Quantitative and Qualitative Network Robustness Analysis Under Different Multiple Failure Scenarios

M. Manzano
Institute of Informatics
and Applications (IIiA)
University of Girona, Girona, Spain
Email: mmanzano@eia.udg.edu

E. Calle
Institute of Informatics
and Applications (IIiA)
University of Girona, Girona, Spain
Email: eusebi@eia.udg.edu

D. Harle
Department of Electronic
& Electrical Engineering (EEE)
University of Strathclyde, Glasgow, U.K.
Email: d.harle@eee.strath.ac.uk

***Abstract*—Society depends now more strongly than ever on large-scale networks. Failures of great significance have occurred in the last years. Thus, it has become of vital importance to define robustness metrics. Classical robustness analysis has been focused on the evaluation of topological characteristics. In this paper we extend this analysis introducing two new robustness metrics that include traffic service requirements: *QuaNtitative Robustness Metric* (QNRM) and *QuaLitative Robustness Metric* (QLRM). A review of some well known graph robustness metrics is provided. In order to compare these metrics with the proposals, a set of six topologies (random, small-world and scale-free) is evaluated. Finally, it is shown that our two new metrics are able to evaluate the performance of a network under a given kind of impairment.**

***Index Terms*—Complex networks, Impairments, Robustness metrics.**

I. Introduction

Large-scale networks supporting the provision of telecommunication, electrical power, rail and fuel distribution services underpin and fulfill keys aspects of modern day living; often their ubiquity is taken for granted. These critical infrastructure networks essentially consist of *nodes* (railway stations, transformers, switches, etc.), *links* (tracks, pipes, cables, etc.) and *dynamic processes* that run over them (trains, oil or gas, electrical power, connections, etc.). This paper considers three different kind of topologies, all of them related to *complex networks* (networks with non trivial topological features): *random*, *small-world* and *scale-free*. Random networks are a primitive and crude representation of such complex networks whereby nodes are randomly connected such that the variance in nodal degree is relatively small. In small-world networks, although the majority of nodes have a limited number of direct neighbours, most can be reached via only a small number of hops. In scale-free networks, the topology is such that some vertices, known as hubs, have a degree that is orders of magnitude larger than the average.

Recently, network failures of great significance have occurred, re-enforcing the need to take the possibility of such large and potentially catastrophic failures into consideration in the underlying network design. The largest and most widespread power outage in history happened across Java and Bali in 2005, affecting some 100 million people, again as consequence of cascade failures [1]. The 2006 earthquake in Taiwan disrupted undersea fibre optic lines and, as a result, banks from South Korea to Australia suffered significant interruptions [2]. In 2009, a major failure in the power supply network of Brazil and Paraguay, left around 87 million residents without power for almost 5 hours [3]. Finally, in 2010 a heavy snowfall in Spain caused a fault in a high tension power cable left 220,000 people in and around the Catalonian city of Girona without electricity. [4]. It is clear that considerable proportions of the world's population could be seriously damaged if a large network experiences significant failures. It is therefore crucial to be able to quantify the network robustness in a reliable manner while taking into account the dynamic processes supported by such networks. In communication networks, a dynamic process refers to a service (*connection*) provided by the network.

Because the underlying networks impact directly on the provisioning, performance and management of any given service, engineers are confronted with fundamental questions such as "how to evaluate the robustness of networks for a given service?" or "how to design a robust network appropriate to the needs of supported services?".

A well known definition for robustness is: *a network is robust if disconnecting components is difficult*. In this work we assume the definition of robustness given in [5]: *is the ability of a network to maintain its total throughput under node and link removal*. The former definition comes from the *classical approach* where basic concepts from graph theory are used. The latter comes from a more *contemporary approach* that considers services running over the network in order to evaluate its robustness.

Between the classical and the contemporary, a wide range of approaches have analyzed the robustness of a network. These have evolved from the earlier approaches that focus mainly on the connectivity of a graph to more recent concepts that consider the spectrum of a graph. Generally, the metrics to compute the robustness of a network, based on graph topological features do not take into account the functioning of a service. Thus, we define two new metrics that do consider, under defined impairments or multiple failures, the impact upon individual services.

Therefore, the aim of this paper is:

1) Analysis and review of several graph robustness metrics.

978-963-8111-77-7

2) Define two new metrics: QuaNtitative Robustness Metric (QNRM) and QuaLitative Robustness Metric (QLRM).
3) Provide a Case study for the use of such metrics based upon a range of topology types.

The paper is structured as follows. Section II provides a classification of the network impairments considered in this work. Section III provides: a background of some well known robustness metrics, defines these metrics and presents our two new metrics (QNRM and QLRM). Section IV then describes the case study considered in this work. Finally, we provide the conclusions of this work and we give some outlines issues that could be considered as future work, in Section V.

II. Network Impairments

The robustness of a network does depend on the type of impairment that occurs. From here on, the term *impairment* refers to any kind of attack, multiple or cascading failures that can occur within a network (it does not refer to physical layer impairments). Several taxonomies have been proposed in order to classify network attacks; specifically within communication networks [6] [7]. Consequently, the discussion presented here simplifies such previous categorizations and focuses on classifying the types of impairments that can occur on the nodes of a network.

A. Static

Static impairments are essentially one-off attacks that affect one or more nodes at any given point. There are, in essence, two forms of static impairments:

1) Random (SR (Static Random)): In the SR case, nodal attacks occur indiscriminately selecting nodes at random.

2) Target (ST (Static Target)): Nodes in an ST attack are chosen in order to maximize the effect of that attack; there is an element of discrimination in the impairment. The choice of attack target may be a function of network-defined features such as nodal degree, between-ness centrality or clustering, as well as other "real-world" features, such as the number of users potentially affected and socio-political and economic considerations.

B. Dynamic

This second type of failures (commonly related to multiple failures such as cascading failures) has a temporal dimension. Two types are defined:

1) Epidemical (DE (Dynamic Epidemical)): Based on epidemic models (EM), there are several forms such as *Susceptible-Infected* (SI) or *Susceptible-Infected-Susceptible* (SIS). Considering a DE, a failure occurs in a node (or a set of nodes of the network) and the failure can spread through the network (becoming an epidemic) or not. The rise and decline in epidemic prevalence of an infectious disease (or failure) is a probability phenomenon dependent upon the transfer of an effective dose of the infectious agent from an infected individual to a susceptible one [8].

2) Periodical (DP (Dynamic Periodical)): A DP is, simply, any kind of impairment that occurs periodically following its characteristic cycle.

III. Metrics of Robustness

In this section, firstly, in III-A, we discuss the general background that underpins the use of metrics of robustness. Secondly, in III-B, we give a brief definition of such metrics. Finally, we propose two new metrics of robustness: QNRM and QLRM.

A. Background

Several topology features are considered in the classical approach which is based upon basic concepts of graph theory: these include average nodal degree, node connectivity [9], heterogeneity [10], symmetry ratio [11], diameter, average shortest path length [12], average neighbor connectivity [13] and the assortativity coefficient [13].

Moreover, in a more contemporary approach, other metrics in networking literature were introduced; including the largest eigenvalue [13] [14], the second smallest laplacian eigenvalue [15] and the so-called average two-terminal reliability [16].

The set of metrics presented in this section is defined in more detail in III-B. None of these metrics matches completely with the advanced concept of robustness that we consider in this paper.

B. Topology characteristics

1) Average nodal degree ($\overline{k}$) : This is the coarsest connectivity feature of any topology. Networks with higher $\overline{k}$ are "better-connected" on average, and, consequently, are likely to be more robust. On one hand, "more robust" means that there are more chances to establish new connections. However, if a node with a high nodal degree fails, potential higher numbers of connections are also prone to be affected. Thus, this metric by itself provides only a limited measure of the robustness of a network which is likely to vary depending on how the nodal degree is actually distributed over the graph.

2) Node connectivity: This metric represents the smallest number of nodes whose removal results in a disconnected or single-node graph. Moreover, connectivity can also be defined as the smallest number of node-distinct paths between any two nodes [9]. This metric gives a crude indication of the robustness of a network in response to any of the impairments defined in Section II.

3) Heterogeneity: Heterogeneity is the standard deviation of the average nodal degree divided by the average nodal degree [10]. In Sydney et al. [17] a range of different attacks (SR and ST) are invoked over a variety of networks, and it can be observed that heterogeneous networks are likely to be more robust. The lower the magnitude of its heterogeneity, the greater the robustness of the topology.

4) Symmetry ratio: This ratio is essentially the quotient between the number of distinct eigenvalues (obtained from the adjacency matrix of the network) of the network and the network diameter. Therefore, on high-symmetry networks, with symmetry values between 1 and 3, the impact of losing a node does not depend on which node is lost, what means that networks perform equally in response to a random (SR) or a target attack (ST) [11]. Random networks do not have, in

general, high symmetry values. However, for random graphs, where nodes are of equal importance in a statistical sense: since links are placed randomly, no node is privileged by design. This condition can not be applied to small-world or scale-free networks.

5) Diameter: The diameter is, like the average nodal degree, another coarse robustness metric of a network. It is the longest of all the shortest paths between pairs of nodes. In general, one would wish the diameter of networks to be low. Scale-free networks generally have small diameters, but are not particularly robust in response to deliberate attacks (ST), due to their relatively low value of node connectivity. Nonetheless, small-world networks represent a combination of the advantages of the properties of random networks (where no node is privileged by design) and scale-free networks (where there is a low diameter).

6) Average shortest path length: Average shortest path length (ASPL) is calculated as an average of all the shortest paths between all the possible origin-destination node pairs of the network. Networks with small ASPL are more robust because, in response to any kind of impairment (SR, ST, DE or DP), they are likely to lose fewer connections.

7) Largest eigenvalue (λ): Most networks with high values for the largest eigenvalue have a small diameter and are more robust. In general, networks with larger eigenvalues have more node and link disjoint paths to choose from. Therefore, this metric provides bounds on network robustness with respect to both link and node removals [13]. This metric is also associated in defining the *epidemic threshold* of a network, which correlates with the severity of an epidemic failure (DE) on a network [14].

8) Second smallest laplacian eigenvalue (λ_2): This metric, also known as *algebraic connectivity*, measures how difficult it is to break the network into islands or individual components. The larger the λ_2, the greater the robustness of a topology against both node and link removal [15].

9) Average neighbor connectivity: This metric provides information about 1-hop neighborhoods around a node. It is a summary statistic of the *Joint degree distribution (JDD)* and it is simply calculated as the average neighbor degree of the average *k*-degree node [13].

10) Assortativity coefficient (r): The assortativity coefficient r, can take values between $-1 \leq r \leq 1$. When $r < 0$ 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 static random and targeted attacks (SR and ST). The opposite properties apply to *assortative* networks with $r > 0$ that have an excess of links connecting nodes of similar degrees [13].

11) Average two-terminal reliability (A2TR): This metric is the probability that a randomly chosen pair of nodes is connected. If the network is fully connected the value of A2TR is 1. Otherwise, it is the sum over the number of node pairs in every 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 number of nodes removed), the more robust the network is in response to an static random attack (SR) that affects the same number of nodes [16].

C. Quantitative and Qualitative Robustness Metrics

Two new robustness metrics are now proposed, which capture the definition given in this paper for robustness and both define key aspects of the services (in our case *connections*) that run over a network. Services can be classified according to different Quality of Service (QoS) parameters, such as: delay, jitter, packet loss, etc. Network failures some, if not all, of these parameters resulting in revised QoS levels. Moreover, from the network operator perspective, failures also affect to the number of established and future connection demands. Considering both aspects (quantity and quality) two new metrics are proposed to evaluate how network services could be affected after different multiple failure scenarios. On one hand, and in order to simplify, the *QuaLitative Robustness Metric* (QLRM) quantifies variations in the average path length of established connections, reflecting that many key QoS parameters are functions of path length (delays, packet loss, etc.). On the other hand, the *QuaNtitative Robustness Metric* (QNRM) evaluates the number of blocked connections.

1) QuaNtitative Robustness Metric: The *QuaNtitative Robustness Metric* or QNRM analyses how an impairment of any kind (SR, ST, DE or DP) affects the number of connections established on a network. In this metric, the number of *Blocked Connections (BC)* in each time step are analyzed. We define a BC as a connection that should have been established at time t but could not be established as a consequence of nodal failures.

Define $BC(t)$ as the number of BC in a given time step, $TTC(t)$ as the number of connections that should have been established in the same time step and $Total$ as the maximum number of time steps. In order to compare different topologies that may not have the same number of $TTC(t)$ in each time step, we compute our metric, in each time step t, with the quotient shown in the following equation:

$$QNRM(t) = \frac{BC(t)}{TTC(t)} \tag{1}$$

Finally, we calculate the average of all values obtained during the interval of interest:

$$QNRM = \frac{\sum_{t=1}^{Total} QNRM(t)}{Total} \tag{2}$$

2) QuaLitative Robustness Metric: The *QuaLitative Robustness Metric* or QLRM analyses how the quality of service on a network varies, when any kind of impairment (SR, ST, DE or DP) occurs. This metric measures the *average shortest path length (ASPL)* in each time step. In contrast to QNRM, QLRM evaluates the *Established Connections (EC)*.

In order to compare the QLRM for different topologies the values obtained from the *average shortest path length (ASPL)* are normalized. Define $U(ASPL)$ as the quotient of the *standard deviation* of the ASPL of the topology and

its ASPL. Also define $U(KoI)$ as the same quotient, but calculated when any *Kind of Impairment* has occurred in the network (and the ASPL has been affected). Then, this metric is defined as follows:

$$QLRM = \frac{U(ASPL)}{U(KoI)} \tag{3}$$

The metric is calculated by normalizing the values with the standard deviations obtained because, the magnitude of increase or decrease of the ASPL of a topology in response to an impairment is not of prime importance for this metric, but rather its variation. With this value we are able to determine the deterioration of the QoS of a network when an impairment occurs, compared to the QoS that the unimpaired network should normally provide.

IV. Case Study

In this section, we choose six different topologies as exemplars to review the metrics defined in the previous section and to compare the previously defined metrics from the literature with the two proposed in this paper.

The rest of this section is structured as follows: in IV-A, we characterize a set of six exemplar topologies with the metrics described in III-B. Furthermore, in IV-B we define a simulation scenario in order to calculate the two new metrics of robustness presented in this work. Finally, in IV-C, first we provide a robustness ranking of the six networks regarding to the graph robustness metrics. Secondly, we show and analyze the results obtained from the simulations.

A. Topologies

The six topologies analyzed in this paper are presented below and their key characteristics are listed in Table I. Topologies have been proposed to show different characteristics in terms of diameter and average node degree. The random networks have been obtained using the Erdős-Rènyi model [18], small-world using the Watts and Strogatz model [19] and scale-free ones using the Barabási-Albert (BA) model [20]. The two random networks are the ones that start with *er-*, while the small-world and scale-free networks are indicated by the *sw-* and *sf-* prefixes respectively.

B. Simulation Scenario

In order to calculate our metrics of robustness, the simulation scenario must be detailed. All the simulations last for 10000 time steps with a traffic load of 80000 connections in total. Source and destination of the connections have been selected randomly and with the restriction that they cannot be adjacent (connections are a minimum of two hops). There is no restriction in link capacity so if there are no failures, all the connections are accepted. The generation of the connections and their duration follows negative exponential distributions with average inter-arrival and holding times of 0.12 and 100 time steps respectively.

Simulations causing the following impairments are carried out:

- SR: A static random attack that affects the 20% of nodes of the network is activated at the start of the simulation.
- DE: The *Susceptible-Infected-Disabled* (SID) epidemic model [21], previously presented by the authors of this work, will be used in this case study. A dynamic epidemic failure that initially affects the 3% of nodes of the network is activated at the start of the simulation, reaching a total of 20% of nodes affected after a period of time (this period is different for each topology and depends upon its specific topological features).

Then, we are able to obtain results showing how the set of exemplar topologies performs in response to either a static random attack (SR) or a dynamic epidemic failure (DE), when both affect the same number of nodes.

C. Results

The results of the case study are presented over. First, a ranking of the topologies based around the traditional robustness metrics is listed. Secondly, the simulation results are provided in order to analyze and compare them with the grades obtained from the graph robustness metrics.

In Table II the classification based on the features of the topologies of IV-A can be observed. In this classification, *1* represents the most robust with increasing rank representing successively reduced robustness. The last row indicates the global ranking of the topologies and is the simple unweighted average of the positions of the previous rankings of each topology.

As it can be seen in Table II, the ranking of the *average two-terminal reliability* is provided. This ranking has been obtained from Fig. 1, which shows how the reliability of the set of topologies evolves when nodes are removed from the network. It is important to note that the *average nodal degree* ranks the topologies as A2TR does. Furthermore, the rankings in Table II are based on topological features of the networks.

On the third row, topologies are ranked by their *node connectivity*. As expected, scale-free networks can be disconnected by removal of just one node. It is interesting to note that, according to the *node connectivity*, the random topologies have the same performance as the scale-free networks. Regarding the *largest eigenvalue*, *sw400d20* is the most robust topology, indicating that, under an epidemic failure (DE), this network performs better than the others. Thereafter, rankings of the *average shortest path length* and the *second smallest laplacian eigenvalue* show interesting results: although *sw400d20* is the most robust, there is no match in the 2^{nd}, 3^{rd} and 4^{th} most robust topologies. The following two rows show the classification based on the *average network connectivity* and on the *assortativity coefficient*. The small-world pair are the most robust, implying that these two networks are less vulnerable under any kind of static impairments (SR or ST).

Finally, the classification regarding to the *symmetry ratio* is shown. In this case, it can observed that the two topologies with less *average nodal degree* are the ones that are more symmetric (and more robust). However, later on we show that, contrarily, these two topologies are highly affected by

TABLE I
CHARACTERISTICS OF THE NETWORK TOPOLOGIES

Characteristic	er400d3	er400d6	sw400d10	sw400d20	sf400d2	sf400d4
Number of nodes	400	400	400	400	400	400
Number of links	618	1205	1996	3975	399	789
Average nodal degree (AND)	3.00	6.03	9.98	19.88	2	3.95
Stdev	1.67748	2.43705	0.97569	1.34867	1.87584	3.69135
Minimum nodal degree	1	1	6	15	1	1
Node connectivity (NC)	1	1	6	15	1	1
Heterogeneity	0.5591	0.4041	0.0977	0.0678	0.9379	0.9345
Symmetry ratio	30.7692	50	57.1428	66.6666	20.6842	50
Diameter	12	7	6	5	18	7
Average shortest path length	5.48	3.56	3.75	2.79	7.28	3.91
Stdev	1.5046	0.86358	0.97115	0.67285	2.38783	0.94979
Largest eigenvalue	4.1158	7.1677	10.10778	20.002101	4.513222	8.343718
Second smallest laplacian eigenvalue	0.11025	0.518127	0.635512	1.657585	0.003921	0.527415
Clustering coefficient	0.2000	0.0512	0.48678	0.53384	0.615	0.03033
Assortativity coefficient	-0.14419	-0.00079	0.00888	0.01585	-0.08945	-0.03827
Average neighbor connectivity	0.0011134	0.0012546	0.0031563	0.0045491	0.0007238	0.0010290
Degree distribution $P(k)$	-	-	-	-	$\sim k^{-3.006345}$	$\sim k^{-2.949767}$

TABLE II
RANKING OF ROBUSTNESS, BASED ON TOPOLOGY FEATURES

	er400d3	er400d6	sw400d10	sw400d20	sf400d2	sf400d4
Average two-terminal reliability (Fig. 1)	5	3	2	1	6	4
Average nodal degree	5	3	2	1	6	4
Node connectivity	3	3	2	1	3	3
Heterogeneity	4	3	2	1	6	5
Largest eigenvalue	6	4	2	1	5	3
Average shortest path length	5	2	3	1	6	4
Second smallest laplacian Eigenvalue	5	4	2	1	6	3
Average neighbor connectivity	4	3	2	1	6	5
Assortativity coefficient	6	3	2	1	5	4
Symmetry ratio	2	3	4	5	1	3
Global Ranking	(4.5) 5	(3.1) 3	(2.3) 2	(1.4) 1	(5) 6	(3.8) 4

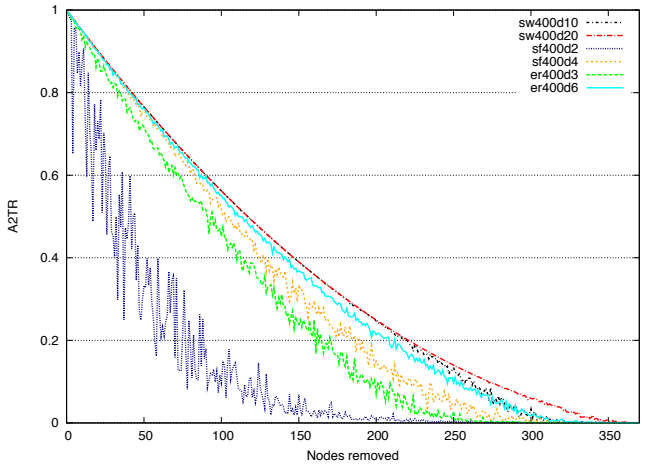

Fig. 1. Average Two-Terminal Reliability of the topologies

any kind of attack (SR and DE) in comparison with the other four exemplars. Thus, *symmetry ratio* would not be a suitable metric in relation to *low average nodal degree* networks.

To summarize the ranking provided in Table II, a global ranking has been calculated and listed in the last row. This final and summary ranking gives an approximation to the robustness of the networks considered in this case study considering the traditional robustness metrics which omit considerations about any connections on the network. Here, the two small-world are the most robust, followed by the random network *er400d6* and the scale-free *sf400d4*. Although the small-world *sw400d20* is ranked as the most robust, there is one metric that considers that this network would be less robust than the others (the *symmetry ratio*). In addition, some metrics differ in identifying the 2^{nd} and 3^{rd} most robust topologies. This means that one should really use a group of metrics to define the robustness rather than rely on any single graph robustness metric. Thus, considering several graph based robustness metrics becomes necessary when robustness of a network is to be analyzed, but such an approach would not be sufficient for a network provider, because it does not take into account the connections that run over a network and does not give any information about the service performance of a network under any kind of impairment.

The results of the simulations are presented further down. In Table III results associated with the QNRM metric can be observed. Table III is divided as follows: rows from 1 until 3 pertain to the behavior of the network in response to a SR impairment while from 4 until 6 pertain to the metric's value in response to an DE failure. The last two rows show the relation

between the DE and the SR in order to facilitate a comparison between the robustness of the networks when either a SR or a DE failure occurs.

As can be observed in Table III, regarding the SR impairment, the most robust topologies are the two small-world networks, followed by *sf400d4* and *er400d6*. The worst network in this scenario is *sf400d2* because it blocks almost the 80% of the connections that should be established. Nevertheless, it is interesting to note that, in response to a DE failure, the third most robust network is the *er400d6*, followed by *sf400d4*.

The last row shows a classification of the topologies sorted by the ratio calculated in the row above it. Then, *sw400d20* is the topology that shows the most improvement in its performance when comparing a SR and a DE failure; the number of blocked connections reducing to almost 50% when an epidemic failure (DE) occurs. Second (*er400d6*) and third (*sw400d10*) position networks have a ratio value extremely close to unity which means that they perform equitably in response to both kinds of impairments. The network where the number of blocked connections in response to an epidemic rises most, compared with a static random impairment, is *sf400d4*. This means that *sf400d4* is a network where the performance varies according to the kind of attack; a characteristic that may not be desirable for a telecommunications network supporting high levels of dynamic connections.

Furthermore, in Table IV results obtained for the QLRM metric are shown. Table IV is structured as follows: first two rows display the average shortest path length (ASPL) feature of each topology with their standard deviation, rows 3 until 6 are related to the robustness metric in response to a SR impairment. The four following rows are associated with the behaviour under a DE failure while the last two rows of the table shows the relation between the DE and the SR to allow a comparison of the robustness of the networks under either SR or DE failures.

The fifth row of Table IV shows the value of QLRM in response to a SR impairment. The ranking provided in the following row reveals that, when the quality of the service is assessed, *sw400d20* is the most robust network of the exemplar set. Networks *er400d6* and *sw400d10* have similar behavior, although the random network is slightly more robust than the small-world examplar. The worst network in terms of QLRM is *sf400d2* because it has the largest variation of the ASPL. It is interesting to note that *sf400d2* decreases its ASPL when a SR impairment occurs because, as can be seen in Table III, this network blocks almost the 80% of connections and establishes only *short-path-length* connections. The robustness characteristics of the exemplar set described in terms of QLRM is similar to the DE failure case (ninth row). The last two rows of Table IV show that (as with QNRM), *sf400d4* is the network that performs poorest when considering DE and SR impairments. It can also be observed that *sw400d20* is, again, the most robust network, and that *er400d6* or *sw400d10* have similar behavior.

Finally, it can be observed that the metrics shown in Table II represent a relatively simplistic approach to define the robustness of a network because the metrics do not take into account the connections that are running over the network. Therefore, the results shown in Table III and Table IV demonstrate that our metrics are able to define the robustness of a network, capturing the definition of robustness assumed in this paper. QNRM and QLRM are able to inform the network designer how the performance of the service would degrade in response to a particular type of impairment. Furthermore, in order to choose the topology when it is known how the functioning of a service would be affected, graph robustness metrics could be considered. Moreover, other kind of topological features (such as the number of links) could also be helpful for the network designer when cost of the network is of key importance.

V. Conclusions and Further Work

In this paper some well-known traditional graph robustness metrics are reviewed. As such metrics do not take into account services that run over a network, two new robustness metrics have been presented: *QuaNtitative Robustness Metric* or QNRM and *QuaLitative Robustness Metric* or QLRM. Moreover, it has been shown that our proposals are able to quantify the performance of a network under particular types of impairment.

In the Case study, a set of topologies has been defined: two random networks, two small-world and two scale-free. A ranking has been provided in order to classify this set of networks by their features related to robustness metrics. Nevertheless, although these metrics could be used to describe the robustness of a network, they are not capable of indicating how service operation can be affected under any kind of multiple failure scenario. Then, the set of topologies has been evaluated with the two proposed metrics (QNRM and QLRM), under static random attacks (SR) and dynamic epidemic failures (DE).

Results have shown that the proposed metrics are able to describe the robustness of a network under different impairments (in this case study: SR and DE). Further, results have also shown which topologies, from the set considered, are more robust under a specific attack: a network can perform differently depending on the impairment form. In summary, the two small-world network are the most robust. Nonetheless, *er400d6* and *sf400d4* could also be considered on specific cases. As it can be observed, the rankings provided by our metrics and the rankings of the graph robustness metrics are different. Therefore, the choice of most robust topologies should be done complementing the information provided by QNRM and QLRM with those provided by the graph robustness metrics. Furthermore, if the cost is taken into account when designing a network, some other features (such as the number of links) of the topologies could be considered.

For further work, more specific QoS parameters could be included in the QLRM metric, giving an improved evaluation of the QoS for the different network services. In addition, it could be interesting to evaluate a wider set of topologies in order to be able to further define what type of topology (random, small-world or scale-free) is more robust in response to a given kind of impairment. Further, it could be also

TABLE III
QUANTITATIVE ROBUSTNESS METRIC RESULTS

Impairment		er400d3	er400d6	sw400d10	sw400d20	sf400d2	sf400d4
Static Random (SR)	QNRM	0.4482	0.3682	0.3453	0.3437	0.7974	0.3592
	Standard Deviation	0.0002	0.0002	0.0004	0.0005	0.0004	0.0005
	Ranking	5	4	2	1	6	3
Dynamic Epidemic (DE)	QNRM	0.4863	0.3687	0.3502	0.1750	0.9148	0.4175
	Standard Deviation	0.0010	0.0007	0.0019	0.0004	0.0009	0.0014
	Ranking	5	3	2	1	6	4
	$\frac{QNRM_{DE}}{QNRM_{SR}}$	1.085	1.0011	1.0142	0.5090	1.1472	1.1622
	Ratio Ranking	4	2	3	1	5	6

TABLE IV
QUALITATIVE ROBUSTNESS METRIC RESULTS

Impairment		er400d3	er400d6	sw400d10	sw400d20	sf400d2	sf400d4
	ASPL	5.48	3.56	3.75	2.79	7.28	3.91
	Standard Deviation	1.5046	0.86358	0.97115	0.67285	2.38783	0.94979
Static Random (SR)	ASPL	6.283	3.818	4.191	3.021	5.818	4.251
	Standard Deviation	0.00032	0.00004	0.0001	0.00002	0.0018	0.00006
	QLRM	0.00019	0.00004	0.00009	0.00003	0.00094	0.00006
	Ranking	5	2	4	1	6	3
Dynamic Epidemic (DE)	ASPL	6.932	3.981	4.153	2.956	5.006	5.224
	Standard Deviation	0.0107	0.0004	0.001	0.00002	0.0532	0.0035
	QLRM	0.00562	0.00041	0.00093	0.00003	0.03240	0.00276
	Ranking	5	2	3	1	6	4
	Total ratio: $\frac{QLRM_{DE}}{QLRM_{SR}}$	30.3069	9.5905	10.0915	1.0219	34.3496	47.4684
	Ratio Ranking	4	2	3	1	5	6

interesting to evaluate the set of networks under static target (ST) and dynamic periodical (DP) failures. Moreover, some other metrics that consider connections running over a network could be contemplated [5] [22]. Finally, some recovery methods could be considered and the Quality of Resilience could be measured with the metric proposed in [23].

REFERENCES

[1] Donnan and Shawn, "Indonesian outage leaves 100m without electricity," *Financial Times*, 2005.

[2] ITPRO. http://www.itpro.co.uk/, 2006.

[3] A. Downie, "Brazil blackout raises more questions for the olympics," *Time*, 2009.

[4] Guardian. http://www.guardian.co.uk/, 2010.

[5] A. Sydney, C. M. Scoglio, P. Schumm, and R. E. Kooij, "Elasticity: Topological characterization of robustness in complex networks," *CoRR*, vol. abs/0811.4040, 2008.

[6] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security (COMPSEC)*, vol. 24, no. 1, pp. 31–43, 2005.

[7] S. Shiva, C. Simmons, C. Ellis, D. Dasgupta, S. Roy, and Wu, "AVOIDIT: A cyber attack taxonomy." University of Memphis, Tech. Rep., August, 2009.

[8] "Enc. britannica," *http://dictionary.reference.com/browse/epidemic*.

[9] A. H. Dekker and B. D. Colbert, "Network robustness and graph topology," in *Proceedings of the 27th Australasian conference on Computer science - Volume 26*, ser. ACSC '04. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2004, pp. 359–368.

[10] J. Dong and S. Horvath, "Understanding Network Concepts in Modules," *BMC Systems Biology*, vol. 1, no. 1, 2007.

[11] A. H. Dekker and B. Colbert, "The symmetry ratio of a network," in *Proceedings of the 2005 Australasian symposium on Theory of computing - Volume 41*, ser. CATS '05. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2005, pp. 13–20.

[12] C. Shannon and D. Moore, "The spread of the witty worm," *IEEE Security and Privacy*, vol. 2, pp. 46–50, 2004.

[13] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, k. c. claffy, and A. Vahdat, "The internet as-level topology: three data sources and one definitive metric," *SIGCOMM Comput. Commun. Rev.*, vol. 36, pp. 17–26, January 2006.

[14] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 4, pp. 1–26, 2008.

[15] A. Jamakovic and S. Uhlig, "Influence of the network structure on robustness," in *ICON*, 2007, pp. 278–283.

[16] S. Neumayer and E. Modiano, "Network reliability with geographically correlated failures," in *Proceedings of the 29th conference on Information communications*, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 1658–1666.

[17] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm, "Characterising the robustness of complex networks," *Int. J. Internet Technol. Secur. Syst.*, vol. 2, pp. 291–320, December 2010.

[18] B. Bollobas, *Random Graphs*, W. Fulton, A. Katok, F. Kirwan, P. Sarnak, B. Simon, and B. Totaro, Eds. Cambridge University Press, 2001.

[19] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, Jun. 1998.

[20] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, October 1999.

[21] E. Calle, J. Ripoll, J. Segovia, P. Vilà, and M. Manzano, "A multiple failure propagation model in gmpls-based networks," *IEEE Network*, vol. 24, pp. 17–22, November 2010.

[22] W. Molisz and J. Rak, "Impact of wdm network topology characteristics on the extent of failure losses," *13th International Conference on Transparent Optical Networks (ICTON)*, 2010.

[23] P. Cholda, J. Tapolcai, T. Cinkler, K. Wajda, and A. Jajszczyk, "Quality of resilience as a network reliability characterization tool," *Network, IEEE*, vol. 23, no. 2, pp. 11 –19, march 2009.