# A Framework for Computing Topological Network Robustness

P. Van Mieghem† , C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos and R. E. Kooij

***Abstract*— Currently, there does not seem to exist a commonly agreed definition of the robustness of a network, nor a framework to modify a network in order to meet some desired level of robustness. The goal of this article is to present a definition and a framework to *compute* topological network robustness.**

## I. Introduction

Any network may be regarded as possessing at least two crucial "features": a network topology or infrastructure and a service for which the network is designed or created. A *network topology* specifies how items, called nodes, are interconnected or related to other nodes by links. The network interconnection pattern, the network topology, can be represented by a graph $G$, consisting of $N$ nodes and $L$ links. Each link in $G$ can be further specified by a set of link weights that reflect attributes such as delay, packet loss, available capacity, distance, monetary cost, synchronization likelihood, trust and/or friendship level, etc.

The *network service* is more abstract and less clearly defined. In general, a service uses the network infrastructure to transport items between a group of nodes, possibly subject to some constraints. A service is specified by a protocol, consisting of the application (software executed at source and destination nodes) and of a network communication "engine". For example, in the Internet, a communication service such as email transports a message from a source node to a destination over the network topology. Other examples of services in complex networks are road transport, neuron transport in the brain, financial transactions on a stock market and news spreading in social networks.

Both the topology and service are usually time-variant and may have their own specific properties and requirements. Although a service is often designed independently of the topology, the end-to-end behavior of a service is influenced by the topology and a topology is most often designed to offer a certain service. There are more services possible over one topology as in the Internet (e.g. file transfer, email, webservices). Thus, in general, the duo of service and topology are not necessarily operating in some optimal way. We believe that a definition of network robustness needs to take both "planes", topology and service, into account.

Here, we interpret *network robustness* as a measure of the network's response to perturbations or challenges (such as failures or external attacks) imposed on the network. Establishing a more precise definition that can be computed is the purpose of this article. A computable measure for network robustness allows us to (a) compare different networks and (b) improve a network to achieve a desirable level of robustness. We ought to mention that the ambition to propose a framework for network robustness is currently "a bridge too far". The network service in particular seriously complicates a computable framework. For instance, we observe that a network that is very efficient in propagating information is, on the other hand, also quite vulnerable to virus or malware spread (that is "undesirable information"). This illustrates that opposite properties in services over a same topology may exist, at any rate, if "virus anti-spread" can be regarded as a service. The broad range of security services in any network are perhaps better regarded as "constraints[1]" to any efficient transport service of items, rather than as a service on its own. In what follows, we adopt this point of view because one hardly builds a network with "security" as the primary service. Apart from clear evaluation criteria of a network service and besides often contradictory service requirements, the robustness of a service may be interpreted differently by the service provider or network operator and by the customer or end-user. As a consequence, this paper proposes, prudently and in a limited way, a framework for *topological* network robustness, that is able, in principle, to take the services into account.

### A. State of the art

The huge complexity in communications networks (due to a multi-layer protocol suite, different aggregation levels, missing service metrics that adequately capture and define robustness properties, and a dynamically changing and uncertain topology) illustrates why, at present, a framework to compute network robustness is still lacking.

A wealth of procedures to evaluate and improve network robustness has been proposed over the last 50 years. A literature overview of the proposed frameworks for resilience (here called robustness) is presented by Cholda *et al.* [13]. The first approach to network robustness was in the context of network reliability [57], [56], [43], [33], primarily aiming at connectivity measures, both deterministic and probabilistic. Network nodes and links are weighted with failure (survival) probabilities and graph theoretic tools together with Boolean logic techniques are used to compute the connectivity between

†Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, P.O Box 5031, 2600 GA Delft, The Netherlands; *email*: P.F.A.VanMieghem@tudelft.nl

[1]Most functionalities (both software as hardware) to secure network services incur additional delay and consume additional network resources, such that they can be considered as limiting or constraining.

arbitrary network endpoints (terminal reliability) [57], [56], [43] and for the network as a whole (network reliability) [33]. The probability of a graph to remain connected after a number of network component failures is studied using graph percolation in [23], [46] and reliability polynomials in [12], [11]. Recently, attention has been given to the study of power law network's reliability [40], [27], [9], since Faloutsos *et al.* [21] showed that the degree distribution of the Internet topology follows a power law. Overall, reliability studies are a valuable tool to address the risk for network disconnectivity via stochastic models. However, reliability studies present two drawbacks. First, reliability studies are shown not to be optimal due to the irregular stress cycles of network elements [16]. Second, these studies ignore the multi-level service nature of networks.

Performance concerns, on the other hand, are explicitly treated in the performability framework, introduced by Meyer in [35]. The term *performability* was initially launched to cover a class of unified performance-reliability measures [35], but soon evolved to a more general theory and tools assessing the capability of systems to perform in the presence of faults [36]. Similar to our framework, performability studies have been trying to incorporate the impact of lower level system processes to higher-level application performance. Contrary to our framework, the emphasis of performability work is not on the network topology: higher levels of abstractions, modeled by stochastic Petri nets and Markovian chains, are necessary to compute performability.

Several international projects such as GRID, AMBER, HIDENETS, ResiliNets and ReSIST have been launched in recent years aiming to improve the robustness level of critical infrastructures. These projects provide important advances in their respective fields (power grids and computing systems) by proposing techniques and algorithms to improve system evolution, assessability, usability or diversity [25]. However, the majority of these studies focus on specific systems, e.g. SQL database software, lacking the generality of a multidisciplinary framework. GRID studies power systems vulnerabilities spurred by the transformation of the European power infrastructure, ReSIST leads research activities to ensure that present and future computing systems would have the desired resilience and survivability.

A recurrent difficulty in the study of network robustness is the lack of standardized terminology. A stream of apparently new metrics – akin to old wine in new bottles – such as the *expandability* or *degree distribution entropy* [53], [19], [38], is being generated in scientific publications. The creation of new words, while innovative, adds complexity to the already confusing robustness terminology. To solve the terminology chaos, already in 1980 a joint committee on "*Fundamental Concepts and Terminology*", formed by the TC on Fault-Tolerant Computing of the IEEE CS and the IFIP WG 10.4, has defined precisely the various robustness concepts of communication systems. Several papers were presented providing definitions and a taxonomy of robustness metrics [2], including reliability, availability, safety, integrity and maintainability. All these concepts were brought under the umbrella term of *dependability*, while subsequent work also addressed the relation of dependability [32] and performability [37] to resilience. However, in spite of the many efforts and apart from some cases like QoS measures in ATM, many service metrics remain hard to compute.

## II. Proposal of a framework for topological network robustness

This section proposes a topology or graph centric framework for network robustness. As for any good framework, we adhere to the following design specifications. First, the framework should be as simple as possible, while covering all networks. Hence, it should be understandable and interpretable. Second, it should be feasible to compute for any network (of finite size).

The second requirement is the reason why we limit the scope of the framework to topological metrics, which can be computed uniquely for a given graph. On the contrary, the computation of service metrics, such as dependability and survivability, turns out to be much harder. Nevertheless, our formulation allows service aspects to be incorporated (see Section III).

### A. The $R$-value

Fig. 1 illustrates a general question in the field of complex networks: "Given a network at a certain time, is that network *appropriate* or *good* for our purposes?" For example, an Internet service provider may ask whether his current network is "good", a neurologist may want to know whether the functional network of the brain of a patient is "normal". Of course, the above question is ill-posed and not clearly stated because *appropriate* or *good* need to be defined.

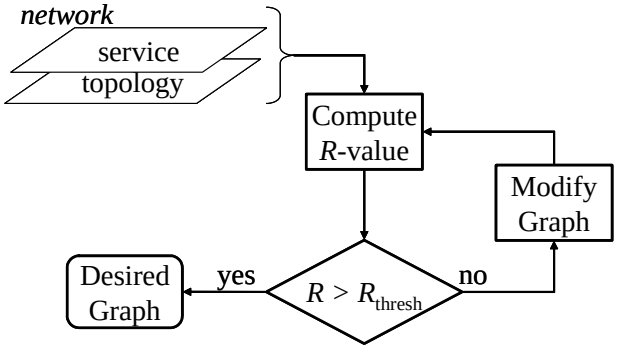


Fig. 1. The organigram or flow chart of the high level goal to achieve network robustness.

We assume that the network graph $G$, defined by a set $\mathcal{N}$ of $N$ nodes that is interconnected by a set $\mathcal{L}$ of $L$ links, the link weight structure and the service (i.e. a software code, protocol or algorithm that specifies the service, see e.g. [47]) are known. A given network at a certain time, defined by a service and a topology as in Fig. 1, is translated into a mathematical object, on which computations can be performed such as the computation of a "goodness" value or robustness value, called the $R$-value. In general terms, the $R$-value is a performance measure that is relevant for the service and

normalized to the interval $[0,1]$. Thus, $R=0$ corresponds to absence of network "goodness" and $R=1$ reflects perfect "goodness". An example of a performance measure is a graph metric such as the average hopcount, the average betweenness, etc. We refer to [4], [17] for a quite extensive discussion and comprehensive list of graph metrics and to [48] for additional properties. One of the main purposes of a network robustness framework is to propose a methodology to define and compute an $R$-value that characterizes a level of robustness and to interpret $R$-values such that classes of desired values can be determined. Section III proposes a definition of the $R$-value and Section V discusses consequences of the proposed $R$-value.

Next, as shown in Fig. 1, the current $R$-value is compared with the minimal desired one, $R_{\text{thresh}}$. The computation of the $R$-value can be part of periodic or event-triggered network maintenance/management operations. Either the $R$-value is sufficient in which case we refrain from taking any corrective action, or the $R$-value is too low, in which case a modification to improve the graph is required. The determination of $R_{\text{thresh}}$ is related to robustness classes, introduced in Section VI-A. A second goal of a network robustness framework is to propose efficient – possibly optimal – strategies how a graph can be modified to increase its $R$-value subject to some cost criterion. This point of view crucially assumes that we have the possibility to alter the topology of the network. Some networks, such as ad-hoc networks or adaptive and growing (e.g. social interaction, biological living) networks, have a flexible topology that varies over time. When the network topology cannot be changed, the robustness can be improved by installing proper functionality at network nodes as discussed in [44] by implementing, for example, a $D^2R^2+DR$ methodology. Using the terminology of [44], Section VI discusses this second "remediation" step.

### B. A challenge: an event that changes the network

Suppose that we know how to compute $R$-values of a network. A snapshot of the network at time $t_0$ gives rise to an $R$-value $R(t_0)$. As long as no events, that change the network, occur during the time-interval $[t_0,t_1]$, the $R$-value does not change and $R(t_1)=R(t_0)$. In this document, we abstract from the precise time at which events occur and only focus on the sequence of changes in the $R$-values caused by these events. This abstraction allows us to employ a discrete time setting (such as in stochastic processing [48, Section 7.1]). If events that change the topology of the network[2] occur at $t_1,t_2,\ldots$, we denote the corresponding set of $R$-values by $R[1]=R(t_1)$, $R[2]=R(t_2),\ldots$ and, in general, the $k$-th event causes an $R$-value equal to $R[k]=R(t_k)$. Thus, square brackets with integer arguments refer to the discrete-time setting, where round brackets with real arguments correspond to a continuous-time setting. If no brackets are used, we assume that the network is viewed at a single instance in time. If network topologies need to be compared, we use subscripts as in $R_G[k]$ to distinguish between graphs. Finally, if several ($m>1$) $R$-values on a graph are computed, the list at discrete time $k$ is denoted by $R_{G;1}[k],\ldots,R_{G;m}[k]$.

A challenge is an event at time $t$ that changes the network and the impact of the challenge is defined as $\Delta R(t)=R(t+\varepsilon)-R(t-\varepsilon)$, where the real number $\varepsilon>0$ is arbitrarily small. In discrete time, the impact of the first challenge is $\Delta R[1]=R[1]-R[0]$, and the impact of the $k$-th challenge is $\Delta R[k]=R[k]-R[k-1]$. Hence, the analogy with stochastic processes is immediate: the impacts are increments, whereas the sequence of events generates a sample path.

### C. An elementary change

Generally, a challenge can be a complex change in a network. Here, we assume that any challenge can be decomposed as a sequence of elementary changes that do not coincide in time. An elementary change is any change that alters a graph related matrix, such as the adjacency or Laplacian matrix [49]. Thus, an elementary change is defined as one of the six modifications: (1) adding a node to $G$; (2) removing a node from $G$; (3) adding a link to $G$; (4) removing a link from $G$; (5) rewiring[3] a link in $G$ and (6) in weighted graphs, changing the link (or/and node) weight. Although a renumbering of the nodes is a change, it does not affect the eigenvalues[4] of the graph, and, hence, most topological metrics of the graph $G$ are unchanged. Hence, a relabeling of nodes is not considered as an infrastructural change, just as a renaming.

### D. Network robustness

The robustness of a network is assessed as the degree of the *network's capability to withstand perturbations during a given time interval*. A perturbation is a series of $n$ elementary changes to which the sequence $\{R[k]\}_{0\le k\le n}$ can be associated. This definition thus implies that a perturbation can be a complex challenge consisting of a well-defined number $n$ of elementary changes. In general, however, $n$ can be a random variable and is not necessarily an a-priori known integer.

For example, suppose that the $R$-value is the percentage of nodes in the largest connected component in the graph $G$ and that a perturbation $P$ consists of uniformly (at random) deleting $n$ links in $G$. Fig. 2 shows three realizations of this perturbation $P$ versus discrete time $k$: a random one and the two most extreme possible. We denote by $\min(R_G[k])=R_{\min}[k]$ and $\max(R_G[k])=R_{\max}[k]$ the minimum and maximum, respectively, of the $R$-value of the graph $G$ at the $k$-th elementary change. If the sequence of $R$-values due to elementary changes, $R[1],R[2],\ldots,R[n]$, is independent, the sequence of the extreme maximum (minimum) one can be a realization (such as in a flipping coin experiment where the sequence with $n$ times heads is a possible, though very unlikely, realization). In general, however, it is possible that

[2]Service changes (for example due to traffic variations) need an entire continuous-time setting, that is, in general, more complex because knowledge about the temporal behavior needs to be properly included. The discrete embedding of a continuous process here eliminates the time-dependence (such as the interarrival times of events) of the process.

[3]Replacing one of the two end points of the link to another node.

[4]If $H$ is a permutation matrix reflecting the renumbering of nodes in the graph $G$ and $A$ is the adjacency matrix of the graph $G$, then the new adjacency matrix $\widetilde{A}=H^{-1}AH$ has the same eigenvalues as $A$ (see [48, p. 438]).

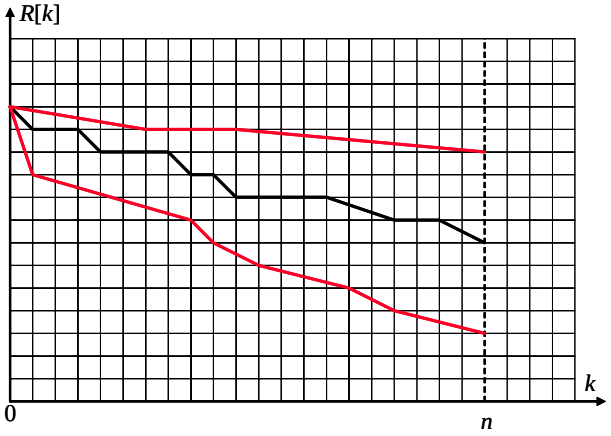


Fig. 2. A sketch of three realizations of a perturbation of a network consisting of $n$ elementary changes: the middle curve is a random realization, while the upper and lower curves reflect the maximum and minimum of (possibly several) extreme realizations as explained in the text.

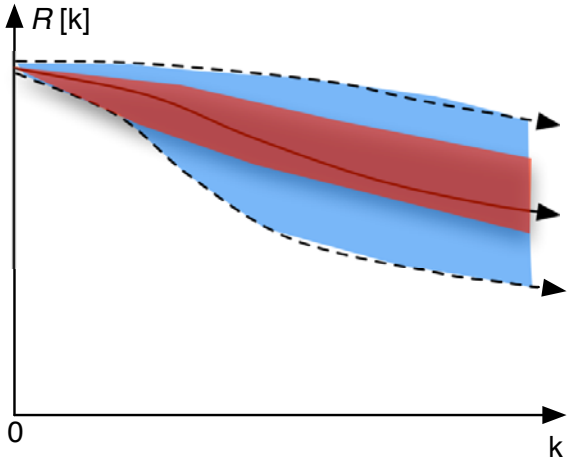


Fig. 3. An illustration of "envelope refining".

extreme realizations are only maximal in some sub-interval of $[0, n]$, and not over the entire interval, because of earlier dependencies. Thus, some extreme realization is maximal in, say $[0, m]$ with $m < n$, and another extreme realization is maximal in $[m, n]$. For example, the order in which links are removed in a graph, generally, is important such that the whole prior history counts. This means that the extreme value over the entire interval may not be a realization of the perturbation process, but an upperbound, thus the maximum of extreme realizations. In the sequel, we call the region between the maximum sequence, $R_{\max}[1], R_{\max}[2], \ldots, R_{\max}[n]$, and the minimum sequence, $R_{\min}[1], R_{\min}[2], \ldots, R_{\min}[n]$, the *envelope* of the perturbation.

The area of the envelope can be regarded as the variation of the $R$-impact of a certain perturbation on a graph. More intuitively, that area quantifies the uncertainty or the amount of risk due to a perturbation. The envelopes may be refined resulting in better risk assessments. When a particular challenge class is not encountered or not possible, the resulting envelope may become narrower and differently shaped as illustrated in Fig. 3.

The example in Fig. 2 illustrates that nearly all perturbations necessitate a stochastic setting. For, relabeling the nodes in a graph does not change the graph, but the sequence of the nodes (or links) that are perturbed *does* matter: the sequence $R[1], R[2], \ldots, R[n]$ is generally a set of dependent random variables, because the present state of the network at discrete-time $k$ does depend on the history of the previous elementary changes. The observation that the description of a network perturbation, measured via a metric $R$, is a stochastic process that is most likely not Markovian implies that analytic computations are, in most cases, intractable and that simulations, approximations or measurements are needed.

From the point of view of robustness, the two extreme realizations or the envelope (or area of the envelope) are most significant. Indeed, if remediation strategies are possible for the extremes, any realization of the perturbation can be counteracted and the threat of the perturbation for the network is averted. Concentrating on the extremes reduces the stochastic perturbation process to a much simpler deterministic process, provided we succeed in computing the extremes. Unfortunately, in most cases, the computation or determination of the extreme realizations (i.e. the best or worst perturbation) is not possible. In general, these are likely NP-complete problems.

We remark that the elasticity, proposed in [45], is actually a realization of a metric or $R$-value due to certain network perturbations.

### *E. Comparing network robustness in two different graphs*

Suppose that the same perturbation is exercised on two, initially connected graphs $G_1$ and $G_2$ and that the impact of the perturbation is measured via the metric $R$. The initial $R$-value for each graph is $R_{G_1}[0]$ and $R_{G_2}[0]$, respectively and, $R_{G_1}[k]$ and $R_{G_2}[k]$ are random variables at discrete time $k$. Depending on the nature of the perturbation, different comparison criteria are possible as shown below.

When the lowest extreme $\min(R_{G_1}[k])$ is always (thus, for any $0 \leq k \leq n$) larger than the highest extreme $\max(R_{G_2}[k])$, then the graph $G_1$ is more robust than $G_2$ with respect to the perturbation $P$. In these, obviously rare cases, the envelopes of both graphs do not overlap as shown in Fig. 4.

The *first and simplest criterion* is: "If $R_{G_1}[n] > R_{G_2}[n]$ (or more precisely[5] $E[R_{G_1}[n]] > E[R_{G_2}[n]]$), then the graph $G_1$ is said to be more robust than $G_2$ with respect to the perturbation $P$ and the metric $R$". If the perturbation is an elementary change ($n = 1$), this criterion is applicable and useful. Examples of elementary changes on different metrics $R$ are presented in [51].

[5]Recall that a perturbation causes the sequence $\{R[k]\}_{0<k<n}$ to be a stochastic process. The expectation is over all possible realizations of the perturbation $P$ in the graph $G$. The stochastic nature thus seriously complicates a rigorous treatment of robustness as defined here, while focusing on the extreme realizations considerably eases the comparison. If the expectation is not shown, we may interpret the criterion as a comparison of the extreme realizations.

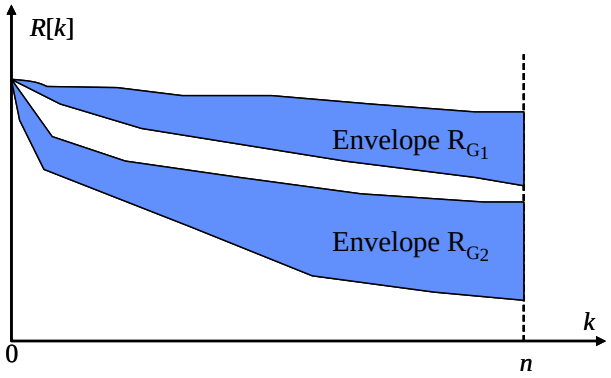


Fig. 4. The envelopes $R_{G_1}$ and $R_{G_2}$ do not overlap.

If the perturbation is not an elementary change ($n > 1$), the above simple criterion is not always desirable because the realizations $\{R_{G_1}[k]\}_{0<k<n}$ and $\{R_{G_2}[k]\}_{0<k<n}$ can intersect more than once such that $R_{G_1}[n] < R_{G_2}[n]$, while $R_{G_1}[j] > R_{G_2}[j]$ for some $0 < j < n$. Thus, the realizations of the perturbation process in both graphs can interlace such that the test "$R_{G_1}[n] < R_{G_2}[n]$?" is not adequate. In those cases, it may be more instructive to consider the summation (or integrated) process. Let us denote the partial sum $r[k] = \sum_{j=0}^{k} R[j]$, that is generally a random variable. A *second criterion* is: "If $E[r_{G_1}[n]] > E[r_{G_2}[n]]$, the graph $G_1$ is said to be more robust than the graph $G_2$ with respect to the perturbation $P$ and the metric $R$".

The hitting time $t$ is the first time at which the $R$-value reaches some threshold value $\rho$, $R(t) = \rho$. The threshold value $\rho$ is some agreed level. Let $k_j$ denote the hitting time in graph $G_j$ for which $R_{G_j}[k_j] = \rho$. A *third criterion* is: "If $k_1 > k_2$, the graph $G_1$ is said to be more robust than the graph $G_2$ with respect to the perturbation $P$ and the metric $R$". In the above example, where the $R$-value is the percentage of nodes in the largest connected component, the requirement that at least half ($\rho = 0.5$) the network must be connected, illustrates this third criterion as the largest (discrete) time at which this requirement is not fulfilled anymore. The longer in time a graph can withstand a perturbation, the more robust that graph is.

Of course, more specific comparison criteria can be defined, but we believe that the three important ones are those explained above: (a) envelope overlap, (b) partial envelope overlap and (c) hitting time. Finally, in spite of the focus on the network topology, we note that the discussed criteria can also be used to compare network services.

## III. Computation and definition of the $R$-value

Here, we confine ourselves to topological metrics. In most cases, more than one topology metric characterizes the network or affects the service. Eventually, however, one number, on which a decision is made, is needed as sketched in Fig. 1. It is important to realize that we can take, in the intermediate process, any useful information into account, but in the end, we need to decide whether the network is robust or not. The general and rigorous way to map a vector with $m$ components into a real, positive number is provided by the norm of a vector (see e.g. [48, p. 445]).

### A. A weighted linear model

We propose to compute the $R$-value of the network robustness by a weighted, linear norm

$$R = \sum_{k=1}^{m} s_k t_k \tag{1}$$

where $s$ and $t$ are the $m \times 1$ weight and the topology vector, respectively. The components of the topology vector $t$ are $m$ graph metrics[6] that characterize the topology/graph. For example, $t_1$ may represent the average hopcount, $t_2$ the minimum degree, $t_3$ the maximum degree, $t_4$ the algebraic connectivity $a(G)$ (second smallest eigenvalue of the Laplacian of graph), and so on. The components of the weight vector $s$ reflect the importance of the corresponding topological metrics for the service. For example, a real-time communication requires certain end-to-end delay bounds. The amount to which metrics influence the end-to-end delay, such as e.g. the average hopcount, the betweenness, the effective graph resistance [49], is reflected by the value of the corresponding component of $s$.

The higher the $R$-value in (1), the larger the robustness. This implies that a metric $t_k$ (or a function of $t_k$, such as the inverse) also should reflect that higher values of $t_k$ lead to higher robustness. In addition, we normalize $R$ to the interval $[0, 1]$. Thus, $R = 0$ corresponds to absence of network robustness and $R = 1$ reflects complete robustness. If $\|.\|_q$ denotes a $q$-norm [48, p. 445], defined as $\|x\|_q^q = \sum_{k=1}^{m} x_k^q$, then the unnormalized $R$-valued, denoted by $\widetilde{R}$, is

$$\left|\widetilde{R}\right| \leq \|s\|_q \cdot \|t\|_q$$

from which normalization follows as

$$0 \leq R = \frac{\left|s^T t\right|}{\|s\|_q \cdot \|t\|_q} \leq 1$$

For example, for the Euclidean norm $\|x\|_2^2 = x^T x = \sum_{k=1}^{m} x_k^2$ of the vector $x$, we have that $s^T t = \|s\|_2 \|t\|_2 \cos(\theta)$, where $\theta$ is the angle between both vectors. Since the components of the topology vector $t$ reflect a different topological metric, the units are different as well as the range of the possible values.

It can be difficult[7] to determine the numerical values of the components $s_k$ based on a service. A simple example, that circumvents the complications induced by the service, considers the weight vector $s$ as a zero-one vector: if $s_k = 0$, then the topology metric $t_k$ is not relevant for the service, while the opposite holds if $s_k = 1$. By this confinement, the $R$-value computation is greatly simplified and (1) can be computed for any graph, provided that the association of the

[6]The number of nodes $N$ and the number of links $L$ are parameters of a graph, not metrics.

[7]An example of the growth dependence of a metabolite on its network topology is given in [58]. Counter examples of services are virus spread (Section IV) and synchronization in networks (the Kuramoto model, see e.g. [41]) that explicitly can be written in terms of the topology.

topology metric $t_k$ with the service can be made. The $R$-value is thus service dependent, even if the topology is the same[8]. For $K$ different services $S_1, S_2, \ldots, S_K$ on a same topology, we may have multiple $R$-values rather than just one value. If $R_{S_j}$ denotes the $R$-value of service $S_j$, then the overall combined service robustness can again be a linear combination,

$$R = w_1 R_{S_1} + w_2 R_{S_2} + \ldots + w_K R_{S_K}$$

where the set of $\{w_j\}_{1 \leq j \leq K}$, properly normalized, reflects how important a certain service is with respect to the others.

### B. A constrained model

Beside the topology vector $t$ and the service vector $s$, we define the additional vector $t_{\min}$ and $t_{\max}$, where the $j$-th component $(t_{\min})_j$ and $(t_{\max})_j$ specifies the minimum and respectively maximum acceptable value of the $j$-th topological metrics $t_j$. In most cases, we are able to determine those extreme acceptable levels of a topological metric.

The weighted linear model is then extended to

$$R_c = 1_{\left\{\cap_{k=1}^{m} t_k \in [t_{\min;k}, t_{\max;k}]\right\}} \sum_{k=1}^{m} s_k t_k \qquad (2)$$

where the indicator is over the intersection of all conditions and where the subscript $c$ reflects these "confinements" or "constraints". If one of the topological metrics $t_k$ does not lie within the required interval $[t_{\min;k}, t_{\max;k}]$, the value of $R_c$ is zero. If all $m$ considered topological metrics satisfy the minimum and maximum levels, then $R_c = R$, defined in (1). The $R_c$ definition avoids that high values of some topological metrics may compensate unacceptably low values of other topological metrics, still leading to an $R$-value that passes the overall requirement $R_{\text{thresh}}$. In addition, if a topological metric $t_k$ does not lie in the required interval, we can immediately take measures to increase/decrease $t_k$, and hence $R_c$, by modifying the topology.

The indicator in (2) makes the definition of $R_c$ non-linear, which complicates analytic computations (e.g. computing the average $E[R_c]$ due to correlations among topological metrics as discussed below).

## IV. Example: Robustness with respect to virus spread

The Susceptible-Infected-Susceptible (SIS) infection model, that arose in mathematical biology, is often used to model the spread of viruses [29], [24], [42], epidemic algorithms for information dissemination in unreliable distributed systems like P2P and ad-hoc networks [10], [20], and the propagation of faults and failures in networks like BGP [15]. The SIS model assumes that a node in the network is in one of two states: infected and therefore infectious, or healthy and therefore susceptible to infection. The SIS model usually assumes instantaneous state transitions. Thus, as soon as a node becomes infected, it becomes infectious and likewise, as soon as a node is cured it is susceptible to re-infection. There are models [18], [29], [54] that include more details like incubation periods, variable infection rates, a curing process that takes a certain amount of time and so on.

If $\beta$ and $\delta$ denote the infection rate along each link and the curing rate for each node respectively, then the effective spreading rate of the virus can be defined as $\tau = \frac{\beta}{\delta}$. In epidemiological theory, many authors (see e.g. [18], [3], [29] and [42]) refer to an epidemic threshold $\tau_c$: for effective spreading rates $\tau < \tau_c$ the virus contamination in the network dies out - the mean epidemic lifetime is of order $O(\log N)$, while for effective spreading rates above $\tau_c$ the virus is prevalent, i.e. a fraction of nodes remains infected with mean epidemic lifetime [24] of the order $O\left(e^{N^\alpha}\right)$. In the case of persistence, we will refer to the prevailing state as a metastable state or steady-state. The epidemic threshold formula $\tau_c = \frac{1}{\lambda_1(A)}$, where $\lambda_1(A)$ denotes the largest eigenvalue or spectral radius of the adjacency matrix $A$ of the graph, is rigorously demonstrated in the $N$-intertwined model [52], in which a mean field application is the only approximation of the exact $2^N$-state Markov SIS model. Moreover, the $N$-intertwined model expresses the governing equations of the spreading process (the service) explicitly in terms of the topology (via the adjacency matrix $A$). It is an example where the service is a well-defined function of the topology.

It is common practice [28] to choose the epidemic threshold $\tau_c$ as a measure for robustness, thus $R = \tau_c$: the larger the epidemic threshold, the more robust a network is against the spread of a virus. This practice corresponds to the notion of hitting time as a measure for robustness, suggested in Section II-E. Because the epidemic threshold is inversely proportional to the largest eigenvalue of the adjacency matrix, it seems easy to compare the robustness of two networks. However, by considering three different graphs on 10 nodes: the complete bipartite graph $K_{2,8}$, the Petersen graph $P$ and the ring graph $C_{10}$, we will show that the comparison of the robustness with respect to virus spread in different networks is not so straightforward. The Petersen graph is a regular graph where every node has 3 neighbors, while the ring graph is a regular graph where every node has degree two. Using the results in [39], the epidemic thresholds and the fraction $y_\infty$ of infected nodes in the steady-state can be determined for the three graphs.

The values are visualized in Figure 5, which shows that $y_\infty(C_{10})$ is always smaller than $y_\infty(K_{2,8})$ and $y_\infty(P)$. Therefore, the ring $C_{10}$ is more robust with respect to virus spread than $K_{2,8}$ and $P$. The comparison between the bipartite graph $K_{2,8}$ and the Petersen graph $P$ is less straightforward. If we only look at the epidemic threshold, the Petersen graph outperforms $K_{2,8}$. However, for $\tau$ sufficiently large, $K_{2,8}$ performs better because then the fraction of infected nodes is lower than for the Petersen graph.

This observation suggests to consider an integrated measure that takes the complete range of $\tau$ values into account. Since the area under the $y_\infty$ versus $\tau$ curve diverges, instead of

[8]Let us recall the example of services with contrasting requirements. A real-time service generally requires a low end-to-end delay, which translates in a small diameter of the graph and a large clustering coefficient. An anti-virus service may want to have a large diameter and a small clustering coefficient. In the first service, transport of packets should propagate as fast as possible, while the anti-virus spread service has just the opposite goals.

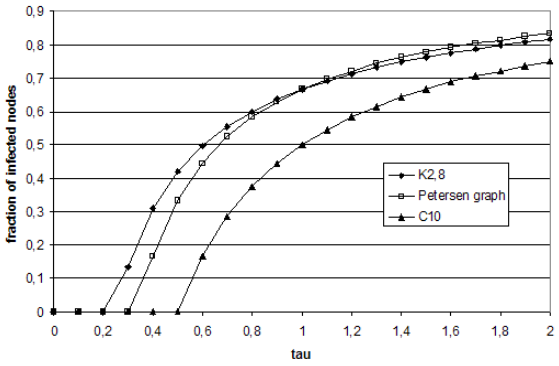


Fig. 5. Fraction of infected nodes for $K_{2,8}$, Petersen graph and $C_{10}$

considering the effective spreading rate $\tau$, the reciprocal of $\tau$ is considered, that is the effective curing rate $s = \tau^{-1} = \frac{\delta}{\beta}$. The viral conductance $VC_G$ of a network $G$, the robustness measure with respect to virus spread that takes into account all values of $\tau$ (and hence $s$), is defined in [30] as

$$VC_G = \int_0^\infty y_\infty(s)ds$$

where $y_\infty(s)$ denotes the fraction of infected nodes in steady-state. The viral conductance $VC_G$ is thus an instance of the second criterion in Section II-E.

In order to reflect both a large threshold (virus-free region) and resistance against infections (when the virus prevails), we may propose, according to (1), $R = \frac{s_1}{\lambda_1(A)} + \frac{s_2}{VC}$. When a large virus-free region is preferred, $s_1 > s_2$ and vice versa. When also connectivity is desired, we may add the algebraic connectivitity $a(G)$ and arrive at $R = \frac{s_1}{\lambda_1(A)} + \frac{s_2}{VC} + s_3 a$.

Other examples can be found in e.g. [1], [14], where the relative size of the largest component is taken as a measure of robustness in the case of removal of a certain percentage of nodes.

## V. Discussion of the proposed $R$-model

The basic design principle of the $R$-model is that it is as simple as possible while still being general. The simplicity follows from its linearity, while its generality from its dimensionality $m$ of the weight $s$ and the topology $t$ vector. Any proposed definition is always debatable, and in the sequel of this section, we discuss some issues related with the $R$-model.

### A. Linearity of the $R$-definition (1)

Apart from simplicity, the linear definition (1) has an important advantage over a non-linear definition,

$$R = f(t, s) = f(t_1, t_2, \ldots, t_m; s)$$

where $f$ is a multi-dimensional function of the vector components $\{t_k\}_{1 \le k \le m}$ of $t$ and, possibly, of $s$. Indeed, in view of the stochastic nature of the perturbations, the average of (1), being the best first order moment estimator of the random variable, equals

$$E[R] = \sum_{k=1}^{m} s_k E[t_k]$$

because the weights $s_k$ emphasize the importance of the topological metric $t_k$ and are independent of the challenges or changes in the topology. Thus, we observe that the average $E[R]$ is again a linear function of the averages of the components $E[t_k]$ for $1 \le k \le m$, because the expectation operator $E[.]$ is linear. On the other hand, $E[R] = E[f(t, s)]$ – which is a multi-dimensional integral – is generally difficult to compute [48], but, more importantly, it will involve dependencies between the components $t_k$. As explained in Section V-C, the dependencies or correlations between topological metrics of a same graph constitute a major difficulty.

In addition, the non-linear function $f$ needs to possess useful properties, such as, for example, convexity. The number of possibilities to propose an acceptable non-linear function $f$ are far larger than a linear one, which will jeopardize the consensus process to agree upon the definition of $R$.

Finally, in view of the inaccuracies in the topology and the link weight structure of the graph – let alone the complexity to valorize a service – non-linear functions generally amplify such errors much harder than a linear function.

These arguments support the choice of the definition (1).

### B. Uniqueness of the topology vector

We first explain the vector interpretation geometrically. Consider the space spanned by the $m$ metrics vectors $e_1, e_2, \ldots, e_m$, where $e_j$ represents the axis of the $j$-th metric. Each metric vector has unit norm, $\|e_j\|_q = 1$, and the projection of $t$ onto $e_j$, $t.e_j = t_j$, equals the value of the $j$-th component of $t$. For each graph $G$, we can compute the topology vector, denoted by $t_G$ to explicitly refer to the graph $G$, and each point or vector $t_G$ with coordinates $(t_1, t_2, \ldots, t_m)$ represents a graph. If we use the Euclidean norm ($q = 2$), then any vector $t_G$ lies within the $m$-dimensional unit-norm ellipsoid[9] with axes equal to the vectors $e_1, e_2, \ldots, e_m$. The indicator in the definition (2) of $R_c$ limits the $m$-dimensional $t$-space to the interior of two hyper-polygons: the "outer"-polygon and "inner"-polygon have corner points defined by the vector $t_{\max}$ and $t_{\min}$, respectively.

The point $t_G$ within the $m$-dimensional unit-norm ellipsoid is not necessarily representing a graph in a unique way. If $m$ is small, for example, more graphs may possess the same topology vector. In addition, a small $m$ may "color" the physical meaning of robustness. For example, if we choose for $t_1$ the minimum degree and for $t_2$ the vertex connectivity, the network robustness basically measures the connectivity of a graph, independently of other topological features that may impact the service such as, for example, the hopcount or diameter. These arguments already underline the necessity to choose $m$ sufficiently large.

[9]Only when all $m$ metrics vectors are orthogonal, each graph point $(t_1, t_2, \ldots, t_m)$ lies within a $m$-dimensional unit sphere.

On the other hand, we associate the service performance to a set $m$ of possibly independent topological metrics. The dimension $m$ depends, thus, on the service and can be small. When packets are transported along a communication network, for example, the robustness reflecting the efficiency of network resource usage can be characterized by basically a few topological metrics: a statistical measure (e.g. the average, the average plus the square root of the variance, the maximum, etc.) of the hopcount or/and of the betweenness.

From a computational efficiency point of view, the number $m$ of different graph metrics should not be too large. Hence, we expect that there is a certain, adequate number for the dimensionality of the metrics space. *The sensitivity of $R$ on the dimension $m$ is a topic of research.*

### C. Orthogonality of the $m$ metrics vectors

The unit metrics vectors $e_i$ and $e_j$ are not necessarily orthogonal. For example, the minimum degree $d_{\min}$ and the algebraic connectivity $\mu_{N-1}$ are correlated because $0 \leq \mu_{N-1} \leq d_{\min}$ (see e.g. [49]), hence, the angle between the corresponding metrics vectors is less than $90^o$ degrees. The higher the correlation between metrics $i$ and $j$, the more the vectors $e_i$ and $e_j$ are aligned. This implies that less information is reflected by dependent metrics. Just as in linear algebra, the ideal coordinate system consists of orthogonal vectors[10]. Hence, the $m$ metrics should be chosen to be as independent or as orthogonal as possible. In general, since all metrics are computed from the adjacency matrix of $G$, we may expect that most metrics are dependent. In addition, the degree of dependence between metrics $i$ and $j$ is graph dependent. In other words, two metrics $i$ and $j$ may be independent for graph $G_1$, but they can be dependent in graph $G_2$. *The dependence between metrics in a graph seems a hard, inherent challenge of the robustness problem.*

A simple example illustrates the problem. Suppose that in graph $G_1$, the three chosen metrics $e_1, e_2$ and $e_3$ are independent such that

$$R_{G_1} = s_1 e_1 + s_2 e_2 + s_3 e_3$$

In graph $G_2$, metric $e_3$ is dependent on $e_1$ and $e_2$. Thus, we may write $e_3 = a e_1 + b e_2$ which results in

$$R_{G_2} = (s_1 + a)\, e_1 + (s_2 + b)\, e_2$$

This shows that $m$ is effectively 2, instead of 3, and that the weight vector $s$ is modified by the topology.

The determination of the dependence between any pair of metrics vectors $e_i$ and $e_j$, equivalent to determining the angles between the metric vectors that form the coordinate system of the metric space, stands on the research agenda. Perhaps, a metrics based approach is better replaced by considering graph theoretic matrices that uniquely define the graph, such as the adjacency $A$, incidence $B$ and Laplacian $Q$ matrix [48, Appendix B]. Another suggestion to circumvent correlations is to focus on the eigenvalues of these graph related matrices. Since these matrices are symmetric for undirected and unweighted graphs, the eigenvalues and corresponding eigenvectors are real. Moreover, the eigenvectors are orthogonal, specifying independent inherent "properties" of the graph. We refer to [49] for a deeper discussion on the meaning of eigenvectors as characterizers of a graph.

A related idea is the graph embedding into a geometric space as proposed in [31]. Since the complete graph as the highest robustness, the distance in the geometric graph space from an arbitrary graph to the complete graph can be regarded as $R$-value. The difficulty, however, lies in finding such a space in which a distance function exists.

### D. Scaling of graphs

Another issue is how networks with different number of nodes $N$ and links $L$ can be compared. In other words, what is a good normalization of a graph matrix[11]. In many complex networks, properties for small size $N$ are different than in the asymptotic regime (large $N$). Perhaps a generally valid scaling or normalization is impossible! The difficulty of comparing two networks with different sizes $N$ or number of links $L$ lies in the fact that the scaling of topological metrics with respect to $N$ or $L$ is network-dependent.

Indeed, consider an Erdös-Rényi (ER) graph $G_p(N)$ with $N$ nodes and where $p$ is the probability to have a link (independent of the existence of other links) between two nodes. If $N$ is small, then $G_p(N)$ is a random graph, whereas for large $N$, $G_p(N)$ tends to a deterministic, regular graph (see [48, p. 488]). This example shows that when a graph of a certain class grows in size, its properties may change. Another similar example appears in the class of power law graphs, that seem quite good models matching the degree distribution in complex networks (such as the Internet). Power law graphs can be constructed by a stochastic growth rule such as preferential attachment. Only when the power law graph is sufficiently large (in practice $N > 500$), a power law for the degree is observed. For smaller graphs (about $N < 300$), the degree does not follow a clear power law [34] and most often an exponential fit is statistically equally significant as a power law fit.

Consider two ER random graphs of $N = 100$ nodes and $N = 1000$ nodes respectively, but with the same link density $p > \frac{\log N}{N}$. Assume that the average hopcount $R = E[H]$ is the robustness measure. Many believe that the two graphs are equally robust because they are generated by the same mechanism, where any two nodes are connected independently with a give probability $p$. The average hopcount of these two networks is approximately [48, p. 346] the same $E[H] \simeq 2-p$. Moreover, network robustness is usually evaluated by comparing the network with others, normally the corresponding ER random graphs, of the same size $N$. Such a scaling is used, in particular in brain functional networks, to examine whether a network possesses the small-world property [55]. In this case, $R = 1$ holds for both example networks and

[10] Any set of linearly independent vectors can be orthogonalized via the Gramm-Schmidt orthogonalization process. In practice, methods based on the eigenstructure of a matrix with the metric vectors $e_1, e_2, \ldots, e_m$ as row or column vectors are more appropriate (such as e.g. the singular value decomposition).

[11] Normalized matrices have been defined, such as the normalized Laplacian $\Delta^{-1}Q$, where $\Delta = \text{diag}(d_j)$ and $d_j$ is the degree of node $j$.

the two networks are still equally robust. However, such a normalization cannot guarantee $R \leq 1$ for any graph. On the other hand, if we simply normalize the metric $R = E[H]/N$ by its maximum value $N$, the smaller network is more robust. This example illustrates the importance of scaling in evaluating the robustness of networks with different sizes.

In summary, the way properties (measured via graph metrics) change with $N$ (or $L$) is generally different for each class of graphs. This means that scaling laws (as function of $N$ or $L$) are graph dependent, which complicates proper comparison between graphs of different sizes $N$ and number of links $L$.

*Comparison of properties in graphs with different number of nodes and links needs to be investigated.*

### E. The comparison of $R$-values

In this section we will give an example illustrating that the interpretation of the comparison of the $R$-values of two graphs is not trivial. We consider a non-normalized $R$-value that only depends on one topological metric, namely, the algebraic connectivity. The algebraic connectivity $a(G)$, defined by Fiedler [22] as the second smallest Laplacian eigenvalue, has received significant attention as an adequate measure of network connectivity and, consequently, as a robustness metric with respect to the removal of nodes and links. It is generally believed (see e.g. [49]) that, "the larger the algebraic connectivity, the more robust the network is with respect to removal of nodes and/or links".

We will give a counter-example to this common belief. Fig. 6 depicts two graphs $G_1$ and $G_2$, each with $N = 7$ nodes, $L = 10$ links and diameter 4, but with different algebraic connectivity $a(G_1) = 0.6338$ and $a(G_2) = 0.5858$. Although $a(G_1) > a(G_2)$, it is easier to disconnect $G_1$ than $G_2$, because one link removal disconnects $G_1$, while two links need to be deleted in $G_2$.

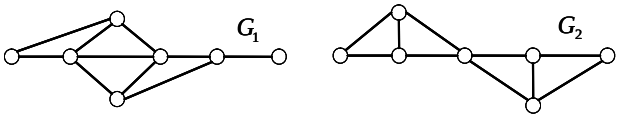


Fig. 6. Two graphs $G_1$ and $G_2$, each with $N = 7$ nodes, $L = 10$ links and diameter 4, but with different algebraic connectivity.

The fact that it is easier to disconnect $G_1$ than $G_2$ by link removal is also reflected by the reliability polynomials $P(G_1)$ and $P(G_2)$. Denoting the availability of each link by $p$ and assuming that the availabilities of two separate links are independent, then we obtain, with $p = 1 - q$, that $P(G_1) = 1 - O(q)$ and $P(G_2) = 1 - O(q^2)$ as $q \to 0$. For $0 < q << 1$, it holds that $P(G_1) < P(G_2)$, hence, it is easier to disconnect $G_1$ than $G_2$, although $a(G_1) > a(G_2)$.

## VI. Remediation

Once we can agree upon a definition like (1) or (2), for each graph, an $R$-value can be determined. If the graph (without altering the service) is changed, a new $R$-value can be computed. As illustrated in Fig. 1, that current $R$-value is compared with the minimal desired one, $R_{\text{thresh}}$ in (1), or the constraints vectors $t_{\max}$ and $t_{\min}$ in (2). If $R < R_{\text{thresh}}$ in (1) or $1_{\left\{\cap_{k=1}^{m} t_k \in [t_{\min;k}, t_{\max;k}]\right\}} = 0$ in (2), modification of the network is required subject to some *criterion*. In what follows, we will discuss briefly (a) robustness classes; (b) how to change/modify a graph; and (c) the criterion.

### A. Robustness classes

We embark on defining $c$ robustness classes. A robustness class specifies, for a certain service, a subinterval of $[0, 1]$ since $R \in [0, 1]$. For example, class $C_1$ contains all graphs whose $R$-values lie between $[0, r_1)$, class $C_2$ contains all graphs in $[r_1, r_2)$, and so on. The idea of robustness classes is related to QoS classes: for a given service, a few number of classes seems more manageable than a continuous range of $R$. Strictly speaking, robustness classes are not necessary in a coherent and consistent framework. But, they make interpretations easier by mapping the $R$-values to a few ranges to which, for example, colors like red, orange, green can be assigned with their usual meaning. For, suppose a graph possesses a value $R = 0.3$, what does this value mean? The definition of robustness classes simplifies the interpretation and determination of the threshold value $R_{\text{thresh}}$.

*At present, we believe that mainly by extensive simulations, a good proposal of the number and the value range of robustness classes can be presented.*

The definition (2) of $R_c$ contains the constraint vectors $t_{\min}$ and $t_{\max}$, whose values can be specified per robustness class.

The concept of robustness classes also emerges in Business Continuity Management (BCM). BCM is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption, see [7], [8]. Within BCM the impact of threats are classified as either high, medium or low.

### B. Modifying a graph

An unweighted graph can be modified by a series of elementary changes as defined in Section II-C: by adding and removing nodes and by adding, deleting, and replacing or rewiring of links. The remedial modification is often the reverse of what a challenging perturbation does.

In weighted graphs, all link weights (e.g. delay, capacity,..) can be modified, in addition to the above discussed structural changes. This again shows that weighted graphs contain a much richer set of modification possibilities. However, the drawback is that the modification of the weighted graph is of considerably higher complexity than that of the unweighted graph. In addition, we encounter again the basic problem of correlations between the link weights of different links in the graph and among different link weights themselves.

How to modify a given graph to enhance its robustness level from $R_1$ to $R_2$ is, in general, difficult to determine. However, the problem is well-defined and the complication lies in the computational feasibility (even tractability), not in the concept, nor in the specification. The problem is thus more of an optimization nature: given a graph, each elementary change

has an effect on $R$ and a specific set of elementary changes – a perturbation – may lead to a minimum desired robustness level $R_{\text{thresh}}$.

We ought to mention that, if the change from $R$ to $R+\Delta R$ is possible, an algorithm that can exhaustively compute all possible elementary changes, eventually can find/construct the modified graph. However, the number of operations to compute may be unacceptably high as illustrated in [51]. Hence, we expect that good modification strategies need to be found. For example, adding a new node/link to high or low degree node may have a higher effect on $R$, than to add that new node/link to an arbitrary node in $G$. Another example is the determination of very robust graphs with extreme spectral gap (or algebraic connectivity): by only deleting a few links in the complete graph in different ways, a large variation of the spectral gap is found: the link removal strategy that maximizes the spectral gap is one that maximizes the minimum degree.

### C. Criteria

In Section VI-B, we have argued that, in most cases, an exhaustive algorithm can be found. However, apart from the computational complexity of the algorithm, also the solution may not be unique. This means that other aspects may finally determine the eventual details to modify the robustness level from $R_1$ to $R_2$. A common criterion is that the graph is modified subject to a minimization of the incurred financial cost, because infrastructural changes are generally expensive.

However, in particular cases and services, other or additional optimization criteria as well as constraints are possible. An example of constraints are limitations imposed to the number of additions (or removals) of nodes or links or of rewirings. Another constraint may restrict only certain subsets of nodes and links in the graph to be changed.

## VII. Conclusions

In summary, the explicit definition of robustness is tightly coupled to what the goal of the network is, or for what service the network is designed. Since a service is clearly dependent on the topology, the *topological* robustness of any service can be expressed as in (1), provided the relevant topological metrics $t_1, t_2, \ldots, t_m$ are known and provided we agree about the corresponding service weights $s_1, s_2, \ldots, s_m$. This framework thus allows us, for a particular service, to compare different networks against various topological perturbations.

In subsections of Section V, we have presented in italics research problems that need an answer because they remain gaps of a coherent robustness framework. Notwithstanding these unsolved problems, we might consider this article as already successful if the linear $R$-model in (1) and/or (2) were to reach consensus and gain general acceptance.

**Acknowledgements.** This research was supported by the European Union Research Framework Programme 7 via the ResumeNet project with contract number FP7 – 224619. We are grateful for the instructive comments of Ariel Orda, Caterina Scoglio, Christian Rohner and Bernhard Plattner.

## References

[1] R. Albert, H. Jeong, A.-L. Barabási, "Error and Attack Tolerance of Complex Networks". Nature 406: 378-382, 2000.
[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Trans. Dependable Secur. Comput., vol. 1, no. 1, pp. 11–33, 2004.
[3] N.T.J. Bailey, *The Mathematical Theory of Infectious Diseases and its Applications*, Charlin Griffin & Company, London, 1975.
[4] S. Baccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, “Complex networks: Structure and dynamics”, 424:175–308, 2006.
[5] B. Bollobas. *Random Graphs*. Cambridge University Press, Cambridge, 2nd edition, 2001.
[6] D. Braess, A. Nagurney, and T. Wakolbinger. On a paradox of traffic planning. *Transportation Science*, 39(4):446–450, 2005.
[7] British Standards Institute, BS 25999-1:2006 Business Continuity Management Part 1: Code of practice.
[8] British Standards Institute, BS 25999-2:2007 Business Continuity Management Part 2: Specification.
[9] 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, p. 5468, 2000.
[10] D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin and M. Faloutsos, “Information Survival Threshold in Sensor and P2P Networks”, IEEE INFOCOM07, 2007.
[11] S.-C. Chang and R. Shrock, “Reliability polynomials and their asymptotic limits for families of graphs,” J.STAT.PHYS., vol. 112, p. 1019,2003.
[12] M. Chari and C. J. Colbourn, “Reliability polynomials: A survey,” J.Combin. Inform. System Sci, vol. 22, pp. 177–193, 1998.
[13] P. Cholda, A. Mykeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk. A survey of resilience differentiation frameworks in communication networks. *IEEE Communications Surveys*, 9(4):32–54, 2007.
[14] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, "Resilience of the Internet to Random Breakdowns". Physical Review Letters 85 (21): 4626-4628, 2000.
[15] F. Coffman, Z. Ge, V. Misra and D. Towsley, “Network resilience: exploring cascading failures within BGP”, Proceedings 40th Annual Allerton Conference on Communications, Computing and Control, 2002.
[16] M. Cushing, J. Krolewski, T. Stadterman, and B. Hum, “U.S. army reliability standardization improvement policy and its impact,” EEE Transactions on Components, Packaging, and Manufacturing Technology. Part A, vol. 19. No. 2, pp. 277–278, 1996.
[17] L. Da F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas. Characterization of complex networks: A survey of measurements. *Advances in Physics*, 56(1):167–242, Februari 2007.
[18] D. Daley and J. Gani, *Epidemic modelling: An Introduction*, Cambridge University Press, 1999.
[19] E. Estrada, “Network robustness to targeted attacks. the interplay of expansibility and degree distribution,” The European Physical Journal B - Condensed Matter and Complex Systems, vol. 52, no. 4, pp. 563–574, 2006.
[20] P. Eugster, R. Guerraoui, A. Kermarrec and L. Massoulié, “From Epidemics to Distributed computing”, IEEE Computer, Vol. 37, pp. 60-67, 2004.
[21] M. Faloutsos, P. Faloutsos, and C. Faloutsos, “On power-law relationships of the internet topology,” in In SIGCOMM, pp. 251–262, 1999.
[22] M. Fiedler, “Algebraic connectivity of graphs”, Czechoslovak Mathematical Journal 23, pp. 298-305, 1973.
[23] H. L. Frisch and J. M. Hammersley, “Percolation processes and related topics,” SIAM Journal on Applied Mathematics, vol. 11, no. 4, pp. 894–918, 1963.
[24] A. Ganesh, L. Massoulié and D. Towsley, “The Effect of Network Topology on the Spread of Epidemic”, IEEE INFOCOM05, 2005.
[25] I. Gashi, P. Popov, and L. Strigini, “Fault tolerance via diversity for offtheshelf products: A study with sql database servers,” Dependable and Secure Computing, IEEE Transactions on, vol. 4, pp. 280–294, Oct.-Dec. 2007.
[26] M. Girvan and M. E. J. Newman. Community structure in social and biological networks. *Proc. Natl. Acad. Sci. USA*, 99:7821–7826, 2002.
[27] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, “Attack vulnerability of complex networks,” Physical Review E, vol. 65, p. 056109, 2002.
[28] A. Jamakovic, R.E. Kooij, P. Van Mieghem and E. van Dam, “Robustness of networks against the spread of viruses: the role of the spectral radius”, 13th Annual Symposium of the IEEE/CVT Benelux, Luik, Belgium, 2006.

[29] J. Kephart and S. White, “Direct-graph epidemiological models of computer viruses”, IEEE Computer Society Symposium on Research in Security and Privacy, pp. 343–359, 1991.

[30] R.E. Kooij, P. Schumm, C. Scoglio and M. Youssef, “A new measure for robustness with respect to virus spread”, IFIP Networking 2009, Aachen, Germany, 2009.

[31] D. Krioukov, F. Papadopoulos, M. Kitsak, A. Vahdat, and M. Boguna, “Hyperbolic Geometry of Complex Networks”, Physical Review E, vol. 82, 036106, 2010.

[32] J.C. Laprie, “From dependability to resilience”, Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Network (DSN 2008), Anchorage, Alaska, USA, June 2008.

[33] V. Li and J. Silvester, “Performance analysis of networks with unreliable components”, IEEE Transactions on Communications, Vol. 32, No. 10, pp. 1105-1110, October 1984.

[34] J. Martin Hernandez, T. Kleiberg, H. Wang, and P. Van Mieghem. A qualitative comparison of power law generators. *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2007), San Diego, California, USA.*, July 16-18 2007.

[35] J. F. Meyer, “On evaluating the performability of degradable computing systems”, IEEE Transactions on Computers, Vol. C.29, No. 8, pp. 720–731, 1980.

[36] J. F. Meyer, “Performability: a retrospective and some pointers to the future”, Performance Evaluation, Vol. 14, pp. 139-156, 1992.

[37] J. F. Meyer, “Defining and evaluation resilience: a performability perspective”, Proceedings of the International Workshop on Performability Modeling of Computer and Communication Systems, Eger, Hungary, September 2009.

[38] M. Menth, M. Duelli, R. Martin, and J. Milbrandt, “Resilience analysis of packet-switched communication networks,” Networking, IEEE/ACM Transactions on, vol. PP, p. 1, August 2009.

[39] J. Omic, R.E. Kooij and P. Van Mieghem, “Virus Spread in Complete Bi-partite Graphs”, BIONETICS 2007, Budapest, Hungary, 2007.

[40] L. Page and J. Perry, “Reliability polynomials and link importance in networks,” Reliability, IEEE Transactions on, vol. 43, pp. 51–58, Mar 1994.

[41] J. G. Restrepo, E. Ott and B. R. Hunt, “Onset of synchronization in large networks of coupled oscillators”, Physical Review E, vol. 71, No. 036151, pp. 1-12, 2005.

[42] R. Pastor-Satorras and A. Vespignani, “Epidemic Spreading in Scale-Free Networks”, Physical Review Letters, Vol. 86, pp. 3200–3203, 2001.

[43] S. Rai and K. K. Aggarwal, “An efficient method for reliability evaluation of a general network”, IEEE Transactions on Reliability, Vol. 27, No. 3, pp. 206-211, August 1978.

[44] J. P. G. Sterbenz, D. Hutchison, E. Etinkaya, A. Jabbar, J. P. Roher, M. Schöller, and P. Smith. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. *Computer Networks*, 2010, to appear.

[45] A. Sydney, C. Scoglio, P. Schumm, and R. Kooij. ELASTICITY: Topological characterization of robustness in complex networks. *Bionetics 2008, Hyogo, Japan*, November 25-28 2008.

[46] M. F. Sykes and J. W. Essam, “Exact critical percolation probabilities for site and bond problems in two dimensions,” Journal of Mathematical Physics, vol. 5, no. 8, pp. 1117–1127, 1964.

[47] P. Van Mieghem. *Data Communications Networking*. Techne Press, Amsterdam, 2006.

[48] P. Van Mieghem. *Performance Analysis of Communications Systems and Networks*. Cambridge University Press, Cambridge, U.K., 2006.

[49] P. Van Mieghem. *Graph Spectra for Complex Networks*. Cambridge University Press, Cambridge, U.K., 2010.

[50] P. Van Mieghem and H. Wang. The Observable Part of a Network. *IEEE/ACM Transactions on Networking*, 17(1):93–105, 2009.

[51] H. Wang and P. Van Mieghem. Algebraic connectivity optimization via link addition. *Bionetics 2008, Hyogo, Japan*, November 25-28 2008.

[52] P. Van Mieghem, J. Omic and R. E. Kooij, “Virus Spread in Networks”, IEEE/ACM Transactions on Networking, Vol. 17, No. 1, pp. 1-14, 2009.

[53] B. Wang, H. Tang, C. Guo, and Z. Xiu, “Entropy optimization of scalefree networks’ robustness to random failures,” Physica A: Statistical Mechanics and its Applications, vol. 363, no. 2, pp. 591 – 596, 2006.

[54] Y. Wang and C. Wang, “Modeling the Effects of Timing Parameters on Virus Propagation”, ACM Workshop on Rapid Malcode, Washington DC, 2003.

[55] D. J. Watts. *Small Worlds, The Dynamics of Networks between Order and Randomness*. Princeton University Press, Princeton, New Jersey, 1999.

[56] R. Wilkov, “Analysis and design of reliable computer networks,” IEEE Transactions on Communications, Vol. 20, No. 3, pp. 660-677, June 1972.

[57] O. Wing, P. Demetriou, “Analysis of Probabilistic networks”, IEEE Transactions on Communication Technology, Vol. 12, pp. 38-41, September 1964.

[58] W. Winterbach, H. Wang, M. Reinders, P. Van Mieghem and D. de Ridder, 2010, "Correlating the topology of a metabolic network with its growth capacity", Bionetics 2010, December 1-3, Boston, USA.