configurations or methods to precisely revert them.

For benchmarking the experiments, we rely on real network datasets and networks generated by two constructive models: Barabasi and Albert's [2] and Klemm-Euguluz [17] models, plus a protocol to promote perturbations on the network and classical topological measures, such as the global and local efficiencies, and the size of the giant component. The findings are that concepts related to community structure can be used to improve the surveillance of communication and service networks in case of failures and attacks. In addition, they can be applied for maintaining/reinforcing the channels of interaction among agents on business, social and professional networks, or for supporting decision making in topology control protocol, w.r.t which connections should be preserved.

The rest of this paper is structured as follows. Section II presents the benchmark and the experiment protocol adopted to evaluate the network sensitivity to attacks and failures. Section III discusses the results of the new protocol to evaluate the role of community links in the network communication. Section IV presents the adaptive mechanisms proposed and their evaluated performances. Finally, Section V summarizes the conclusions and contributions, and point out some issues for future research.

II. BENCHMARK AND PROTOCOL FOR NETWORK ASSESSMENT

A combination of models and metrics provides the benchmark for assessing the exposure of complex networks to failures and attacks, and for supporting a targeted analysis. This section outlines the framework applied for carrying this analysis. The main components are the network models, the centrality measures, and the simulation protocol.

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-401-5

A. Complex Network Models

The interaction among agents in a complex system tends to create efficient networks at global and local levels, often under a scale-free degree distribution. Based on this, many researchers have proposed different models to create networks with particular topological properties as convenient simulations of real networks. For our study we consider two of the most widely used models: the Barabasi and Albert's (BA) model [2] and the Klemm-Euguluz (KE) model [17], referred from this point on as BA networks and KE networks, respectively.

Table I presents the models main topological properties values: the number of network nodes (n) and edges ($|\mathrm{E}|$), the average degree ($\langle \mathrm{k} \rangle$), and the global ($E_{glob}$) and local ($E_{loc}$) efficiencies - see Section II-D for technical details on how the efficiencies are computed.

TABLE I. TOPOLOGICAL PROPERTIES OF BA AND KE NETWORKS

Network	n	$\|\mathrm{E}\|$	$\langle k \rangle$	E_{glob}	E_{loc}
BA	1000	5979	11.95	0.37	0.047
KE	1000	5973	11.94	0.30	0.60

B. Real Network Datasets

Real datasets were considered for the experimental analysis. Some of them are classical benchmarks for studies in community-related approaches, the others are classical datasets in the complex networks literature, in general. The datasets and their main topological properties are shown in Table II.

TABLE II. DESCRIPTION AND PROPERTIES OF REAL NETWORK DATASETS

Dataset	n	$\|\mathrm{E}\|$	$\langle k \rangle$	E_{glob}	E_{loc}
The US heaviest traffic airports [18]	500	2980	11.92	0.37	0.62
The protein interaction of yeast [1]	417	511	2.45	0.19	0.05
American College football	115	613	10.6	0.45	0.40
Dolphins	62	159	5.13	0.37	0.26

C. Failures and Attacks Protocols

This work is based on the assumption that community structure can be worthwhile to support the evaluation and mitigation of vulnerable topological states. Thus, the network target of analysis has its nodes classified according to the community they belong. The approach to find and update communities is presented in [19].

For simulating failures, nodes are considered autonomous agents that can leave the network at random with a uniform probability distribution. On the other hand, to reproduce a possible scenario of attacks, central nodes must be removed from the network. There are several criteria to rank nodes according to their positions in the network, in general, the Betweenness Centrality (BC) has been considered as a convenient measure of centrality w.r.t. communication. BC establishes higher scores for nodes that are contained in most of the shortest paths between every pair of nodes in the network. In fact, considering communication networks, nodes with this feature are likely to be crucial to maintaining the network functionality.

For a given node i and a pair of nodes j, l, the importance of i as a mediator of the communication between g and l can be established as the ratio between the number of shortest paths linking nodes j, l which passes through node i ($g_{jl}(i)$), and the total number of shortest paths connecting nodes j and l (g_{jl}). Then, the BC of a node i is simply the sum of this value over all pairs of nodes, not including i [20]:

$$BC(i) = \sum_{j<l} (g_{jl}(i)/g_{jl}). \quad (1)$$

For assessing the relevance of community structure information to detect and mitigate vulnerable topological network configurations, a protocol for attacks and failures concerning the role of central nodes in the community structures were applied. It encompasses: 1) ranking nodes according to BC or random criteria; 2) removing links of the most central node from the network considering its role in the node community: inside, outside or both; and 3) computing the target properties values. At each iteration, the node ranking is updated until a previously defined fraction (f) of nodes become disconnected from the network.

The adaptive mechanism must compensate the central node failures with addition of new links. Thus, for its performance evaluation the most central nodes are completely removed from the network. For validation purposes, three heuristics were defined considering the constraints of creating new links according to their roles: *inside* or *outside* the community, or *both*. For model-based networks, the results were averaged over five realizations.

D. Evaluation Mechanisms

A network is modeled as a graph $G = (N, E)$ defined by a set of nodes (or vertices) $N = 1, 2, ..., n$ and a set of links (or edges) $E \subseteq NXN$. A connection between vertices may be absent when there is no direct relationship or communication between them, or it may assume a value in $[0, 1]$ representing the strength (weight) of the connection. Only undirected and unweighed networks are considered here.

The impact assessment is supported by classical topological metrics related to the most important topological features found in real networks, as follows.

1) Global Efficiency: Latora *et al.* [21][22] introduced a measure of efficiency which computes how efficiently nodes exchange information either in a local or global scope, independently of whether the network is weighted or unweighted, connected or disconnected. For a given pair of nodes (i, j), its contribution to the global efficiency is inversely proportional to the shortest distance between them (d_{ij}), therefore $e_{ij} = \frac{1}{d_{ij}}$.

The global efficiency $\mathcal{E}_{glob}(G)$ of a graph G can then be defined as:

$$\frac{\sum\limits_{i \neq j \in G} e_{ij}}{n(n-1)} = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}, \quad (2)$$

and therefore, $\mathcal{E}_{glob}(G) \geq 0$. From this point on, we normalize this measure, considering the ideal situation G_{ideal} where all the possible $n(n-1)/2$ edges are in the graph, this

is the case when $\mathcal{E}_{glob}$ assumes its maximum value. Thus, the normalized efficiency is:

$$E_{glob}(G) = \frac{\mathcal{E}_{glob}(G)}{\mathcal{E}_{glob}(G_{ideal})}. \quad (3)$$

2) Local Efficiency: The local efficiency is defined as the ratio between the number of edges that actually exist among i's neighborhood (not including i itself) and the total number of possible links. If the nearest neighborhood of i is part of a clique, there are $k_i(k_i-1)/2$ edges among the corresponding nodes, where k_i is the degree (number of links) of node i. Formally,

$$E_{loc}(G) = \frac{1}{n}\sum_{i \in G} E_{loc}(G_i), \quad (4)$$

where

$$E_{loc}(G_i) = \frac{1}{k_i(k_i-1)} \sum_{l \neq m \in G_i} \frac{1}{d_{lm}}. \quad (5)$$

and G_i is the subgraph induced by the nodes directly connected to i.

3) Giant Component: In most real-world complex networks, it has been observed that there is a large connected component, often called giant component, together with a number of small components containing no more than a few percent of the nodes [23]. A connected component of a graph is a set of nodes such that a path exists between any pair of nodes in this set. Its analysis may provide valuable insights for quantitative analysis, for instance, on how information dissemination and percolation in Epidemiology-related systems are affected by the disconnection or loss of nodes [23]–[29].

Notice that the size of the largest connected component is often equated with the graph-theoretical concept of the "giant component", although technically the two are the same only in the limit of large graph sizes [4]. For the sake of simplicity, we adopt herein the denomination "giant component" whenever we refer to the largest component. As a matter of fact, the connectivity of a network G can be estimated by the relative size $S(G)$ of the giant component, given by the fraction of nodes in the network taking part in the largest connected component:

$$S(G) = \frac{n_{Giant}}{n}, \quad (6)$$

where n_{Giant} is the number of nodes in the giant component and n is the number of nodes in the network.

III. Community-based network robustness

For assessing the role that central elements play in the community structure concerning robustness to failures and attacks, the protocol for link removals (see Subsection II-C) was applied. The results are depicted using blue, red, and green lines representing the removal of node's link(s) according to inside, outside and both (inside and outside) criteria, respectively.

Figures 1 to 4 show the evolution of global efficiency and the giant component (y-axis) during the process of attacks, represented by the fraction of nodes removed from the network (x-axis). The results stress the importance of links between communities, emphasizing that losing channels of communication between communities may be potentially harmful to the network connectivity. It means that those nodes responsible for linking communities may be the key elements for evaluating and mitigating topological states of vulnerability.

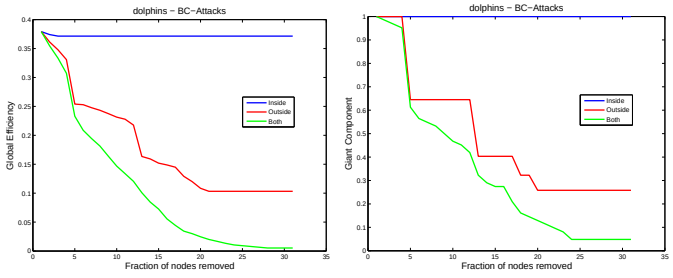

Figure 1. Global efficiency and giant component – BC attacks for dolphins network.

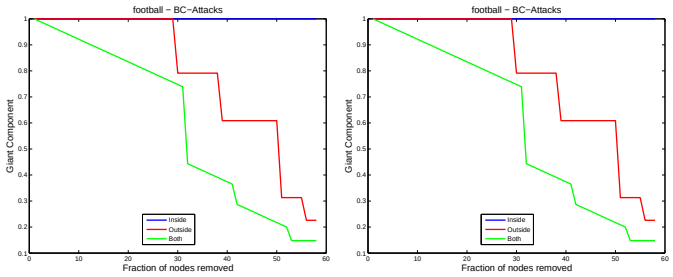

Figure 2. Local efficiency and giant component — BC attacks for football network.

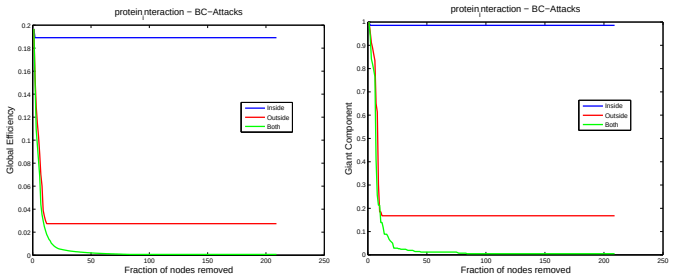

Figure 3. Global efficiency and giant component — BC attacks for Protein Interaction network.

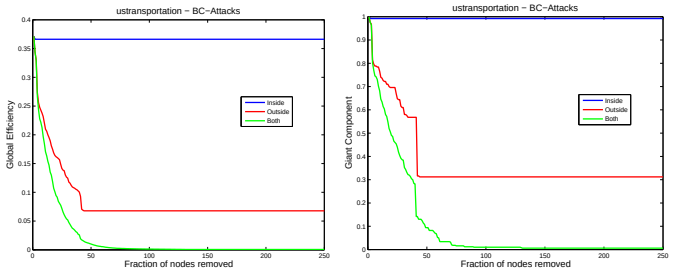

Figure 4. Global efficiency and giant component — BC attacks for UStransportation network.

Figure 5 illustrates the classification of links at each network state during the perturbation process considering the

removal of both links (inside and outside) for the Dolphins network. The inter-communities bars represent the fraction of nodes that are connecting nodes from different communities. In turn, the intra-community bars represent those links that are connecting nodes belonging to the same community. They are computed taking into account the entire network (on the left) and the links that were removed from the network (on the right). Notice that at the beginning of the perturbation process, despite the fraction of intra-communities links considering the entire network is around 0.3, they were the majority of links lost. Furthermore, they were those which more severely affect the network connectivity (see Figure 1), highlighting the importance of these links to the network connectivity.

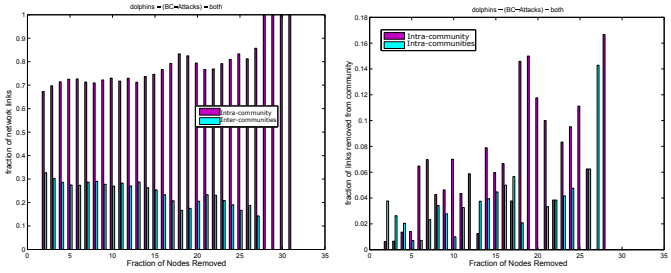

Figure 5. Link statistics — BC attacks for Dolphin network.

Figure 6 shows the results for BA and KE networks.

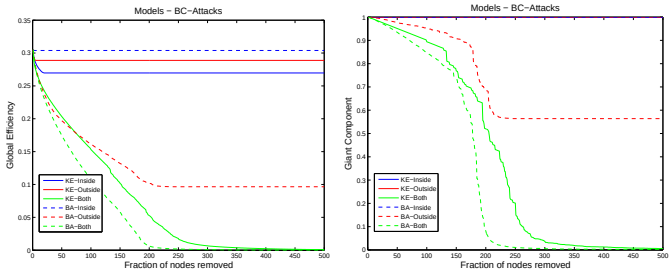

Figure 6. Global efficiency and giant component — BC attacks for BA and KE networks.

The property values of BA networks (dashed lines) showed the same pattern that real network topologies. On the other hand, for the KE networks the removal of both types of links were necessary to actually impact the network connectivity, thus deviating from most of the results achieved for inside and outside strategies, even for some other real networks not presented in this paper.

IV. Adaptive Mechanism

The approach proposed here is based on the previous work presented in [15]. It considers nodes as the main agents for controlling the necessary information and procedures responsible for evaluating and promoting changes in the network topology. For that, some nodes are assumed to be more likely to affect the network connectivity according to some likelihood status, and thereby, nodes in their neighborhood can be defined as in a vulnerable state. Here, the unit of analysis changes from nodes to a higher hierarchic structure according to the graph partition generated by the community detection technique [19]. A partition P is a division of a graph into clusters, such that each vertex is assigned to one and only one cluster. Even though some approaches consider vertices belonging to two or more clusters simultaneously [30], here each node takes part of a single community/cluster.

A community C is classified as in a vulnerable state if some specific property value is lower than expected. Two states are thus defined: vulnerable ($V_{C,t} = 1$) and not vulnerable ($V_{C,t} = 0$), according to:

$$V_{C,t} = \begin{cases} 1 & \text{if } \delta_{C,t} >= \gamma \\ 0 & \text{if } \delta_{C,t} < \gamma \end{cases}$$

where $\delta_{C,t}$ represents the target property value for community C at a specific time t. The threshold to set a community as vulnerable is given by the parameter γ. Both the target property and the vulnerability threshold can be set out as convenient for the vulnerability problem being handled.

The adaptation process is straightforward. It encompasses two main functionalities: the vulnerability assessment and the creation of new links. In compliance with the attacks and failures protocol, after each node removal, every community C assesses its vulnerability state. If applicable (*i.e*, when $\delta_{C,t} < \gamma$) new links are added in the network to try to reverse or minimize the adverse effects of the resulting topological configurations. For validation purposes three strategies were implemented:

- *inside*: adding connections between nodes belonging to the same community,
- *outside*: creating link(s) between node(s) from the vulnerable community to other(s) neighboring community(ies),
- *both*: the combination of inside and outside strategies.

The criteria for the definition of new connections are tied to the vulnerability property. According to the results discussed in [15], the local efficiency is a potentially good estimator for detecting and mitigating vulnerable states. Consider then the concept of local efficiency (5) at the community level:

$$E_{loc}(C_i) = \frac{1}{k_{in}(C_i)(k_{in}(C_i)-1)} \sum_{l \neq m \in C_i} \frac{1}{d_{lm}}. \quad (7)$$

where $k_{in}(C_i)$ is the number of nodes belonging to community C_i.

For new inside links, the non-connected nodes exhibiting the lowest and the highest local efficiency are connected. As the probability of sharing common neighbors is higher inside the community, this new connection tends to enhance the local community robustness.

The *outside* strategy considers that each vulnerable community (source community) should reinforce its connection with the neighboring communities with which it is weakly connected. Considering C as the set of communities in G and C_i the set of nodes belonging to community i, the neighboring of community C_i is $N(C_i) = \{(C_j \in C | e_{v,u} \in E \wedge v \in C_i \wedge u \in C_j\}$ and $k_{out}(C_{i,j})$ the number of times a community C_j appears in $N(C_i)$. For a vulnerable community C_i, the lowest community degree value $min(k_{out}(C_{i,j}) | C_j \in N(C_i))$ is the threshold to define the neighbor community(ies) to create a connection. It means that those neighboring communities

with fewer connections are the targets for new connections, thus creating an alternative path between them.

The strategy to identify which nodes will receive new connections in both source and target communities is the same: the priority is for choosing nodes without any link with other communities. In the case of absence of nodes showing this feature, those nodes without connections with the target community are selected.

The *both* strategy combine the inside and outside procedures.

A. Results

For performance evaluation, the vulnerability threshold was set to $\gamma = E_{loc}(G) * 0.5$. This definition relies on the assumption that communities with local efficiency below the network local efficiency (see (4)) are more likely to be vulnerable.

Figures 7 to 12 present the adaptive mechanisms performance. Each line shows the evolution of global efficiency (on the left) and size of the giant component (on the right) during the process of attacks regarding different adaptation strategies: H is the original heuristic [15], $E_{loc}(outside)$, $E_{loc}(inside)$ and $E_{loc}(both)$ are for the *outside*, *inside* and *both* strategies, respectively. For benchmarking, G depicts networks without any running adaptive mechanism.

As expected, the improvements accomplished by the $E_{loc}(inside)$ strategy were irrelevant. The results for the original strategy demonstrate that its performance is related to the network local efficiency, mainly because the creation of links depends on the existence of non-vulnerable nodes. It means that vulnerable states can be detected, but the requirement to add links is not fulfilled. The evolution of both global efficiency and size of the giant component for Football, UStransportation and KE networks, which exhibit the higher scores for local efficiency (see Tables II and I), demonstrate that.

On the other hand, $E_{loc}(outside)$ and $E_{loc}(both)$ strategies produced significant results for all networks evaluated and were able to maintain the majority of nodes connected to the giant component. It is important to notice the influence of the initial network configuration regarding its sensitivity to attacks. For instance, the Football and Dolphins networks are less affected by attacks, so the adaptive community-based mechanisms were able to maintain the global efficiency and nodes in the giant component for most iterations, with the addition of a few links (see Figure 13). In turn, for more sensitive topologies, such as Protein Interaction and UStransportation networks, a small fraction of nodes was not able to be maintained in the giant component, despite the number of links created in the beginning of the adaptation process. Therefore, considering these networks sensitivity, the community-based heuristic improved the network robustness.

Figure 13 shows the proportion of new links created at each iteration. Notice that for the Football network a few nodes were added to the network considering the community-based heuristic. Regarding the Protein Interaction network, the proportion of new links for *outside* and *both* strategies at the beginning of process are around 0.40 of the total number of links in the network.

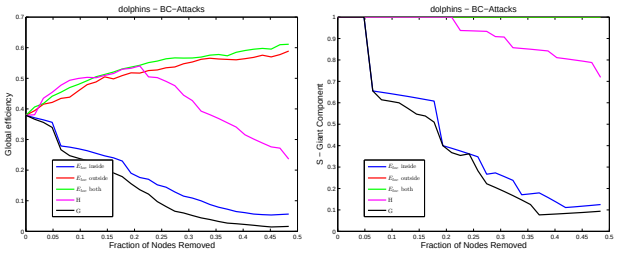

Figure 7. Global efficiency and giant component — Adaptation - Dolphin network.

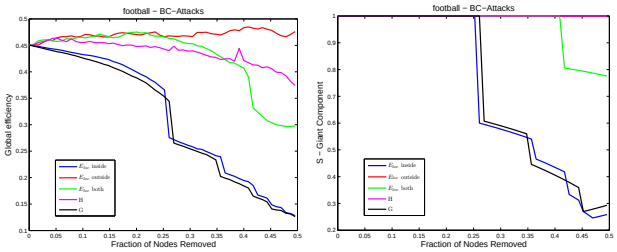

Figure 8. Global efficiency and giant component — Adaptation - Football network.

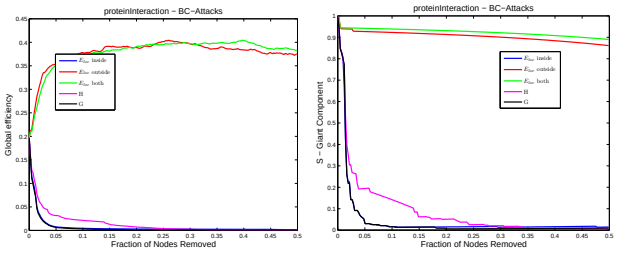

Figure 9. Global efficiency and giant component — Adaptation - Protein Interaction network.

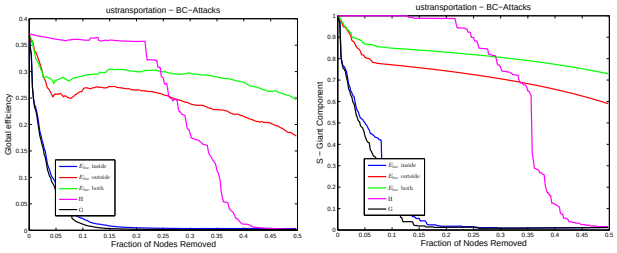

Figure 10. Global efficiency and giant component — Adaptation - USTransportation network.

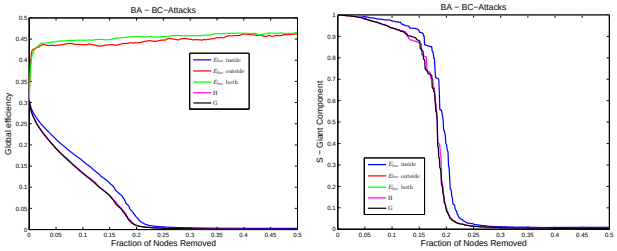

Figure 11. Global efficiency and giant component — Adaptation - BA networks.

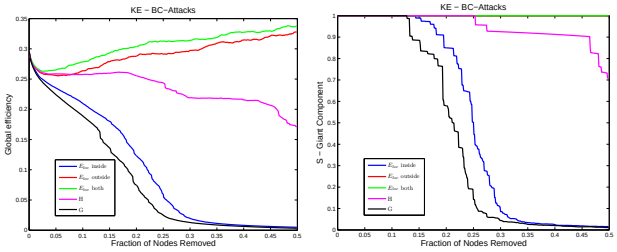

Figure 12. Global efficiency and giant component — Adaptation - KE network.

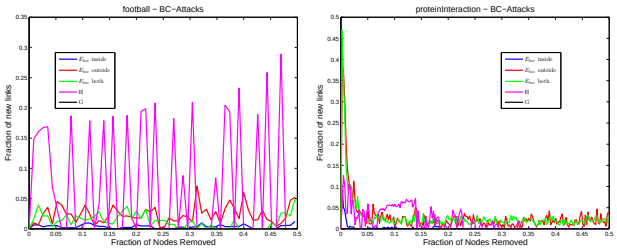

Figure 13. Global efficiency and giant component — Adaptation - USTransportation network.

As highlighted before, this network topology is quite sparse, exhibiting low scores for efficiencies and average degree, so it is necessary to create more links to provide a more robust network. However, after the initial adjustments, the network was able to accommodate perturbations and to maintain its global efficiency and the size of the giant component.

V. Conclusion

The first aspect highlighted here is that central nodes are probably those connecting communities and, therefore, information about the community structure can be worthwhile to design networks that are more resilient to failures and attacks. Taking this premise into account, community-based mechanisms to evaluate and mitigate vulnerable topological configurations were proposed in this paper. The solution comprises three main components: community identification, vulnerability detection and vulnerability mitigation. For the first component, a well-established method was applied [19]. For the second, a mechanism based on previous results from [15], but adapted to communities instead of nodes, was proposed. It considers as vulnerable those communities exhibiting local efficiency below the network local efficiency. Finally, the proposed heuristic to mitigate possibly vulnerable states relies on the creation of additional links between communities. For reinforcing the importance of the community structure, three different strategies were evaluated, considering creating links inside or outside the communities, or both. The $outside$ and $both$ community-based heuristics outperformed both the $inside$ community strategy and the original method based on node information. Furthermore, they showed less sensitivity to the network topological properties. Thus, the community-based heuristics showed to be a good prospect towards robust mechanisms to deal with the vulnerable topological configurations w.r.t. network robustness to attacks. Future works comprise the evaluation of local mechanisms for communities detection and parameter estimation, as well as the model validation considering larger datasets.

Acknowledgment

The authors would like to thank to FAPESP (procs. no.2012/25058-9, 2013/13447-3 and 2014/13800-8) for the financial support to carry out this research.

References

[1] A. Barabási and Z. Toroczkai, “Center for complex network research,” online, January 2010, network database. [Online]. Available: http://www.barabasilab.com/rs-netdb.php

[2] R. Albert and A. L. Barabási, “Statistical mechanics of complex networks,” Rev. Mod. Phys., vol. 74, no. 1, Jan. 2002, pp. 47–97. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.74.47

[3] E. Almaas and A. L. Barabasi, “Power laws in biological networks,” in Power laws, scale-free networks and genome biology, E. V. Kroonin, Y. I. Wolf, and G. P. Karev, Eds. Springer Science, 2006, pp. 1–11.

[4] M. E. J. Newman, “The structure and function of complex networks,” SIAM Review, vol. 45, no. 2, 2003, pp. 167–256. [Online]. Available: http://link.aip.org/link/?SIR/45/167/1

[5] M. Marchiori and V. Latora, “Harmony in the small-world,” PHYSICA A, vol. 285, 2000, p. 539.

[6] R. Albert, H. Jeong, and A.-L. Barabasi, “Error and attack tolerance of complex networks,” Nature, vol. 406, no. 6794, July 2000, pp. 378–382.

[7] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, “Efficiency of scale-free networks: error and attack tolerance,” Physica A: Statistical Mechanics and its Applications, vol. 320, Mar 2003, pp. 622–642.

[8] L. Dall’Asta, A. Barrat, M. Barthelemy, and A. Vespignani, “Vulnerability of weighted networks,” Journal of Statistical Mechanics: Theory and Experiment, vol. April 2006, 2006, p. P04006.

[9] M. Kurant, P. Thiran, and P. Hagmann, “Error and Attack Tolerance of Layered Complex Networks,” Phys. Rev. E, vol. 76, no. 026103, 2007, p. 026103.

[10] C. Ghedini and C. H. C. Ribeiro, “Rethinking failure and attack tolerance assessment in complex networks,” Physica A: Statistical Mechanics and its Applications, vol. 390, no. 23–24, November 2011, pp. 4684–4691.

[11] Z. He, S. Liu, and M. Zhan, “Dynamical robustness analysis of weighted complex networks,” Physica A: Statistical Mechanics and its Applications, vol. 392, no. 18, 2013, pp. 4181 – 4191. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S037843711300410X

[12] J. Wang, C. Jiang, and J. Qian, “Robustness of interdependent networks with different link patterns against cascading failures,” Physica A: Statistical Mechanics and its Applications, vol. 393, no. 0, 2014, pp. 535 – 541. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378437113007607

[13] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle, “Endurance: A new robustness measure for complex networks under multiple failure scenarios,” Computer Networks, vol. 57, no. 17, 2013, pp. 3641 – 3653. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613002740

[14] X. Wang, E. Pournaras, R. Kooij, and P. Van Mieghem, “Improving robustness of complex networks via the effective graph resistance,” The European Physical Journal B, vol. 87, no. 9, 2014. [Online]. Available: http://dx.doi.org/10.1140/epjb/e2014-50276-0

[15] C. Ghedini and C. H. C. Ribeiro, “Improving resilience of complex networks facing attacks and failures through adaptive mechanisms,” Advances in Complex Systems, vol. 17, no. 02, 2014, p. 1450009.

[16] Y. Yang, Z. Li, Y. Chen, X. Zhang, and S. Wang, “Improving the robustness of complex networks with preserving community structure,” PLoS ONE, vol. 10, no. 2, 02 2015, p. e0116551. [Online]. Available: http://dx.doi.org/10.1371%2Fjournal.pone.0116551

[17] K. Klemm and V. M. Eguíluz, “Growing scale-free networks with small-world behavior,” Physical Review E, vol. 65, no. 5, 2002, p. 057102.

[18] V. Colizza, R. Pastor-Satorras, and A. Vespignani, “Reaction-diffusion processes and metapopulation models in heterogeneous networks,” Nature Physics, no. 3, 2007, pp. 276–282.

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-401-5

[19] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," Journal of Statistical Mechanics: Theory and Experiment, vol. 2008, no. 10, 2008, p. P10008. [Online]. Available: http://stacks.iop.org/1742-5468/2008/i=10/a=P10008

[20] S. Wasserman, K. Faust, and D. Iacobucci, Social Network Analysis : Methods and Applications (Structural Analysis in the Social Sciences). Cambridge University Press, November 1994.

[21] V. Latora and M. Marchiori, "Economic small-world behavior in weighted networks," The European Physical Journal B - Condensed Matter and Complex Systems, vol. 32, 2003, pp. 249–263.

[22] ——, "Efficient behavior of small-world networks," Phys. Rev. Lett., vol. 87, Oct 2001, p. 198701. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.87.198701

[23] P.-Y. Chen and K.-C. Chen, "Information epidemics in complex networks with opportunistic links and dynamic topology," in Global Telecommunications Conference (GLOBECOM). IEEE, Dec 2010, pp. 1–6.

[24] J. Wu, H. Z. Deng, Y. J. Tan, and D. Z. Zhu, "Vulnerability of complex networks under intentional attack with incomplete information," Journal of Physics A: Mathematical and Theoretical, vol. 40, no. 11, 2007, pp. 2665–2671.

[25] M. Latapy and C. Magnien, "Complex network measurements: Estimating the relevance of observed properties," INFOCOM. The 27th Conference on Computer Communications, April 2008, pp. 1660 – 1668.

[26] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," Phys. Rev. E, vol. 66, Dec 2002, p. 065102.

[27] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," Physical Review Letters, vol. 85, no. 25, Dec. 2000, pp. 5468–5471.

[28] R. Cohen, K. Erez, D. B. Avraham, and S. Havlin, "Resilience of the Internet to Random Breakdowns," Physical Review Letters, vol. 85, no. 21, Nov. 2000, pp. 4626–4628.

[29] S. N. Dorogovtsev, J. F. F. Mendes, and A. N. Samukhin, "Giant strongly connected component of directed networks," Phys. Rev. E, vol. 64, no. 2, 2001, p. 025101.

[30] S. Fortunato, "Community detection in graphs," Physics Reports, no. 3-5, pp. 75 – 174.

Copyright (c) IARIA, 2015. ISBN: 978-1-61208-401-5