On the Temporal Evolution of Backbone Topological Robustness

Dimitris Maniadakis, Athanasios Balmpakakis, and Dimitris Varoutas, *Member, IEEE*
Dept. of Informatics and Telecommunications
University of Athens
Athens, Greece
{D.Maniadakis, A.Mpalmpakakis, D.Varoutas}@di.uoa.gr

***Abstract*—As society progressively depends on large-scale telecommunications networks and their connectivity rapidly rises over time, it becomes of vital importance to study their topological features. On the backbone level uncertain disturbances of its constituent parts may affect a sizable proportion of the population, thus this can well explain the recent focus on evaluating backbone robustness metrics. Unlike previous empirical studies, which are limited to static snapshots of topologies, in this paper robustness algorithms are applied to networks over time. The temporal evolution of topological robustness is studied for a set of four real backbone networks by observing snapshots taken at regularly spaced points in time. It is found that only half of the fundamental robustness properties are changing over time with even fewer improving their values. The introduction of the time factor extends the robustness analysis and allows for deriving results on the network robustness dynamics.**

Keywords— backbone network topology; complex networks; network planning and design; network robustness; temporal network evolution

I. INTRODUCTION

As the Internet market continues its spectacular growth, more and more applications are competing for network bandwidth. As a result, the related telecommunications networks evolve with rapidly escalating resources and connectivity, and progressively become an essential component of the national economic and social fabric. Unfortunately, this rising connectivity has an inherent vulnerability; if a network experiences a failure in its constituent parts this may have a dramatic impact on the behavior of the entire network and consequently affect a sizable proportion of the population. For example, earthquakes, tornadoes, floods, fires, power outages, malfunctioning due to equipment aging, fiber cuts, viruses and worms, terrorist attacks, and even operator mistakes may cause serious disruption for several days, especially when they are related to the backbone network which carries aggregated traffic connecting major nodes-cities of a country. Indeed, recently, analogous challenges have already been identified, for instance by the European Union [1], and policy steps have been made to establish procedures for the evaluation and protection of such critical infrastructures [2].

A key requirement towards diminishing the impact of such performance degradations, and accordingly reducing the economic loss, is the understanding of the topological aspects that prominently affect the network robustness. Robustness can be considered as a system's ability to respond to changes in the external conditions while maintaining normal behavior [3] and as an indicator of the performance subject to specific challenges [4]. In particular, topological or structural robustness refers to surviving of connected components when damage occurs on the structure of the network, like node and link failure [3]. Thus, the assessment of topological robustness has to be included in the earliest stages of network planning and deployment in order to determine the response of the network to disturbances, especially in an increasingly uncertain and variable environment. Even when concerning the design of network protocols at interacting network layers, the topological robustness is a key feature to support their evaluation. Therefore, telecommunications engineers, security experts and policy makers seek to understand the techniques for determining network robustness and estimating the appropriate performance metrics that quantify the robustness of this critical infrastructure.

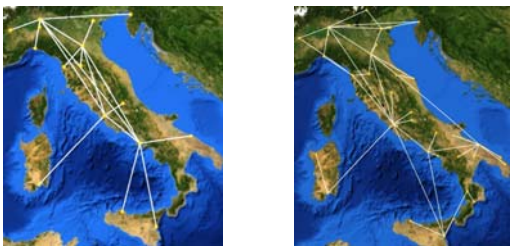
Topological robustness has been studied in the context of graph theory and complex networks in order to explicitly propose different robustness measures, such as heterogeneity, symmetry ratio, algebraic connectivity, etc. [3, 5-13], or in order to use them for evaluating real-world networks [14]. For instance, in [5] robustness is measured as algebraic connectivity, and hence the study points to explicit influence of the network structure on the robustness. However, little is known about the relation between all these metrics over time, since the previous studies are concerned with static network snapshots [13, 14].

Given the lack of information about real network evolution over long periods, it is hard to convert robustness findings into statements about trends over time. Nevertheless, almost all large real-world networks evolve over time by the addition and deletion of nodes and links. In practice most telecommunications networks are designed incrementally over time. Studying the evolution of network connectivity over time can offer unique insights that cannot be derived from a single static snapshot. Recent findings on temporal network evolution

mostly focus on the growth of Autonomous System (AS) level router network [15, 16] providing evidence that networks densify over time and that average distance between nodes often shrinks over time. Thus, while one can assert that real networks retain certain trends for the basic statistical metrics, it has not been clear how robustness metrics behave over time.

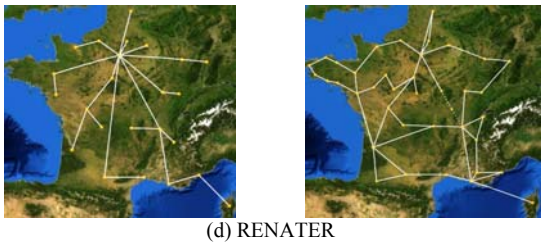
Contrary to previous empirical studies, such as [14], this paper studies the temporal evolution of topological robustness. In particular, it explores the characteristics of four real backbone telecommunications networks over a temporal sequence of nodal interactions and uses twenty metrics to quantify topological robustness and identify their trends. Apart from the inherent graph-theoretic interest, the study of the structural properties of real networks always gives critical information about the network behavior and contributes to understanding its robustness and performance. To the best of our knowledge, this is the first detailed study of backbone topological robustness evolution over time. This study complements previous studies, which have focused on the robustness of telecommunication networks and allows to answer to the following questions: *How do backbone networks evolve over time? Do all robustness metrics point in the same direction? What metric do network engineers appear to optimize as robustness metric?*

(a) CESNET



(b) GARR

(c) GEANT



(d) RENATER

Fig. 1. Initial and final connectivity layouts of the considered networks.

The rest of this paper is structured as follows. In Section 2 the relevant topological metrics are presented. Section 3 describes the dataset and discusses the results of applying the robustness algorithms. Finally, Section 4 concludes the analysis and proposes the directions for future work.

II. TOPOLOGICAL ROBUSTNESS METRICS

The common approach of regarding a telecommunication network as a graph is considered here. In particular, the topology is defined as an undirected and unweigthed graph which abstracts the connectivity of a backbone network.

There is a wide range of topological properties offered for investigation, from the mean degree to more complex measures, such as the assortativity coefficient. A set of twenty commonly used measures that are more relevant to the topological robustness of a telecommunication network is selected at this point and can be seen in Table I. Given space limitations, notations and definitions are excluded here, although a brief description of the robustness metrics follows along with results in the next Section. In Table I, references include definitions and formulas of the considered metrics.

TABLE II. METRICS FOR THE EVALUATION OF ROBUSTNESS

Topological Robustness metric	***Reference***
Mean degree	[17]
Average shortest path	[17]
Diameter	[17]
Average clustering coefficient	[17]
Assortativity coefficient	[17]
Vulnerability	[6]
Algebraic connectivity	[5]
Efficiency	[18]
Normalized betweenness centrality	[19]
Entropy	[20]
Average two-terminal reliability - targeted	[21]
Average two-terminal reliability - random	[21]
Symmetry ratio	[7]
Effective graph resistance	[8]
Natural connectivity	[9]
Percolation threshold	[10]
Heterogeneity	[11]
Average neighbor connectivity	[13]
Node connectivity	[12]
Edge connectivity	[12]

NOC/OC&I 2013, ISBN: 978-1-4673-5822-4

III. DATASET AND RESULTS

A. Dataset description

In the present paper the focus is particularly on backbone networks. Since public data about backbone topologies are limited for business competitiveness and security reasons, it is chosen to use time-evolving topologies of Research and Education Networks (REN) from a repository of well known real telecommunication networks [19]. The number of available networks is further limited when imposing the requirement of snapshots for a period of at least 10 years and final network size of at least 40 nodes. Finally, data from four real backbone networks are collected and analyzed, namely *CESNET*, *GARR*, *GEANT* and *RENATER*. The network configurations are on the Points-of-Presence (PoP) level of the logical - IP layer. The PoP level is motivating since it shows the wide-area links which are the most interesting when it comes to network design optimizations and it is the level at which robustness is often considered. The logical topology is usually the lightpath topology of an optical network, with a link or edge between two nodes (PoPs) if there is a lightpath between them.

For ease of presentation, all considered networks are depicted to start at the same time step t=1 and each time step represents a year. However, actual initial and final date, as well as number of samples may be different for the networks under study, as seen in Fig. 2 and Fig. 3. The number of nodes and edges grows linearly over time. Nodes and edges are tripled on average at the final state. Thus, it is of great interest to investigate how the robustness measures have changed over those years.

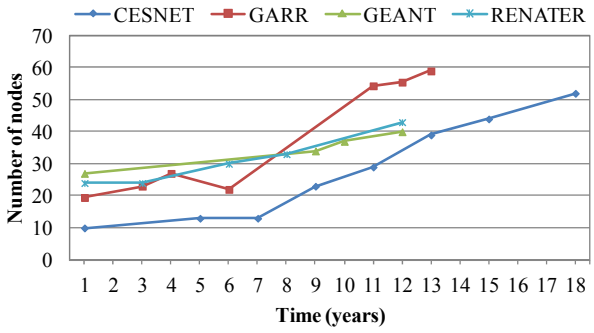


Fig. 2. Number of nodes over time.

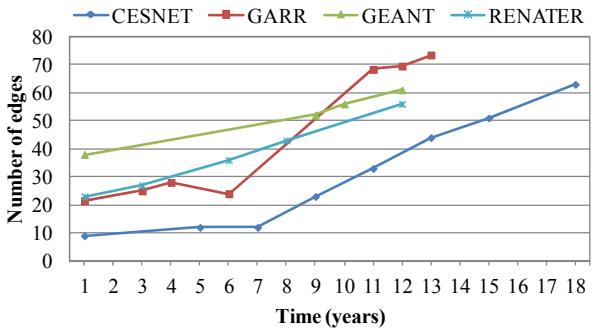


Fig. 3. Number of edges over time.

B. Topological robustness results

First, the mean degree of a network is the average degree over all nodes and is a common connectivity feature of any topology [17]. The degree of a node is in fact the number of edges connected directly to that node. If a node with a high degree fails, there are more options to redirect traffic, thus networks with higher mean degree are “better-connected” on average and are expected to be more robust. However, this is a coarse metric since this is a mean value and there are at the same time nodes highly connected and others poorly connected. As seen in Fig. 4, the mean degree appears to be unchanging or slightly increasing over time for all networks.

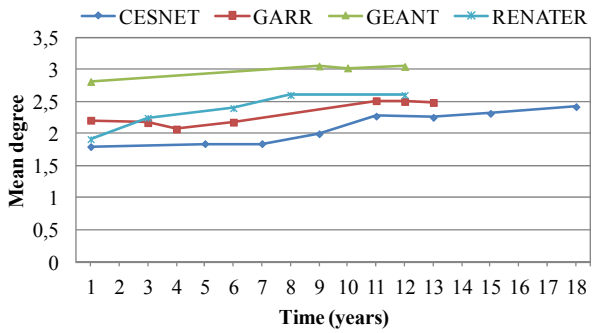


Fig. 4. Mean degree over time.

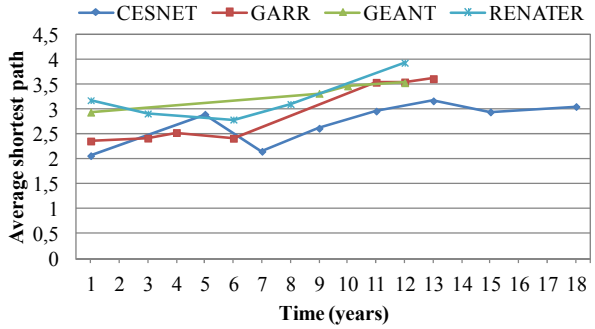


Fig. 5. Average shortest path over time.

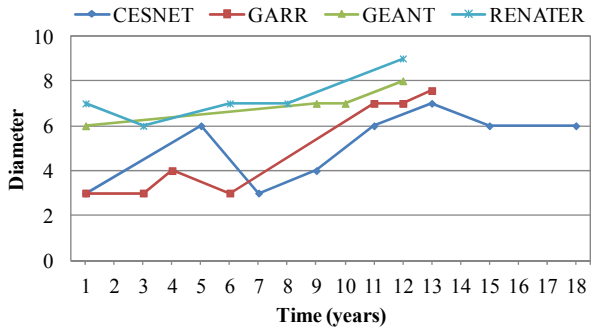


Fig. 6. Diameter over time.

The average shortest path is calculated as an average of all the shortest paths between all the possible origin-destination node pairs of the network [17]. Networks with small average shortest path are more robust since in the case of a failure they are likely to lose fewer connections. As observed in Fig. 5, average shortest path is slowly growing over time.

The diameter is another common robustness metric of a network [17]. It is the longest of all the shortest paths between pairs of nodes and in general, a low diameter means higher robustness. However, in Fig. 6, all networks get higher diameter over time.

Next, the average clustering coefficient, which provides an overall indication of the clustering in the networks based on triplets of nodes [17], shows that networks or snapshots with higher values are most robust, since their nodes are more interconnected with their neighbors. The overall trend in Fig. 7 is that average clustering coefficient increases over time.

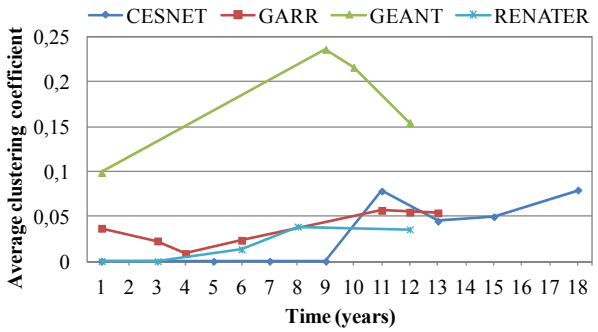


Fig. 7. Average clustering coefficient over time.

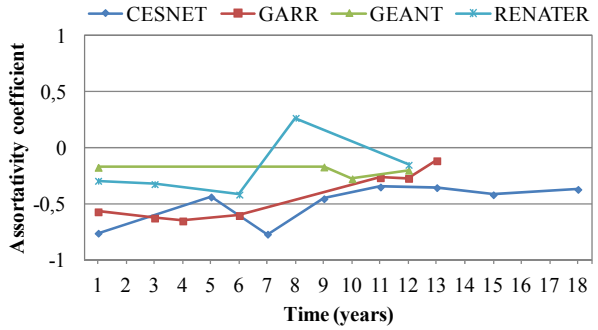


Fig. 8. Assortativity coefficient over time.

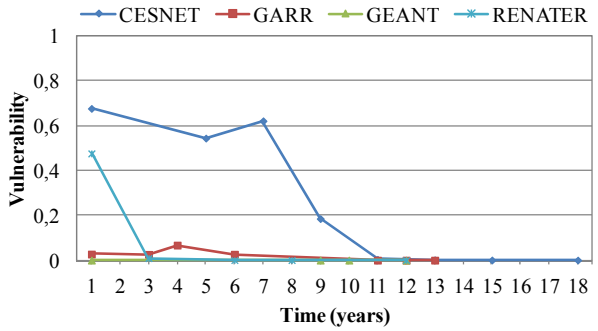


Fig. 9. Vulnerability over time.

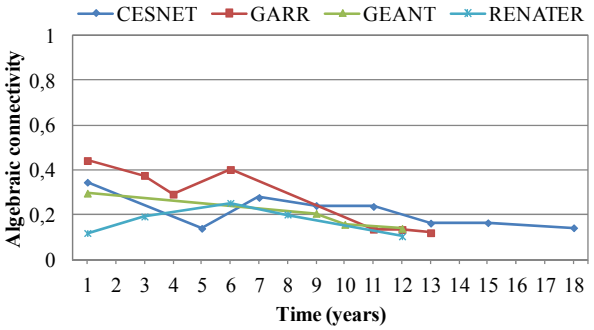


Fig. 10. Algebraic connectivity over time.

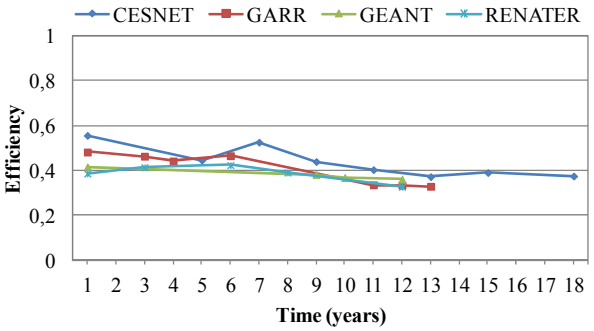


Fig. 11. Efficiency over time.

Concerning the assortativity coefficient [17], when values are negative the network is called to be dissassortative, which means that has an excess of links connecting nodes of dissimilar degrees. Such networks are vulnerable to both random and targeted attacks. The opposite properties apply to assortative networks with positive values that have an excess of links connecting nodes of similar degrees. In Fig. 8, this metric takes higher values over time, with the exception of *GEANT* network where it remains constant.

Although the concept of vulnerability has been introduced from different points of view, here the vulnerability of a network is strongly related to its regularity and the number of alternative edges that can balance a random or intentional attack [6]. Smaller values indicate higher robustness. It is found, as presented in Fig. 9, that network vulnerability decreases over time.

The algebraic connectivity measures how difficult it is to break the network into islands or individual components [5]. It is defined as the second smallest laplacian eigenvalue and the larger it is, the greater the robustness of a topology against both node and link removal. It can be observed in Fig. 10 that it gradually receives lower values for all networks.

The concept of efficiency of a network has been established as a measure of how efficiently it exchanges information [18]. It is similar to the distance and is the averaged sum of the reciprocal (multiplicative inverse) of the distances. Great

NOC/OC&I 2013, ISBN: 978-1-4673-5822-4

values of efficiency, point to great network robustness. In Fig. 11, it is seen that efficiency slowly decreases over time.

Considering the normalized betweenness centrality [19], it derives by dividing the maximum betweenness centrality by the average betweenness centrality for a network. Betweenness centrality quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. This normalized metric is indicative of the hierarchy of the network and higher values indicate an increased vulnerability of targeted failures. Its behavior may be considered unchanging over time, with the exception of *CESNET* network, as seen in Fig. 12.

The entropy of a graph is interpreted as its structural information content and serves as a complexity measure [20]. It provides an average measure of network's heterogeneity, since it measures the diversity of the link distribution. Smaller values of entropy specify networks that are likely to be more robust. Fig. 13 depicts that all networks increase their entropy to one extent or another.

Average two-terminal reliability (ATTR) metric is the probability that a randomly chosen pair of nodes remains connected after a failure [21]. It is the sum over the number of node pairs in the connected component divided by the total number of node pairs in the network. This ratio gives the fraction of node pairs that are connected to each other. Therefore, the higher the value (for a given node percentage removed, i.e., here 10%), the more robust the network is in response to a failure that affects the same number of nodes. Two methods are applied for node removal; the targeted attack which removes the high-degree nodes and the random failure that randomly removes nodes. In Fig. 14 and Fig. 15, both methods are found to leave almost unchanged the ATTR metric.

The symmetry ratio is the ratio of the number of distinct eigenvalues of the network to the network diameter (actually, plus one in the denominator) [7]. Low symmetry values lessen the impact of losing a node. Thus, low values indicate more robust networks. In Fig. 16, symmetry ratio is growing over time.

The notion of effective graph resistance is derived from the field of electric circuit analysis where it is defined as the accumulated effective resistance between all pairs of nodes [8]. It intuitively measures the presence and quality of back-up path possibilities. The smaller the effective graph resistance, the more robust the network. However, this metric is shown in Fig. 17 to take higher values as the time passes.

The natural connectivity characterizes the redundancy of alternative paths by quantifying the weighted number of closed walks of all lengths [9]. The theoretical motivation of this measure arises from the fact that the robustness of a network comes from the redundancy of alternative paths. The higher the value of natural connectivity, the more robust the network. Indeed, in Fig. 18 all networks increase their natural connectivity over time.

Percolation threshold [10] is actually the critical fraction of nodes that need to be removed before the network disconnects. A high percolation threshold indicates a high fraction of nodes

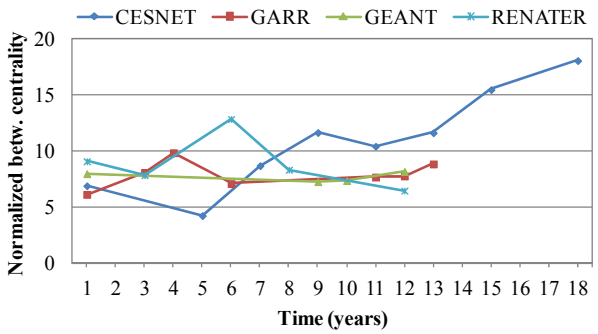


Fig. 12. Normalized betweenness centrality over time.

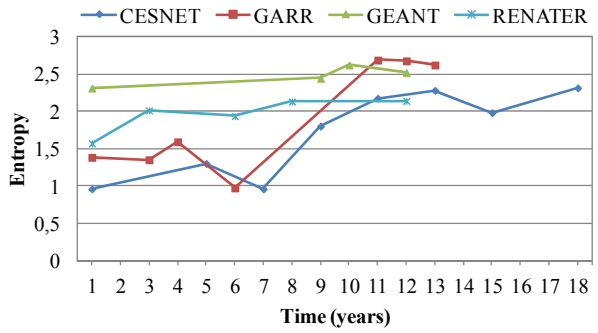


Fig. 13. Entropy over time.

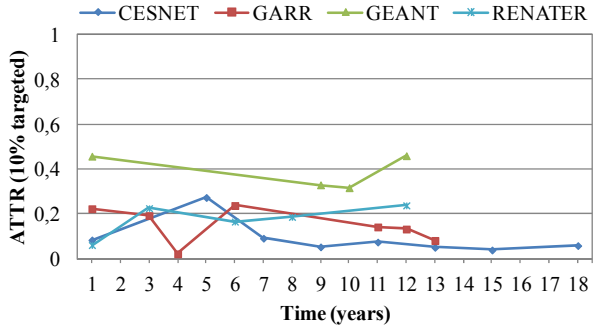


Fig. 14. ATTR – targeted (removal of 10% targeted nodes) over time.

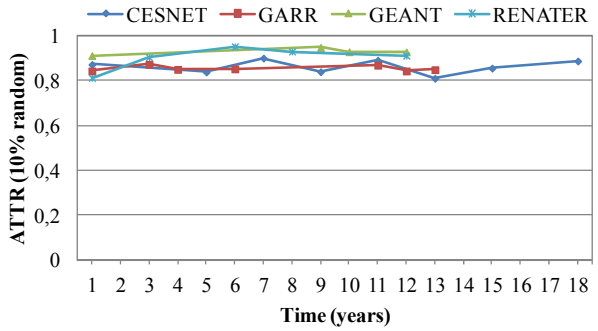


Fig. 15. ATTR – random (removal of 10% random nodes) over time.

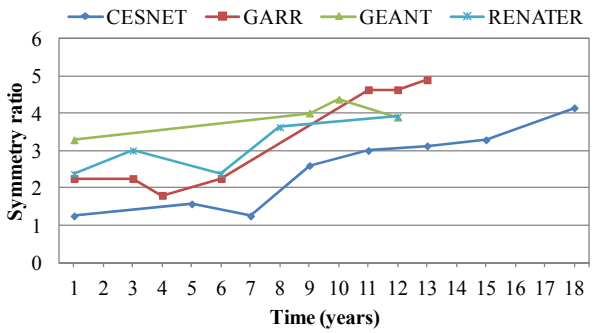


Fig. 16. Symmetry ratio over time.

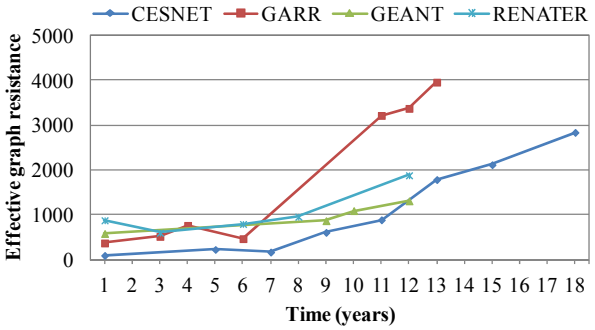


Fig. 17. Effective graph resistance over time.

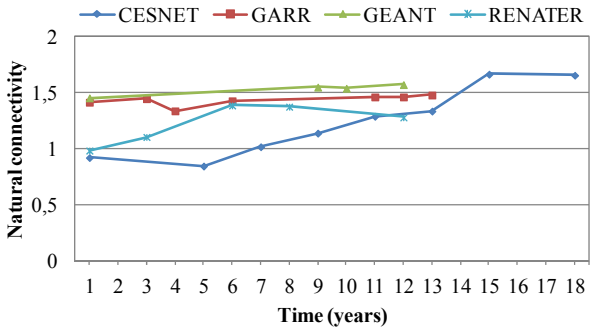


Fig. 18. Natural connectivity over time.

that can be removed without problems, which means the network is more robust. According to Fig. 19, the percolation threshold can be regarded as approximately unchanging over time.

Heterogeneity is the standard deviation of the mean degree divided by the mean degree [11]. The lower the magnitude of its heterogeneity, the greater the robustness of the topology. It can be seen in Fig. 20 that heterogeneity is roughly unchanging over time.

Average neighbor connectivity provides information about 1-hop neighborhoods around a node. It is calculated as the average neighbor degree of the average k-degree node [13]. Higher values of average neighbor connectivity indicate higher robustness. With the exception of *CESNET* network, this metric may be considered as unchanging over time, as observed in Fig. 21.

Node connectivity represents the smallest number of nodes whose removal results in a disconnected or single-node graph [12]. Thus, higher values mean higher robustness. In Fig. 22, this metric appears unchanging over time.

Similarly, edge connectivity represents the smallest number of edges whose removal consequences in a disconnected or single-node graph [12]. In the same way as node connectivity, higher values represent higher robustness. Also, in Fig. 23 this metric turns out to be time-invariant. Of course, in star-like networks as those presented here, node and edge connectivity will always be one, since there is actually only one node and link disjoint path from the farthest node in the hierarchy to each other. This fact in conjunction with the observed high diameters makes topologies not particularly robust.

C. *Discussion of results*

There are many similarities in the robustness evolution between the different networks that allow for a classification of the robustness metrics (Table II). The evaluated features may be discriminated in unchanging features that stay constant over time, and in changing features that exhibit distinct changes over time. It is worth noting that almost half of the considered measures are time-invariant measures, thus their evaluation could be conducted using single snapshots of the topology. However, for the changing features, robustness appears to be dynamic in time and one robust network may be less robust in

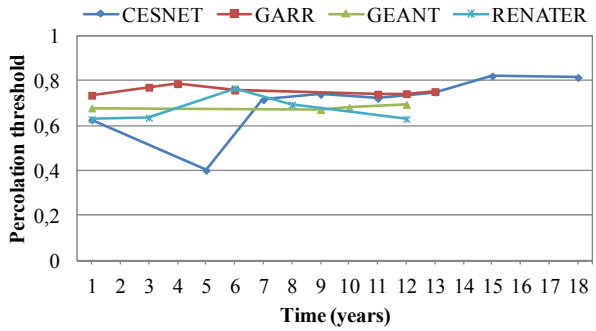


Fig. 19. Percolation threshold over time.

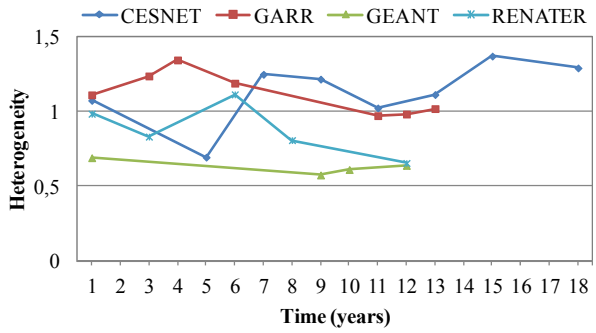


Fig. 20. Heterogeneity over time.

NOC/OC&I 2013, ISBN: 978-1-4673-5822-4

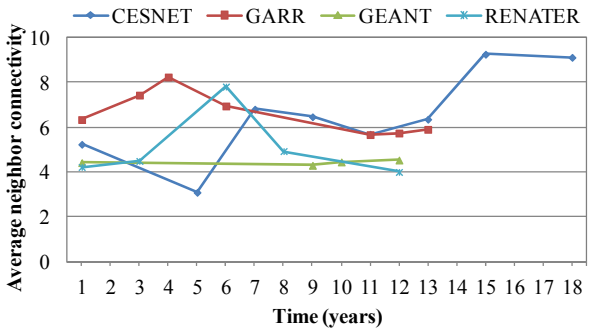


Fig. 21. Average neighbor connectivity over time.

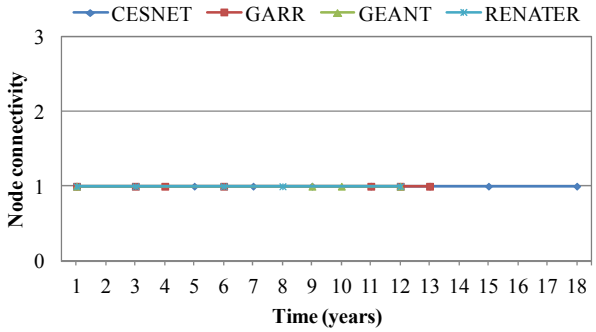


Fig. 22. Node connectivity over time.

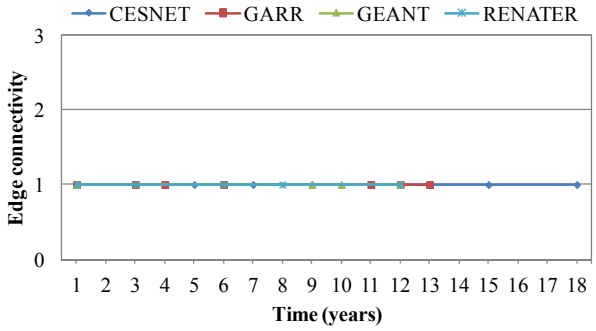


Fig. 23. Edge connectivity over time.

subsequent periods.

Besides, it is obvious that not all of the changing features are pointing in the same direction. For example, in our dataset, average clustering coefficient, assortativity coefficient, vulnerability and natural connectivity demonstrate improvement, while other measures appear to worsen over time. It seems as if backbone networks have been designed to be more efficient in response to these specific kinds of robustness. Interconnection with neighbors, as derived by the average clustering coefficient and redundancy of alternative paths, as derived by the natural connectivity, emerge as the network engineers' priorities in the backbone design. Results also indicate that links more and more connect nodes of similar degrees; the backbone configurations are gradually changing from disassortative networks to assortative networks, confirming the popularity of ring-based topologies in the backbone. The vulnerability metric, as an indicator of response of the topology subject to attacks on nodes and edges, is as well observed to always be improved over time.

Beyond improvements, it is surprising to discover that some well-recognized metrics are getting worse. For example, the average distance between nodes appears increasing, in contrast to the literature findings that it often shrinks over time [15]. This is probably due to the fact that in backbones all nodes from the beginning of the observation belong to only one connected component, which is rare enough in other real-world networks. Moreover, contradictory outputs are obtained by the measurements of algebraic connectivity which show that no great attention is paid to the difficulty to cut the network into independent components. The decrease in the efficiency metric is in accordance to the increase in the average distance between nodes, and this may be explainable as most studied networks are in their early growth stage. The robustness deterioration caused by the entropy increase probably presents the engineers' low priority on balanced link distribution. As well, the observed high symmetry ratio (low symmetric networks) and high effective graph resistance indicate that there are obstacles or low intention to achieve a departure from random topologies and in the same time to retain good back-up path possibilities.

Although the results may not generalize beyond these networks, they represent a case study and a first attempt to

TABLE II. OBSERVED TRENDS OF ROBUSTNESS METRICS

Topological Robustness metric	*Trend over time*
Mean degree	unchanging
Average shortest path	worsening
Diameter	worsening
Average clustering coefficient	improving
Assortativity coefficient	improving
Vulnerability	improving
Algebraic connectivity	worsening
Efficiency	worsening
Normalized betweenness centrality	unchanging
Entropy	worsening
Average two-terminal reliability - targeted	unchanging
Average two-terminal reliability - random	unchanging
Symmetry ratio	worsening
Effective graph resistance	worsening
Natural connectivity	improving
Percolation threshold	unchanging
Heterogeneity	unchanging
Average neighbor connectivity	unchanging
Node connectivity	unchanging
Edge connectivity	unchanging

perform extensive graph-based robustness analysis over time. There are biases in the collection methodology since networks are samples of published academic networks that satisfy the data availability over time. So, the results here are descriptive rather than representative, but nevertheless provide some insights on the way the fundamental network robustness properties vary with time.

IV. CONCLUSIONS

In this paper a robustness analysis over time of four real telecommunication networks has been carried and several well-known robustness metrics have been considered.

It is surprising to find, based on the growth patterns of these networks, that only about half of the regarded measures have changed over the past years, even though the number of their nodes and edges has tripled on average during this time period. Regarding the measures that do change, not all of them are pointing in the same direction. For example, average clustering coefficient, assortativity coefficient, vulnerability and natural connectivity exhibit improvement, while many other measures appear to worsen over time. Besides, caution is needed for the interpretation of the trends on the metrics which may appear conflicting e.g., existence of alternative paths appears improving in terms of average clustering coefficient but worsening in terms of effective graph resistance. The above results indicate the importance of evaluating real networks and models against a wide variety of measures rather than relying on a single metric, and evidently over time. Network modeling efforts will need to incorporate mechanisms that handle such changing dynamics. Results also have potential application in various settings, including forecasting of time-varying network parameters, in anomaly detection on networks, and in creating realistic network generators.

In terms of future work, it would be interesting to further examine the robustness metrics for which the robustness is found to degrade over time. Also, the consideration of data from commercial networks, for long time periods and at several network levels would allow for useful comparisons. Finally, a supplement of the present robustness evaluation is intended that will examine functional robustness and services performance, in a service discriminated approach (e.g., Video-on-Demand, Internet Protocol television, Peer-to-peer, etc.). This functional robustness, as the ability of the network to maintain its total throughput or at least minimize the traffic disruption [22], should take into account the functioning of the services offered. This may require a departure from the classic shortest path choices and consider more expedient algorithms, such as Suurballe's algorithm [23].

REFERENCES

[1] European Commission Information Society and Media Directorate-General, "Availability and Robustness of Electronic Communications Infrastructures - The 'ARECI' Study - Final report," 2007, pp. 1-149.

[2] Council of the European Union, "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," Official Journal of the European Union, 2008, pp. L 345/375-382.

[3] A.-L. Barabási and Z.N. Oltvai, "Network biology: understanding the cell's functional organization," Nature Reviews Genetics, vol. 5, pp. 101-113, 2004.

[4] J.P. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, vol. 54, pp. 1245-1265, 2010.

[5] A. Jamakovic and S. Uhlig, "Influence of the network structure on robustness," 15th IEEE International Conference on Networks (ICON), pp. 278-283, 2007.

[6] R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, and M. Romance, "Effective measurement of network vulnerability under random and intentional attacks," Journal of Mathematical Modelling and Algorithms, vol. 4, pp. 307-316, 2005.

[7] A.H. Dekker and B. Colbert, "The symmetry ratio of a network," in Proceedings of the 2005 Australasian Symposium on Theory of Computing, vol. 41, pp. 13-20, 2005.

[8] W. Ellens, F. Spieksma, P. Van Mieghem, A. Jamakovic, and R. Kooij, "Effective graph resistance," Linear Algebra and its Applications, vol. 435, pp. 2491-2506, 2011.

[9] J. Wu, Y.-J. Tan, H.-Z. Deng, Y. Li, B. Liu, and X. Lv, "Spectral measure of robustness in complex networks," arXiv preprint arXiv:0802.2564, 2008.

[10] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," Physical Review Letters, vol. 85, pp. 4626-4628, 2000.

[11] J. Dong and S. Horvath, "Understanding network concepts in modules," BMC Systems Biology, vol. 1, p. 24, 2007.

[12] A.H. Dekker and B.D. Colbert, "Network robustness and graph topology," in Proceedings of the 27th Australasian Conference on Computer Science, vol. 26, pp. 359-368, 2004.

[13] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, and A. Vahdat, "The Internet AS-level topology: three data sources and one definitive metric," ACM SIGCOMM Computer Communication Review, vol. 36, pp. 17-26, 2006.

[14] M. Manzano, J. Marzo, E. Calle, and A. Manolovay, "Robustness analysis of real network topologies under multiple failure scenarios," 17th European Conference on Networks and Optical Communications (NOC), pp. 1-6, 2012.

[15] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: densification laws, shrinking diameters and possible explanations," in Proceedings of the eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, pp. 177-187, 2005.

[16] V. Rosato and F. Tiriticco, "Growth mechanisms of the AS-level Internet network," EPL (EuroPhysics Letters), vol. 66, pp. 471-477, 2007.

[17] M.E. Newman, "The structure and function of complex networks," SIAM review, vol. 45, pp. 167-256, 2003.

[18] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," Physical Review Letters, vol. 87, pp. 198701-198704, 2001.

[19] S. Knight, H.X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The Internet topology zoo," Journal on Selected Areas in Communications, IEEE, vol. 29, pp. 1765-1775, 2011.

[20] R. Solé and S. Valverde, "Information theory of complex networks: On evolution and architectural constraints," Complex Networks, pp. 189-207, 2004.

[21] T.B. Brecht and C.J. Colbourn, "Lower bounds on two-terminal network reliability," Discrete Applied Mathematics, vol. 21, pp. 185-198, 1988.

[22] A. Sydney, C. Scoglio, P. Schumm, and R. Kooij, "Elasticity: topological characterization of robustness in complex networks," in Proceedings of the 3rd International Conference on Bio-Inspired Models of Network, Information and Computing Sytems (BIONETICS), 2008.

[23] J.W. Suurballe and R.E. Tarjan, "A quick method for finding shortest pairs of disjoint paths," Networks, vol. 14, pp. 325-336, 1984.