Network robustness and resilience: survey of metrics

Fernando Morales, Elisa Schaeffer, Ivana Bachmann, Javiera Figols, and Javier Bustos

***Abstract*—We survey metrics that seek to capture in numerical terms the resilience and the robustness of a network, represented in graph-theoretical terms. After a brief introduction and the establishment of notation and terminology, we present the identified metrics compiled from journals published between 2006 and 2015, these metrics are cataloged in terms of the network elements on which the calculation of each metric is based: vertex-based, edge-based, subgraph-based, and finally spectrum-based metrics. We then describe some of the numerous application areas for such metrics and close with a discussion of open problems and future directions.**

***Index Terms*—Network theory (graphs), reliability, robustness**

I. Introduction

A system that manages to either maintain or at least restore operability under failures or attacks is *resilient*. This survey explores the definitions given in literature in hopes of quantifying the *resilience* of a networked system. When resilience is considered as tolerance against *random failures* of network components, it is often referred to as *robustness* [1]. In the literature, also the terms *flexibility* and *confiability* are used for related concepts [2, 3]. Sources of random failures in networked systems include component overload, loss of energy or telecommunication links, erroneous configuration of components, and failures of electronic devices.

When the interest does not lie in random failure but instead in how well a networked system withstands *deliberate attacks* [4], the term *vulnerability* is often used. A typical usual goal for such an attacker is to cause the greatest possible disruption to the system [5, 6] and the attack may consist in a sequence of attacks instead of a single one [7].

When multiple threats exist against a system, the vulnerability of a system as a whole can be quantified in terms of the individual impacts and the occurrence probabilities of the threats [8]; this also extends to robustness against random failures when the impacts and probabilities can be estimated. The possible events may then be ranked from the most severe (the highest product of impact and likelihood) to the least severe.

In both cases — robustness and vulnerability —, the impact of the damage is not the only measure of interest, but also the speed at which the system is able to recover from is relevant [9]. Strategies and methodologies for controlling the "resilience cycle" (referring to the state changes between operational, broken, and recovered) [8, 10] emphasize how all systems are prone to failures and that a thorough understanding of the normal operation of a system provides a necessary foundation for identifying possible problems. The basic steps involve *identifying* threats, *detecting* undesirable events, and having formulated *response plans* for any events that may compromise system functionality.

E. Schaeffer is with the School of Mechanical and Electrical Engineering (FIME) of the UANL, Mexico

Draft, May 14, 2018.

A. Our contribution

The scope of this article is to catalog the robustness metrics for complex networks that have been proposed in top-tier journals published from 2006 to 2015. As far as the authors knowledge this is the first systematic literature review about network robustness metrics.

Our survey differs from the rest in its scope, we focus on those that have been used in the literature for the express purpose of determining structural aspects related to the robustness or the resilience of a network. For a survey of general structural metrics for networks, including those that are not intended to capture resilience-related characteristics, we refer the reader to the work of da F. Costa et al. [32].

B. Our findings

In our survey, with no attempt towards mathematical rigor, we use the term *metric* to refer to a function that yields a numerical value that can be used as a measurement of how strongly a specific characteristic is present when given as input a network structure, possibly carrying out some modifications on that structure. One common modification is the introduction of a *failure* in one or more of the network's components. For an arbitrary metric M, its *deterioration* can be calculated as the difference between its value for the entire network M_0 and the average of the metric values at various failure percentages M_i, normalized by M_0 [31]. The metrics of our interest produce quantities that are informative regarding the grade of robustness or resilience that the network in question exhibits in its structure. The ranges of values may vary, although a typical range is the interval from zero to one. It depends on the definition of each metric whether a high or a low value is desirable.

Based on the origin and the concepts studied with each metric, we grouped metrics in the following classes (note that a metric may belong to no group or to more than one group):

Connectivity how the vertices are connected.
Degree specifically, the number of connections per vertex.
Distance the distances between the vertices.
Percolation elimination of elements from the graph.

Centrality the role of an element in the paths that exist in the graph.

Spectral based on the eigenvalues or eigenvectors of a matrix-representation of the graph.

Other types of structural properties is the *searchability* of a network structure [33, 34], based on Shannon's information entropy[1] that seeks to quantify the availability of local information for reaching a specific destination by traversing the network (e.g., with a random walk). This is related to how easy many types of routing problems will be to solve in a given network.

And we identified the following application areas:

Critical infrastructure power grids and transportation.

Telecommunications information sharing, such as telephony or internet.

Supply networks interactions among suppliers, distributors, and consumers.

Biology and Medicine protein and gene networks.

Social networks organizations, epidemics, and online communities

A field not covered by our survey is where structural characterization has direct applications, such as epidemiology [36–40], where vaccination planning, for example, is affected by how the network is formed.

Even though the reviewed metrics can be applied to the design of a network with adequate robustness and resilience, the majority are aimed to the quantification of the robustness present in an existing system, and then using this information to carry out structural improvements or protections. An interesting area of opportunity would be the proposal of metrics that guide the growth of a system during its construction so as to maintain the resilience as high as possible given the budget limitations under which the construction needs to be carried out. Also multi-objective approaches that seek to maximize resilience in terms of multiple measures and visualizations that allow for intuitive analysis of the values of multiple metrics on a single system would be of value.

II. Graph theory

Networked systems consisting of interconnected components are often modeled in terms of graphs. A *graph* is a pair of two sets: the *vertices* (also known as nodes; these represent the components of the system) and the *edges* (also known as connections; these represent links between the components of the system). Each vertex $v \in V$ represents an entity of interest, possibly with an associated vector of properties (such as name, cost, capacity, type), whereas each edge $(u, v) \in V \times V$ connects a vertex $u \in V$ to a vertex $v \in V$ — also the edges may have an associated property vector (representing distance, transfer rate, etc.).

An edge is *directed* if the connection it represents is only operational in one direction — from the source u to the target v — whereas an *undirected* edge represents a bidirectional connection. An edge is *reflexive* if its source and target are the same vertex. A *simple* graph may contain at most one edge per each vertex pair, but a *multigraph* could have more than one edge between a pair of vertices.

The *degree* of a vertex $d(v)$ is the number of edges incident to it, that is, the number of edges that have v as an endpoint. A graph is k-regular if all of its vertices have degree k. For undirected graphs, it does not matter whether v is the source or the target of an edge; for directed graphs, the number of edges with v as the source is called its *out-degree* $d^o(v)$ whereas the number of edges with v as the target is called its *in-degree* $d^i(v)$. The set of vertices adjacent to v in G is denoted by $\Lambda(v)$ and is called the *neighborhood* of v, again with the distinction between $\Lambda^o(v)$ and $\Lambda^i(v)$ for directed graphs.

The *degree sequence* of a graph is a vector formed by the degrees of the vertices and the *degree distribution* refers to the relation between degrees present in the graph and the frequency of each. The *maximum degree* is often denoted by Δ and high-degree vertices are often called *hubs*, especially when the degree distribution is far from uniform. In natural networks, a commonly reported — although frequently disputed — shape of the degree distribution is a *power law* where the frequency of a degree is proportional to a negative power, $\Pr[d(v) = k] \sim k^{-\gamma}$ [11] — such graphs are said to be *scale-free*.

Graphs representing real-world networks are often sparse [12], meaning that the edge set E is a rather small subset of $V \times V$. A common numeric quantity to capture such sparseness of a graph $G = (V, E)$, expressed in terms of $n = |V|$ (called the *order* of the graph) and $m = |E|$ (called the *size* of the graph) is the *average degree*

$$d = m/n, \tag{1}$$

or a close variant of that ratio with the goal of normalizing the quantity to a specific range in terms of whether the edges are directed, reflexive, etc. It is also common to talk about the *density* of a graph as the ratio of the actual graph size and the maximum possible size given the order of the graph; for the undirected and non-reflexive case the common formulation is

$$\delta = \frac{2m}{n(n-1)}, \tag{2}$$

which equals one if all possible pairs of vertices are connected by an edge and zero if no edges are present in the graph.

A *subgraph* S of G has its vertex set as a subset V_S of V and the edge set E_S is a subset of those edges in E that have both endpoints in S; if all such edges are present, the subgraph is said to be *induced*. The density of the subgraph induced by $\Lambda(v)$ is known as the *clustering coefficient* of v, which we denote by $c(v)$; the global average of $c(v)$ computer $\forall v \in V$ is called the clustering coefficient of the graph. A subgraph in which all vertices are connected to all of the other vertices is called a *clique*; graphs with all the possible edges present are said to be *complete*.

A *path* is a sequence of edges that lead from a vertex v to a vertex u. The path is *simple* if it contains no repeated edges. The *path length* is the number of edges contained in a simple path, $\ell(v, u)$, sometimes considered in terms of the number of vertices which is $\ell(u, v) + 1$ if $v \neq u$, whereas if $u = v$, the

[1] *Information entropy* is defined as the negative logarithm of the probability mass function for a given value, that is, the probability of a message being understood by a receiver if a noisy channel was used [35].

path is called a *cycle*. Given a pair of vertices u and v, there may well be several paths in a given graph to connect them; the length of the shortest of those paths is called the *distance* $D(u, v)$. The maximum distance over all pairs of vertices in a graph is called its *diameter*, $\mathcal{D}$. The average distance is, evidently, the average taken over the distances of all pairs of distinct vertices. Also, the distance of a vertex from itself is considered zero as an empty edge sequence is an adequate path. The inverse distance is called the *efficiency* of the vertex pair and the efficiency of a graph is a (possibly normalized) average efficiency over the set of all vertex pairs [13, 14].

A set of vertices that are all connected to one another within a graph is called a (connected) *component*; in directed graphs, strong connectivity refers to paths existing in both directions, whereas k-connectivity refers to the existence of multiple paths that do not share edges and/or intermediate vertices. A graph with only one component is said to be *connected*, whereas one with multiple components is disconnected.

The edges of a graph are easily expressed in terms of an *adjacency matrix* $\mathbf{A}$ where the vertex set is labeled as $V = \{1, 2, \ldots, n\}$ in order to associate the element a_{ij} to whether or not vertices i and j are connected by an edge:

$$a_{ij} = \begin{cases} 1, & \text{if } (i,j) \in E, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

The matrix $\mathbf{D}$ is a diagonal degree matrix derived from $\mathbf{A}$ as row sums:

$$d_{ij} = \begin{cases} d(i), & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

The *Laplacian* matrix

$$\mathcal{L} = \mathbf{I} - \mathbf{D}^{\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}}, \tag{5}$$

where $\mathbf{I}$ is the identity matrix, is an useful tool for studying the structural properties of a graph [15], especially through its *spectrum*, i.e., the eigenvalue sequence $\lambda_1, \ldots, \lambda_n$, ordered such that $\lambda_i \leq \lambda_j$ for $i < j$. For example, the multiplicity of λ_1 is the number of connected components in the graph.

A. Complex networks

In general, introducing *redundancy* into a system may serve to increase its robustness [16], although this evidently tends to increase the costs of building and maintaining the system in question. Besides, redundancy alone is no guarantee of robustness; it is necessary to have a scale-free degree distribution for that to function [17].

Scale-free and bimodal degree distributions have been found more resilient [7, 18], even though there are differences in terms of whether vulnerability against attacks or robustness against failures is desired [17, 19]. As attacks tend to focus on maximizing the damage, regular graphs are less vulnerable due to the lack of obvious targets [20]. Also, just having a uniform degree distribution is helpful if the connectivity is high although the graph is sparse [6]. Also the effect of degree correlations (i.e., the way in which the degrees of the end points of the edges in a graph are correlated) has been studied in relation to resilience [21] — a graph is often said to be *dissortative* if the degrees are negatively correlated over the edge set and *assortative* when edges are mostly found between vertices of similar degrees.

Attempting to modify a system in order to increase its resiliency is a task of *structural optimization* where some objective functions that measure the resilience are optimized by adding, removing, or modifying the vertices and the edges, while a set of constraints (such as location, capacity, cost) are respected [22]. Another alternative for systems that contain smart components that are able to alter their configuration or behavior is to let the system adapt and thus dynamically recover from adverse events. Such an adaptation requires identifying possible threats, generating possible actions for each and estimating their expected impact, selecting and executing an action, and then evaluating its effect in order to determine if adequate recovery has been achieved [23].

An accessible alternative to adaptive or structurally optimized systems is to *simulate* the behavior of a system of interest: identify a potential problem, recreate it in a simulation, and explore possible counteractions to overcome it [24]. In a similar mind-set, the study of complex networks has given rise to a field of research that proposes and analyzes *generators* that artificially produce network topologies with some desired characteristics, such as those of the internet [25]. The classical model of Gilbert [26] as well as that of Erdős and Rényi [27, 28], both of which place edges uniformly at random among the vertices, yield graphs with binomial degree distributions, small average distance, and low local densities. Watts and Strogatz [29] proposed a model that combines a relatively low average distance with high local densities, but maintains the roughly normal shape of the degree distribution. Barabási et al. [30] then proposed a model where the degree distribution is scale-free, the average distances are small, but the local densities are low. From there on, hundreds of generation models have been proposed for all imaginable combinations of structural properties. Using such generators to explore possible system topologies previous to building an actual system is a cost-efficient way to examine the resilience from a system before even deciding how to build it.

In this work, with no attempt towards mathematical rigor, we use the term *metric* to refer to a function that yields a numerical value that can be used as a measurement of how strongly a specific characteristic is present when given as input a network structure, possibly carrying out some modifications on that structure. One common modification is the introduction of a *failure* in one or more of the network's components. For an arbitrary metric M, its *deterioration* can be calculated as the difference between its value for the entire network M_0 and the average of the metric values at various failure percentages M_i, normalized by M_0 [31]. The metrics of our interest produce quantities that are informative regarding the grade of robustness or resilience that the network in question exhibits in its structure. The ranges of values may vary, although a typical range is the interval from zero to one. It depends on the definition of each metric whether a high or a low value is desirable.

For a survey of general structural metrics for networks, including those that are not intended to capture resilience-related characteristics, we refer the reader to the work of da

F. Costa et al. [32]. In this survey, we focus on those that have been used in the literature for the express purpose of determining structural aspects related to the robustness or the resilience of a network. Other types of structural properties that are of practical interest include the *searchability* of a network structure [33, 34], based on Shannon's information entropy[2] that seeks to quantify the availability of local information for reaching a specific destination by traversing the network (e.g., with a random walk). This is related to how easy many types of routing problems will be to solve in a given network. Another field where structural characterization has direct applications is epidemiology [36–40], where vaccination planning, for example, is affected by how the network is formed.

III. Vertex-based metrics

Many vertex-removal metrics are functions of the number of vertices removed from the graph; the definitions can be applied either to as worst-case analysis, average-case analysis, or as repeated random sampling as to which subset of vertices is removed (the removal of different subsets of the same cardinality can have drastically different effects on the graph structure depending on which vertices are removed). Random removal is considered to be a model of *failures* whereas worst-case removal is considered a model of *attack*.

The *connectivity robustness function* [14] is computed by removing (at random) $k \in [0, n]$ vertices from the input graph and computing the order of the largest connected component for each k, normalized by $n - k$ in order to yield values in $[0, 1]$. The study of the connectivity and load balancing in networked systems that undergo eliminations of vertices or edges has been widely studied [2, 22, 42]. The mathematical modelling of the phenomenon is related to that of *percolation* [43].

In addition to mere connectivity concerns in terms of existence of paths, also service-related measures have been proposed: a service-oriented subgraph S is *self-sufficient* with respect to service requests if each service required by $v \in V_S$ can be satisfied by $w \in V_S$. A graph G is said to be *k-failure resilient* in terms of vertices if an arbitrary subset of k or less vertices from G may fail and yet the remaining subgraph is self-sufficient. With these definitions, Rosenkrantz et al. [44] propose a metric for vertex resilience as the largest k for which the network is k-failure resilient. The proposed resilience metric is also applicable on edges: the *edge resilience* of a graph is the largest integer k such that the graph is k edge-failure resilient, meaning that the remaining graph is self-sufficient after the loss of k or less arbitrary edges. These calculations are of exponential complexity.

A metric defined for removals of vertex subsets of cardinality k is the *k-resilience factor* of Salles and Marino [45] which is the percentage of connected induced subgraphs produced by removing $k - 1$ vertices of all possible (connected and disconnected) induced subgraph. Averaging this $\forall k \in [2, n-1]$ yields the *resilience factor*. Note that the number of a possible subgraphs for a graph has exponential asymptotic behavior[3], for which the calculation is computationally demanding for even graphs of moderate order.

If one generalizes from vertex removals to arbitrary perturbations of the graph structure, the calculation can be formulated as computing the difference between the order of the largest connected component in the original graph to that of a perturbed graph, called *perturbation score* [46]. The robustness of different graphs can be compared to each other by applying a similar perturbation to both and computing the difference of the scores thusly obtained. Given two graphs as input, they define *preferential perturbation* as a perturbation that maximises the perturbation in the first graph while minimising it in the second graph. Then, a *maximum perturbation score* can be defined as the maximum of ratio between the preferential perturbation score and the proportion of vertices that are removed.

Another method that takes into account all the vertices instead of only those belonging to the largest connected component is the *pairwise disconnectivity index* [47] which is computed in terms of the number of vertex pairs that are connected in the original graph $\mathcal{P}(V)$: the pairwise disconnectivity index of a vertex v is the number of vertex pairs that remain connected when v is removed from the graph $\mathcal{P}(V \setminus \{v\})$, which could naturally be generalized to removing arbitrary subsets of vertices instead of single vertices.

IV. Edge-based metrics

An alternative to vertex-based approached are metrics that are instead defined in terms of the edges. Mahadevan et al. [21] use the density of the subgraphs induced by the hubs as a robustness measure, whereas Zeng and Liu [48] use the average fraction of edges in the largest connected component after $k \in \{1, \ldots, m\}$ edge removals, as a robustness measure.

Under the assumption that edges connecting vertices of low content-similarity are more significant in maintaining the global connectivity, Cheng et al. [49] propose *bridgeness*, defined as

$$b_e = \frac{\sqrt{S_i S_j}}{S_e}, \tag{6}$$

where i and j are the source and the target vertices of the edge e, and S is the *clique size* corresponding to the specified graph element, i.e., the number of vertices in the largest clique in which it belongs. The upside is that this depends only on local information, and the downside is that finding the maximum cliques is NP hard.

In the presence of edge weights, the computation of metrics including that information becomes an obvious choice. The options for how to proceed are numerous, as many of the vertex-based metrics can be extended to the case of edges, with or without weights, but also the classical *maximum-flow* problem is a promising starting point. It is defined in a weighted graph in the following manner: given a source vertex s and a target vertex t (the latter also known as a

[2] *Information entropy* is defined as the negative logarithm of the probability mass function for a given value, that is, the probability of a message being understood by a receiver if a noisy channel was used [35].

[3] The possible subsets of $n-k$ vertices is the binomial coefficient for n and k, which for all values of $k \in [0, n]$ sum to 2^n, and hence for the proposed range the sum is $2^n - 2n - 1 \in \mathcal{O}(2^n)$.

sink), which is the maximum amount of flow that can be routed from s to t, each edge having flow only in a single direction, and the amount of flow on each edge not exceeding the edge weight (called its *capacity*) [50]. Notice that the sum of incoming flows must equal the sum of outgoing flows $\forall v \in V \setminus \{s,t\}$ and the sum of outgoing flow at s must equal that of the incoming flow of t. A well-known solution for the maximum-flow problem is the Ford-Fulkerson algorithm [51]. This solution is valid not only for simple graphs but also for multigraphs, having all flows respecting the edge orientation.

Based on the maximum-flow problem, Pien et al. [52] propose the *relative area index* of a vertex in terms of a parameter u and the maximum flow at that vertex $F^v_{max}(u)$, where the parameter u controls the capacity reduction either in relative or absolute terms, with u_0 being the smallest possible value, and u_T being the largest possible value. Supposing that the flow at a vertex is monotonically decreasing in u, the relative area index can be computed as

$$\frac{\int_{u_0}^{u_T} w(u)(F^v_{\max}(u_0) - F^v_{\max}(u))du}{\int_{u_0}^{u_T} w(u)F^v_{\max}(u_0)du}, \tag{7}$$

where $w(u)$ is a weight function over u.

A variant of looking at single edges is computing things in terms of the number of edges at a vertex, that is, degree-based metrics. Schneider et al. [53] a metric for a degree-based attack where the vertices are eliminated from the highest degree to the lowest (with or without recalculating the degrees after vertex removals) and after each elimination, the order of the largest connected component C_t at that moment is computed; the sum of C_t over $t = 1, \ldots, n$ is then normalized by n and used as a robustness measure. Wang et al. [54] propose the entropy of the degree distribution as a measure. Yet another option is *vertex load* defines as the degree of a vertex multiplied by the sum of the degrees of its neighbors elevated to a power, the exponent being a tunable parameter [55].

V. Subgraph-based metrics

Many proposed metrics are based on elements of a higher level: the nature of subgraphs of various kinds is used to characterize the resilience or the robustness. In this section, we briefly review proposals of this category.

A. Paths

A common way to characterize graph structure is by computing the distances over all vertex pairs (for example with the Floyd-Warshall algorithm, which has complexity $\mathcal{O}(n^3)$ [51]). Upon knowing the distance matrix and immediately available data derived from that such as the average distance and the diameter, other more complex calculations can be carried out to characterize the network.

Li et al. [56] define *delta efficiency* as the average of the differences in efficiency over all vertex pairs after a vertex removal and further define*fragility* of a system as the average delta efficiency over single-vertex removals. Their proposed *dynamic robustness metric* is a weighted version of this: the average delta efficiency over all vertices, weighted by the failure probability of each vertex.

Zhang et al. [57] study the loss of functionality under attack terms of the individual functionalities of vertices as follows. Define the initial *functionality* of a vertex v as one: $\forall v \in V : F_0 = 1$. Then, define the functionality of v *after* attack number i that eliminates vertex v_i is defined as

$$F_i(v) = F_{i-1}(v) - \frac{1}{D(v,v_i)^2 d(v)} F_{i-1}(v), \tag{8}$$

where the distances and the degrees are computed after the attack number $k-1$. Zhang et al. [57] then define *functionality loss* as the sum of the differences of vertex functionality before and after the attack over the sequence of k attacks,

$$L(v) = \sum_{i=1}^{k} F_{i-1}(v) - F_i(v). \tag{9}$$

The *global functionality loss* is then measured as

$$\sum_{v \in V, v \notin A} L(v), \tag{10}$$

where $A = \{v_1, v_2, \ldots, v_k\}$ is the set of vertices removed in the attack sequence. This also would allow an extension to consider edge removals instead of vertex removals.

Another, quite popular measure based on paths is the *betweenness* of a vertex or an edge: the number of shortest paths is computed for the element of interest (using fractions when more than one path of minimum length exists) over all vertex pairs in the graph [58]. As this becomes a computational burden for large graphs, estimation methods based on random walks have been proposed [59].

Scellato et al. [60] propose a metric based on *temporal efficiency*, defined in terms of the way in which the efficiency (in terms of the average path length) of a graph degrades (as a percentage of the original efficiency) after damage is made (such as vertex or edge removals or lowering the level of functionality at a vertex or an edge if the graph is modelling some system in which the elements may be partially operative).

A way to quantify path *diversity* [10] takes as input the shortest (or otherwise optimal) path P_0 and another alternative path P and computes

$$D(P) = 1 - \frac{|P \cap P_0|}{|P_0|}, \tag{11}$$

where the path may be represented either as a set of vertices visited on it or the set of edges it traverses.

Piraveenan et al. [61] denotes, at time t, a non-percolation state of vertex v by $x^t_v = 0$ and a fully percolated state by $x^t_v = 1$, while a partially percolated state corresponds to $0 < x^t_v < 1$. The fraction

$$\frac{x^t_v}{[\sum_{u \in V} x^t_u] - x^t_w} \tag{12}$$

indicates the contribution of s to the total percolation, excluding v.

Piraveenan et al. [61] define a *percolated path* as a shortest path from $v \in V$ to $w \in V$ such that v is infected, and

then the *percolation centrality* of a vertex as the proportion of percolated paths that go through it of all (percolated or not) paths:

$$PC^t(v) = \frac{1}{N-2} \sum_{s \neq v \neq r} \frac{\sigma_{s,r}(v)}{\sigma_{s,r}} \frac{x_s^t}{[\sum x_i^t] - x_v^t}. \quad (13)$$

If each vertex has the same level of percolation > 0, $\frac{x_s^t}{[\sum x_i^t]-x_v^t}$ becomes $\frac{1}{N-1}$, then $PC^t(v) = BC(v)$, where $BC(v)$ is the betweenness centrality of that vertex.

Xin and Yang [62] propose *subgraph centrality* (S_C), defined as the sum of closed walks at all vertices in the graph. The main idea of this metric is that a set of closed walks are able to denote all the alternative routes between vertices in a graph. If there exist more alternative routes between any pair of vertices, the system is more robust. Given the adjacency matrix A, it applies for the eigenvalues $\lambda_1 \leq ... \leq \lambda_n$, S_C that

$$S_C = \sum_{k=1}^{\infty} \sum_{i=1}^{n} (A^k)_{ii} = \sum_{k=1}^{\infty} \sum_{i=1}^{n} \lambda_i^k, \quad (14)$$

and using a Taylor series $e^x = \sum_{k=0}^{\infty} x^k/k!$, a finite approximation is achieved:

$$\begin{aligned} S_C &= \log_e \left(\sum_{i=1}^{n} \sum_{k=1}^{\infty} \frac{\lambda_i^k}{k!} \right) \\ &\approx \left(\sum_{i=1}^{n} \sum_{k=0}^{\infty} \frac{\lambda_i^k}{k!} \right) \\ &= \left(\sum_{i=1}^{n} e^{\lambda_i} \right). \end{aligned} \quad (15)$$

B. Other types of subgraphs

Vodák et al. [63] propose determining, for a given k, the average number of edges that need to be removed to break the graph into k connected components, whereas Tang et al. [64] propose the *random-robustness index* computed as a normalized sum of the size of the largest connected component (generalizable to be computed over a single attack or a sequence of attacks, where each attack results in a removal of one or more vertices or edges). Another approach is to study the *communities* (also known as *clusters*) that are present in a graph [65, 66]; Ma et al. [67] compute *community robustness* as follows: compute for each community the proportion of vertices that survive an attack, and average this over the set of communities for a single attack or a sequence of attacks.

Sáenz-de Cabezn and Wynn [68] define metrics bases on *minimum vertex cover*; $V' \subseteq V$ is a vertex cover if $\forall e \in E$ it applies that $V' \bigcap e \neq \emptyset$ (thinking of the edge as a set of its endpoints) and the smallest such cover is the minimum vertex cover. They define the *covering degree* of $v \in V$ as the number of minimal vertex covers that contain v and the *covering index* of v as the number of minimum vertex covers that contain v plus the ratio of the number of minimal vertex covers that contain v to the total number of minimal vertex covers of G. They find that both of these metrics perform better than using vertex degree and/or betweenness centrality for attacks in graphs where no index recalculation is allowed.

VI. Spectral metrics

In addition to the classes of metrics discussed in the previous section, also ones that are based on computing the graph spectra (eigenvalues, eigenvectors, or both) have been proposed.

Generalized robustness index [69] approximates the normalized subgraph centrality (NSC). For each vertex i in the graph, given an eigenvalue-eigenvector pair $(\lambda_i, \mathbf{u}_i)$, NSC is defined $\forall i \in V$ as

$$\text{NSC}_k(i) = \sum_{j=1}^{k} u_{i,j}^2 \sinh(\lambda_j) \quad (16)$$

where k is the number of the eigenvalues that will contribute to the approximation of the subgraph centrality and $u_{i,j}$ is the jth element of the eigenvector $\mathbf{u}_i$. Based on the normalized subgraph centrality NSC_k of each vertex $i \in V$, they define the generalized robustness index r_k of a graph as

$$\sqrt{\frac{1}{|V|} \sum_{i=1}^{|V|} \left(\log u_{i,1} - \left(\log \sinh^{-1/2} \lambda_1 + \frac{\log \text{NSC}_k(i)}{2} \right) \right)^2}. \quad (17)$$

Delvenne and Libert [70] propose the *entropy rank*, defined for an aperiodic, strongly connected, and unweighted graph as the asymptotic stationary probability distribution of a surfer that visits each link with a given probability such that each walk is equally probable, regardless of the initial state, computed from the dominant eigenvectors of the adjacency matrix. They also define the *free energy rank* for directed, unweighted graphs by using instead a matrix in which zeroes have been substituted by a very small constant as is done in PageRank calculations [71]). Such ranks could then be used in a manner similar to which the betweenness measures of vertices and edges are used to define resilience metrics.

Based on the formulation of Estrada [72] where a weighted sum of the number of closed walks in a graph (S) is obtained from the powers of the adjacency matrix as

$$S = \sum_{i=1}^{n} e^{\lambda_i} \quad (18)$$

where n is the number of vertices and λ_i are the eigenvalues, Yi-Lun [73] formulate *local natural connectivity* as

$$\overline{\lambda} = \ln \left(\frac{1}{n} \sum_{i=1}^{n} e^{\lambda_i} \right), \quad (19)$$

which corresponds to the average eigenvalue of the graph. If a graph G has k connected components named $G_1, ..., G_k$ with $n_1, ..., n_k$ vertices respectively. Be the spectrum of all partitions G_i noted by $\lambda_{i1}, ..., \lambda_{in_i}$, thus the natural connectivity $\overline{\lambda}$ of G can be decomposed as follows:

$$\overline{\lambda} = \ln \left(\frac{1}{n} \sum_{i=1}^{k} n_i e^{\overline{\lambda_i}} \right), \quad (20)$$

where

$$\min\{\overline{\lambda_1}, ..., \overline{\lambda_k}\} \leq \overline{\lambda} \leq \max\{\overline{\lambda_1}, ..., \overline{\lambda_k}\}. \quad (21)$$

Wu et al. [74] study the redundancy of alternative paths as a measure of network robustness — their interest lies in

ensuring that a path remains between vertices in spite of network damage — and find that the number of closed walks (i.e., paths that start and end in the same vertex) in a graph is a good indicator for the existence of alternative paths. Thus, considering that shorter closed walks have more influence on the redundancy of alternative paths than longer ones, authors scale the contribution of closed walks to the redundancy of alternative paths by dividing them by the factorial of the length k, that is:

$$S = \sum_{k=0}^{\infty} \frac{n_k}{k!} \tag{22}$$

where n_k is the number of closed walks of length k. Estrada [72] demonstrates that Eq. (22) can be written as

$$S = \sum_{j=1}^{n} e^{\lambda_j}, \tag{23}$$

where λ_j is the j-th eigenvalue of the adjacency matrix of G. Therefore, Wu et al. [74] define the mean eigenvalue as

$$\bar{\lambda} = \ln\left(\frac{S}{n}\right) = \ln\left(\frac{\sum_{n}^{j=1} e^{\lambda_j}}{n}\right) \tag{24}$$

which is a normalized version of the *local natural connectivity*.

The *reconstructability coefficient* [75] is a metric based in, for sufficiently large number of vertices, a portion a of the smallest eigenvalues (in absolute value) can be removed from the spectrum and the adjacency matrix is still reconstructable with its original eigenvectors. The maximum number of eigenvalues that can be set to zero (removed from the spectrum) that still permits the adjacency matrix be reconstructed exactly is the reconstructability coefficient. In the spectral domain, the more "robust" the graphs, the less spectral bases eigenvectors are needed to reconstruct the graphs.

Youssef et al. [76] propose a metric called *viral conductance* based on the spread of susceptible-infected-susceptible (SIS) epidemics on networks: an infected vertex can infect susceptible neighbors or cure itself and become susceptible to re-infection. Denoting the number of infected vertices in the population pf size N at time t by $Y(t)$, $y(t) = Y(t)/N$ represents the fraction of infected vertices. Viral conductance is then defined as

$$\int_0^{\rho} y_{\infty}(s)ds = \rho \bar{y_{\infty}}, \tag{25}$$

where y_{∞} is the function that satisfies the time evolution of SIS epidemics, ρ is the spectral radius (i.e., the maximum eigenvalue) of the adjacency matrix of G (requiring $y_{\infty}(\rho) = 0$, the reciprocal of the epidemic threshold) and $\bar{y_{\infty}}$ is the average value of the fraction of infected vertices for all $0 \leq s \leq \rho$.

VII. Applications

The application areas where measuring resilience and robustness are numerous, starting for a good planing of cities aiming to avoid infrastructure bottlenecks (roads, commute, airports), protecting networks from major catastrophes, and to understand the reason after a major outage.

For instance, the US-Canadian power grid outage and the Italian blackout (2003) [77], the 2006 earthquake in Taiwan which disrupted undersea fiber optic communication lines and resulted in banks from South Korea to Australia suffered massive interruptions [78], the 2010 earthquake in Chile which dismembered national Internet connection [79], and an old lady cutting Armenian Internet access in 2011 [80] are examples of outages which could be avoided by a good robustness analysis.

In this section, we discuss in greater detail a handful of examples presented in our literature review, focusing on those that have received more attention in the literature.

A. Critical infrastructure

The operation of critical infrastructure requires planning and preparation for interruptions, and the ability to respond to crises efficiently. For example, the design of detours upon traffic work or accidents as well as the planning of evacuations [2, 81] are related to the resilience and robustness of road networks.

In a *transportation network*, the edges represent the links (road or railroad segments, flights, etc.), and each edge has an associated weight that models the amount of traffic on that edge, it is called the *flow*. When the flows are known, *vehicle-hours of travel* (VHT) can be computed as the weighted sum of the flows over the edges, using the travel times as weights, at an equilibrium. A transportation network is at *equilibrium* when it is not possible to any of its users to reduce their travel times by an unilateral change of route (cf. a game-theoretical equilibrium) [82].

Now, if an edge is added or removed, the VHT will change, and the magnitude of that change can be used as a metric for the impact of that edge — note that eliminating an edge does not only affect the flow on that edge but may force changes on flows along other edges in order for an equilibrium to be reached. Novak et al. [83] propose a metric called *network trip robustness*, computed as the sum of the changes in VHT over all edges, normalized by the total demand of the graph.

When the system under study transports something (whether physical goods or network traffic), it is not enough to model and characterize the structure of the system but also the dynamics of the load itself need to be taken into account. Murray-Tuite [9] addresses the modeling of arrival processes and measurement of queue lengths and waiting times for such systems.

In *telecommunication networks* [21], where possible service interruptions include hardware failure, weather-related issues, as well as intentional malicious attacks. As in transportation networks, telecommunication networks usually have more than one possible route for each transfer, and the routing of traffic over multiple options is a relevant problem as such [84, 85].

Tizghadam and Leon-Garcia [86] define *criticality* (for vertices or edges) as the *random-walk betweenness* of an element over the weight of that element. The random-walk betweenness for an element for a given source-destination pair is the expected value of the number of passes on that element for a random walk that initiates at the source before reaching

the destination. Summing this over all possible pairs gives the random-walk betweenness of the element. *Network criticality* then becomes a sum over the critical of its elements.

Cheng et al. [87] propose a formulation in terms of network flow. Based on the idea that network components adjacent to an attack centre fail with a high probability, while those away from the centre linearly decrease in the failure probability, they propose the global graph resilience metric *compensated Total Geographical Graph Diversity (cTGGD)* that characterizes the geographical diversity for different physical network topologies.

Geographical diversity is defined as the minimum distance between any vertices along a given path and the nearest vertex in the shortest path. That is, $D(P_a)$ such that $D \geq d$ is defined as the minimum (geographical) distance between any vertex members of path P_a and that of the shortest path (excluding source and destination vertices). Then, for a given alternative paths between the vertex pair (s, d), the *effective geographical path diversity* (EGPD) is defined as the total (weighted) utility of the alternative simple paths

$$\text{EGPD} = 1 - e^{\lambda k_{sd}} \tag{26}$$

where λ is a constant to weight the utility of alternative paths and k_{sd} is the sum of each path's geographical diversity:

$$k_{sd} = \sum_{i=1}^{m} D(P_i) \tag{27}$$

Total graph geographical diversity (TGGD) is then defined as the average of the EGPD value of all vertex pairs within that graph, and *compensated total geographical graph diversity* (cTGGD) as TGGD weighted by the total number of links of the Graph.

Pien et al. [52] study the European air traffic network (ATN). Specifically, the flight assignments under capacity restrictions (airport capacities and en-route airspace) given the increasing demand for flights (expected to increase by 2.5% between 2015 and 2021). Considering the ATN as a graph where vertices are airports and links among them the flight routes, authors proposed the Relative Area Index (RAI) as a robustness index. The RAI is calculated via linear programming based on the change in the maximum network flows, that is:

$$\text{RAI}^i = \frac{\int_{u_0}^{u_T} w(u)(F^i_{\max}(u_0) - F^i_{\max}(u))du}{\int_{u_0}^{u_T} w(u)F^i_{\max}(u_0)du}, \tag{28}$$

where $F^i_{\max}(u)$ is the maximum network flow when a capacity reduction expressed by u is applied to vertex i and $w(u)$ is a weight factor to assigns different priorities to different ranges of capacity reductions, depending of the studied problem, such as vertex of interest or different scenarios.

Murray-Tuite [9] studies vehicular traffic assignments by four resilience dimensions: adaptability, mobility, safety, and the ability to recover quickly; presenting multiple resilience metrics for the given dimensions. Examples of such metrics are: the percentage of total vehicles that used an specific lane (adaptability), the number of vehicles exposed to hazards (security), the amount of time required to evacuate town's residents (mobility), and the amount of time, money, and outside assistance required to restore connectivity at an acceptable level of service (recovery).

The *relative entropy* or *Kullback-Leibler distance* of two probability density functions $p(x)$ and $q(x)$ is defined as

$$D\left(\frac{p}{q}\right) = \sum_{x \in A} p(x) \log \frac{p(x)}{q(x)}; \tag{29}$$

relative entropy is a measure of the distance between two random distributions and in statistics, it corresponds to the logarithm expectation of likelihood ratios. Typically, $p(x)$ represents a true distribution, while $q(x)$ represents a theoretical distribution. Feng and Wang [88] proposes that $p(x)$ will be deemed the railway network distribution being studied, and $q(x)$ will be treated as the railway network with a completely disordered distribution. Therefore, using relative entropy to measure robustness, $q(x)$ is defined as uniform degree distribution $1/N$ (disordered network) and $p(x)$ the actual degree distribution of the network. Eq. (29) then becomes

$$D(p) = \sum_{x \in V} p(x) \log(Np(x)). \tag{30}$$

Pahwa et al. [89] propose the idea of "*intentional islanding of a power system*", that is an emergency response for isolating failures that might propagate and lead to major disturbances. The main idea is to partition power grids into islands to minimize the load shedding not only in the region where the failures start, but also in the topological complement of the region, avoiding cascading failures. To obtain the islands, authors solved the optimization problem, the formulation considers two parts of the system, the island (the region where the initial failure occurs) and the topological complement of the island. This technique aims at minimizing load shedding in both, the island and also its topological complement. Also, to limit the failure to a small portion of the system, the objective includes the minimization of the island size. However, the optimization problem is not scalable and in its best case its resolution method is $\mathcal{O}(N^5)$.

Ko et al. [90] propose a network robustness metric for *power grids* as the sum of *electrical nodal robustness* and *significance* of each vertex. The electrical nodal robustness of a vertex is the sum of the normalized power flow (measured in Watts (W)) values of each link connected to that vertex, weighted by the logarithm of this normalized power flow and the tolerance parameter α_i of that link:

$$R_{n,i} = -\sum_{i=1}^{L_i} \alpha_i p_i \log(p_i), \tag{31}$$

where L_i are the set size of the links connected to the vertex i. The minus sign $(-)$ is used to compensate the negative electrical nodal robustness value that occurs due to logarithm of normalised flow values. The tolerance parameter of a link is simply the inverse of the loading level of an arbitrary line i, which is the ratio between the load and the maximum capacity of the corresponding line. The load is often measured as the link betweenness centrality and the capacity of a line is defined

as the maximum power flow that can be carried by the line. The electrical nodal *significance* on the other hand is the power distributed by a vertex, normalized by the sum of all power distributed by all vertices.

Ko et al. [91] also work with *effective graph resistance* computed as the sum of all the effective resistances between all pairs in a network. It is a measure of electrical path length between two vertices that uses a weighted Laplacian matrix,

$$R_{ij} = L^+_{ii} - 2L^+_{ij} + L^+_{jj}, \tag{32}$$

where M^+ is the Moore-Penrose pseudo-inverse of the matrix M.

B. Supply-chain management

Supply chains that are linear flows of goods from suppliers to customers, and can be modeled as "*supply networks*", where a supply network is a graph of vertices of two kinds: supply (or supplier) and demand (or requester) vertices. Main problems related to supply networks are: how to fulfill a given demand, what happens in route failures, what happens if there are production issues, or, more in general, what happens with the supply network's performance in case of a major catastrophic event [92].

Zhao et al. [93] propose measuring *supply availability* as the percentage of demand vertices with direct access at least one supply vertex and *best delivery efficiency* as the reciprocal of the average of length of the shortest supply paths of the demand vertices. Furthermore, they define *average delivery efficiency* in terms of the inverse length of supply paths, averaged over all possible demand-supply vertex pairs, and *network connectivity* where at least one supply vertex needs to be present at each connected component.

Plagányi et al. [94] propose the supply chain index that computes for each component of a supply chain the proportion of product received from each supplier (thinking of these as flows), and the weighs these by the square of the proportion of product that flows into that receiver, summing over all components.

C. Biology and medicine

In biology and medicine, biological systems are modeled as mutation paths, and the structure (and robustness) of such networks is studied. For instance, Quayle et al. [46] study the robustness to perturbation for a pair of non-directional networks, motivated by applications in cancer network modeling. The main idea is how to create a maximal perturbation in a network while in the other is minimal, achieving what they called a "*preferential perturbation*". Authors defined then the *Average perturbation gradient*, that is, the ratio of maximum perturbation score divided with the number of vertices removed.

Tagore and De [95] study biochemical reactions present in organisms. They noticed that if any one of the paths for production of the same metabolite is hampered, an alternate path tries to overcome this defect and helps in combating the damage. Thus, they simulated attacks over the mutation pathways networks having metabolites represented by a vertex in the graph, and edges representing reaction links.

Authors defined two robustness metrics, the *Random Resilience Score* which is the ratio of number of metabolites removed randomly until the power-law network property breaks, to the total number of metabolites; and *Targeted Resilience Score*, which is the ratio of number of metabolites removed by a targeted attack until power-law network property breaks.

D. Social networks

Robustness metrics applied to social networks has been widely studied before, for instance in the study of trust [96], the effects of missing data [97], leadership [98], etc.

Fragmentation (F) [99] The ratio between the number of pairs of vertices that are not connected in the fragmented network after removing a fraction q of vertices by the total number of pairs in the original fully connected network. The idea behind Fragmentation is to apply the fundamentals of percolation theory to social networks, comparing F with a traditional measure used in percolation theory P_∞ (the fraction of vertices in the largest cluster relative to the total number of vertices). Authors found that, for a network obtained after removal a fraction q of vertices above the percolation threshold, $P_\infty \approx (1-F)^{1/2}$.

Sensitivity [100] Given n variables, $t_1, \ldots, t_n$ representing the weighted degree of each vertex and a centrality function C such that $C(t_v)$ is the centrality measure for the vertex v Sensitivity of the vertex i with respect of the vertex j is defined as

$$s_{ij} = \frac{\partial C_i(t_1, \ldots, t_n)}{\partial t_j}. \tag{33}$$

As many centrality metrics are algebraic operations on the adjacency matrix, the derivative is expanded in terms of the derivatives of the adjacency matrix, using

$$\frac{\partial C(A)}{\partial t} = \frac{dC}{dA}\frac{\partial A}{\partial t}. \tag{34}$$

The main advantage of using derivatives to visual analysis is their cost: approximating the derivative using finite differences implies a cost proportional to $\mathcal{O}(|V|)$ instead of, for instance $\mathcal{O}(|V|^3)$, if betweenness centrality is calculated.

VIII. Open problems and future directions

Although the reviewed metrics can be applied to the design of a network with adequate robustness and resilience, the majority are aimed to the quantification of the robustness present in an existing system, and then using this information to carry out structural improvements or protections. An interesting area of opportunity would be the proposal of metrics that guide the growth of a system during its construction so as to maintain the resilience — present and future — as high as possible given the budget limitations under which the construction needs to be carried out. Also multi-objective approaches that seek to maximize resilience in terms of multiple measures and visualizations that allow for intuitive analysis of the values of multiple metrics on a single system would be of value.

TABLE II
A COMPARATIVE STUDY OF EXISTING METRICS.

Article	Event		Quantity		Removal of		Impact measurement			
	Failure	Attack	Isolated	Sequence	Vertex	Edge	Components	Paths	Service	Other
Yang et al. [14]	✓	☞	✓	✓	✓	☞	order	✗	✗	
Rosenkrantz et al. [44]	✓	☞	✓	✓	✓	✓	✗	✗	✓	
Salles and Marino [45]	✓	☞	✓	✓	✓	☞	number	✗	✗	
Quayle et al. [46]	☞	✓	✓	☞	✓	☞	order	✗	✗	
Potapov et al. [47]	☞	✓	✓	☞	✓	☞	✗	number	✗	
Pien et al. [52]	✓	✓	✓	✗	✓	✗	✗	flow	✓	
Schneider et al. [53]	✗	✓	☞	✓	✓	☞	order	✗	✗	
Wang et al. [54]*	✓	☞	✓	✓	✓	☞	✗	✗	✗	degree, entropy
Wang and Rong [55]*	✓	✓	✓	☞	✓	☞	✗	✗	✗	degree, entropy
Li et al. [56]	✓	✓	✓	☞	✗	✓	✗	✓	✗	
Zhang et al. [57]	✓	✓	✓	✗	✓	☞	✗	distances	✗	
Scellato et al. [60]	✓	☞	✗	✓	✓	☞	✗	distances	✗	
Piraveenan et al. [61]	✓	✓	✓	☞	✓	✗	✗	distances	states	
Xin and Yang [62]	✓	✓	✓	☞	✓	☞	✗	spectral	✗	
Vodák et al. [63]	✓	✓	✓	✓	☞	✓	✓	✗	✗	
Tang et al. [64]	☞	✓	☞	✓	✓	✓	✓	✗	✗	
Ma et al. [67]	☞	✓	☞	✓	✓	☞	communities	✗	✗	
Sáenz-de Cabezn and Wynn [68]	✗	✓	✓	☞	✓	✗	number, order	✗	✗	
Malliaros et al. [69]	✗	✗	✗	✗	✗	✗	✗	spectral	✗	
Delvenne and Libert [70]	✗	✗	✗	✗	✗	✗	✗	spectral	✗	
Yi-Lun [73]	✓	✓	✓	☞	✗	✓	✗	spectral	✗	
Wu et al. [74]	✓	✓	✓	☞	✗	✓	✗	spectral	✗	
Liu et al. [75]	☞	✓	✗	✗	✗	✗	✗	spectral	✗	
Youssef et al. [76]	✗	✗	✗	✗	✗	✗	✗	spectral	✗	
Novak et al. [83]	✗	✗	✓	✓	✗	✓	✗	flow	✓	
Tizghadam and Leon-Garcia [86]	✗	✗	✓	✗	✓	✓	✗	random walks	✗	
Cheng et al. [87]	✓	☞	☞	✓	✓	☞	✗	flow	✓	
Feng and Wang [88]*	✓	✓	✓	☞	✓	☞	✗	✗	✗	deg entropy
Pahwa et al. [89]	✓	✓	✗	✗	✗	✗	communities	✗	✓	
Ko et al. [90]	☞	✓	✓	☞	☞	✓	✗	flow	✓	
Ko et al. [91]	☞	✓	✓	☞	☞	✓	✗	flow	✓	
Zhao et al. [93]	✓	✓	✓	☞	✓	☞	✓	✓	✓	
Plagányi et al. [94]	✓	✗	✓	✗	✓	✓	✗	flow	✓	
Tagore and De [95]*	✓	☞	✓	☞	✓	✗	✗	✗	✗	degree, entropy
Correa et al. [100]*	✗	✓	✓	✗	✗	✓	✗	✗	✗	degree, entropy

The columns indicate, in order, the type of disturbance (random failure or a deliberate attack), what graph elements are removed in the disturbance, and in terms of which aspect the impact is quantified.
We mark by ✓ the ones present, by ✗ the ones absent, and by ☞ those that are not included in the proposal but that would be natural extensions of the proposal.

Many of the proposed metrics lack theoretical understanding as only limited computational experiments are reported. Studying their theoretical foundations would also permit determining which are variants of others and whether they are correlated or otherwise dependent. For those metrics that have high computational cost, approximations calculated from samples (for example by carrying out random walks in the analyzed graph) would be of practical use, especially if the approximation ratios were mathematically established.

IX. CONCLUSIONS

This survey concentrates on the existing proposals for quantifying resilience and robustness of networked systems in terms of the properties of the graphs that represent them. Such concepts are formulated to capture the capability of recovery from failures and attacks as well as the ability to resist them. Existing literature has an abundant selection of metrics that have been proposed for this task; many are based on iteratively removing elements of the graph (mainly vertices or edges) and computing a function that in some fashion measures the structural integrity of the remaining graph after each elimination. Common measurements include the effect of the removals on the paths or flows present in the graph (in terms of their number, redundancy, length, or connectivity) as well as spectral properties (i.e., eigenvalues of the adjacency matrix).

The application areas for resilience metrics are numerous; we mention, among others, works related to transport, telecommunications, supply chains, biological systems, and social networks. For example, a robust network of highways is minimally affected by an incident that disables some lanes of traffic, a robust supply chain quickly recovers from a delayed delivery, and a resilient power grid prevents a single failure from cascading to other parts of the system.

TABLE I
LIST OF METRICS WITH THEIR COMPUTATIONAL COMPLEXITY (CC).

Name of the metric	Ref.	Year	CC
Aggregated remaining flow	[87]	2015	$\mathcal{O}(n^4)$
Average delivery efficiency	[93]	2011	$\mathcal{O}(n^4)$
Average perturbation gradient	[46]	2006	$\mathcal{O}(n^2)$
Best delivery efficiency	[93]	2011	$\mathcal{O}(n^3)$
Bridgeness	[101]	2010	$\mathcal{O}(3^{n/3})$
Community Robustness	[67]	2013	$\mathcal{O}(n^3)$
Compensated total graph geographical diversity	[87]	2015	$\mathcal{O}(n^6)$
Connectivity robustness function	[14]	2013	$\mathcal{O}(n)$
Covering degree	[68]	2014	$\mathcal{O}(3^{n/3})$
Covering index	[68]	2014	$\mathcal{O}(3^{n/3})$
Deterioration	[31]	2013	variable
Dynamic robustness metric	[56]	2012	$\mathcal{O}(n^3)$
Effective geographical path diversity	[87]	2015	$\mathcal{O}(n^4)$
Effective graph resistance	[91]	2014	$\mathcal{O}(n^3)$
Efficiency function	[14]	2013	$\mathcal{O}(n^3)$
Entropy rank	[70]	2011	$\mathcal{O}(n^3)$
Entropy of the degree distribution	[54]	2006	$\mathcal{O}(n)$
Fragility	[56]	2012	$\mathcal{O}(n^3)$
Fragmentation	[99]	2007	$\mathcal{O}(n)$
Free energy rank	[70]	2011	$\mathcal{O}(n^3)$
Generalized robustness index	[69]	2015	$\mathcal{O}(n^3)$
Geographical path diversity	[87]	2015	$\mathcal{O}(n^6)$
Global functionality loss	[57]	2011	$\mathcal{O}(n^4)$
Link robustness index	[48]	2012	$\mathcal{O}(nm)$
Local natural connectivity	[73]	2011	$\mathcal{O}(n^3)$
Maximum perturbation score	[46]	2006	$\mathcal{O}(n^2)$
Natural connectivity	[74]	2011	$\mathcal{O}(n^3)$
Network connectivity	[93]	2011	$\mathcal{O}(n^3)$
Network criticality	[86]	2010	$\mathcal{O}(n^3)$
Network robustness metric	[90]	2013	$\mathcal{O}(n^3)$
Network trip robustness	[83]	2012	$\mathcal{O}(n^4)$
Vertex load	[55]	2009	$\mathcal{O}(n^2)$
Vertex/edge criticality	[86]	2010	$\mathcal{O}(n^3)$
Vertex/edge resilience	[44]	2009	$\mathcal{O}(n^2)$
Normalized aggregated remaining flow	[87]	2015	$\mathcal{O}(n^4)$
Pairwise disconnectivity index	[47]	2008	$\mathcal{O}(n^3)$
Percolation centrality	[61]	2013	$\mathcal{O}(n^3)$
Perturbation score	[46]	2006	$\mathcal{O}(n)$
Preferential perturbation score	[46]	2006	$\mathcal{O}(n)$
Random resilience score	[95]	2011	$\mathcal{O}(n^2)$
Random-robustness index	[64]	2015	$\mathcal{O}(n^2)$
Reconstructability coefficient	[75]	2010	$\mathcal{O}(n^3)$
Relative area index	[52]	2015	$\mathcal{O}(n^2m)$
Relative entropy	[88]	2013	$\mathcal{O}(n)$
Resilience Factor	[45]	2011	$\mathcal{O}(2^n)$
Sensitivity	[100]	2012	variable
Subgraph centrality	[62]	2012	$\mathcal{O}(n^3)$
Supply availability	[93]	2011	$\mathcal{O}(n^3)$
Supply chain index	[94]	2014	$\mathcal{O}(n)$
Targeted resilience score	[95]	2011	$\mathcal{O}(n^2)$
Temporal efficiency	[60]	2013	$\mathcal{O}(n^3)$
Total graph geographical path diversity	[87]	2015	$\mathcal{O}(n^4)$
Unique robustness Measure	[53]	2011	$\mathcal{O}(n^2)$
Viral conductance	[76]	2011	$\mathcal{O}(n^3)$

Future challenges include the theoretical analysis of the proposed metrics and their relationships as well as the development of quickly-computable while yet precise approximations to lower the cost of the analysis, as well as the proposal of methods that guide the construction of a new network towards resilience instead of simple analyzing an existing one. A tool for interactive visualizations of multiple resilience metrics for large graphs would be especially welcome both those who apply the metrics on real-world systems.

ACKNOWLEDGMENT

This work was partially funded by CORFO 15BPE-47225: "Estudio y recomendaciones sobre la resiliencia de la infraestructura del internet chileno".

REFERENCES

[1] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," *Physical Review Letters*, vol. 85, p. 4626, 11 2000.

[2] D. M. Scott, D. C. Novak, L. Aultman-Hall, and F. Guo, "Network robustness index: A new method for identifying critical links and evaluating the performance of transportation networks," *Journal of Transport Geography*, vol. 14, pp. 215–227, 05 2006.

[3] E. K. Morlok and D. J. Chang, "Measuring capacity flexibility of a transportation system," *Transportation Research Part A: Policy and Practice*, vol. 38, pp. 405–420, 07 2004.

[4] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Physical Review Letters*, vol. 86, p. 3682, 04 2001.

[5] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted disruptions," *IEEE Systems Journal*, vol. 5, pp. 28–39, 03 2011.

[6] E. Estrada, "Network robustness to targeted attacks. the interplay of expansibility and degree distribution," *The European Physical Journal B*, vol. 52, pp. 563–574, 08 2006.

[7] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H. E. Stanley, "Optimization of network robustness to waves of targeted and random attacks," *Physical Review E*, vol. 71, p. 047101, 2005.

[8] P. Smith, D. Hutchison, J. P. G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: A systematic approach," *IEEE Communications Magazine*, vol. 49, pp. 88–97, 07 2011.

[9] P. M. Murray-Tuite, "A comparison of transportation network resilience under simulated system optimum and user equilibrium conditions," in *Proceedings of the 2006 Winter Simulation Conference*, L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, and D. M. N. R. M. Fujimoto, Eds. IEEE, 2006, pp. 1398–1405.

[10] J. P. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network

resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommunication Systems*, vol. 52, pp. 705–736, 02 2013.

[11] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[12] E. D. Demaine, F. Reid, P. Rossmanith, F. S. Villaamil, S. Sikdar, and B. D. Sullivan, "Structural sparsity of complex networks: Bounded expansion in random models and real-world graphs," arXiv.org, techreport arXiv:1406.2587, 06 2014.

[13] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, p. 198701, 2001.

[14] T. Yang, Z. Lin, and B. Yuan, "A betweenness calibration topology optimal control algorithm for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, 2013.

[15] F. R. K. Chung, *Spectral Graph Theory*, ser. CBMS Regional Conference Series On Mathematics. American Mathematical Society, 1997, vol. 92.

[16] H. Huang and J. A. Copeland, "A series of Hamiltonian cycle-based solutions to provide simple and scalable mesh optical network resilience," *IEEE Communications Magazine*, vol. 40, pp. 46–51, 11 2002.

[17] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 07 2000.

[18] B. Bollobás and O. Riordan, "Robustness and vulnerability of scale-free random graphs," *Internet Mathematics*, vol. 1, no. 1, pp. 1–35, 2004.

[19] ——, "Robustness and vulnerability of scale-free random graphs," *Internet Mathematics*, vol. 1, pp. 1–35, 2003.

[20] A. H. Dekker and B. D. Colbert, "Network robustness and graph topology," in *Proceedings of the 27th Australasian conference on Computer science*, vol. 26. Australian Computer Society, Inc., 2004, pp. 359–368.

[21] P. Mahadevan, D. Krioukov, M. Fomenkov, B. Huffaker, X. Dimitropoulos, K. C. Claffy, and A. Vahdat, "The internet AS-level topology: three data sources and one definitive metric," *ACM SIGCOMM Computer Communication Review*, vol. 36, pp. 17–26, 01 2006.

[22] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A: Statistical Mechanics and its Applications*, vol. 357, pp. 593–612, 11 2005.

[23] P. Cholda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk, "A survey of resilience differentiation frameworks in communication networks," *IEEE Communications Surveys & Tutorials*, vol. 9, pp. 32–55, 10 2007.

[24] A. Schaeffer-Filho, P. Smith, A. Mauthe, D. Hutchison, Y. Yu, and M. Fry, "A framework for the design and evaluation of network resilience management," in *Proceedingsof the IEEE Network Operations and Management Symposium*. IEEE, 2012, pp. 401–408.

[25] A. Medina, I. Matta, and J. Byers, "On the origin of power laws in Internet topologies," *ACM Computer Communication Review*, vol. 30, no. 2, pp. 18–28, 2000.

[26] E. N. Gilbert, "Random graphs," *Annals of Mathematical Statistics*, vol. 30, no. 4, pp. 1141–1144, 1959.

[27] P. Erdős and A. Rényi, "On random graphs I," in *Selected papers of Alfréd Rényi*. Akadémiai Kiad, 1976, vol. 2, pp. 308–315, first publication in 1959.

[28] ——, "On the evolution of random graphs," in *Selected papers of Alfréd Rényi*. Akadémiai Kiad, 1976, vol. 2, pp. 482–525, first publication in 1960.

[29] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small world' networks," *Nature*, vol. 393, pp. 440–442, 1998.

[30] A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," *Physica A: Statistical Mechanics and its Applications*, vol. 272, pp. 173–187, 1999.

[31] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Y. Zomaya, "On the characterization of the structural robustness of data center networks," *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 1–1, 2013.

[32] L. da F. Costa, F. A. Rodrigues, G. Travieso, and P. Villas Boas, "Characterization of complex networks: A survey of measurements," *Advances in Physics*, vol. 56, no. 1, pp. 167–242, 2007.

[33] M. Rosvall, A. Trusina, P. Minnhagen, and K. Sneppen, "Networks and cities: An information perspective," *Physical Review Letters*, vol. 94, no. 2, p. 028701, 01 2005.

[34] K. Sneppen, A. Trusina, and M. Rosvall, "Hide-and-seek on complex networks," *Europhysics Letters*, vol. 69, no. 5, pp. 853–859, 2005.

[35] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423 & 623–656, July & Oct. 1948.

[36] C. Moore and M. E. J. Newman, "Epidemics and percolation in small-world networks," *Physical Review E*, vol. 61, no. 5, pp. 5678–5682, 2000.

[37] S. A. Pandit and R. E. Amritkar, "Characterization and control of small-world networks," *Physical Review E*, vol. 60, no. 2, pp. R1119–R1122, 1999.

[38] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[39] R. Cohen, S. Havlin, and D. ben Avraham, "Efficient immunization strategies for computer networks and populations," *Physical Review Letters*, vol. 91, no. 24, p. 247901, 12 2003.

[40] M. Boguá, R. Pastor-Satorras, and A. Vespignani, "Epidemic spreading in complex networks with degree correlations," in *Statistical Mechanics of Complex Networks*, ser. Lecture Notes in Physics, R. Pastor-Satorras, M. Rubi, and A. Diaz-Guilera, Eds., vol. 625. Springer-Verlag GmbH, 2003, pp. 127–147.

[41] B. Kitchenham, "Procedures for performing systematic reviews," Keele University, techreport TR/SE-0401, 07 2004.

[42] 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, 12 2000.

[43] M. E. J. Newman and D. J. Watts, "Scaling and percolation in the small-world network model," *Physical Review E*, vol. 60, no. 6, pp. 7332–7342, 1999.

[44] D. J. Rosenkrantz, S. Goel, S. Ravi, and J. Gangolly, "Resilience metrics for service-oriented networks: a service allocation approach," *IEEE Transactions on Services Computing*, vol. 2, no. 3, pp. 183–196, 2009.

[45] R. M. Salles and D. A. Marino, "Strategies and metric for resilience in computer networks," *The Computer Journal*, p. bxr110, 2011.

[46] A. Quayle, A. Siddiqui, and S. Jones, "Preferential network perturbation," *Physica A: Statistical Mechanics and its Applications*, vol. 371, no. 2, pp. 823–840, 2006.

[47] A. P. Potapov, B. Goemann, and E. Wingender, "The pairwise disconnectivity index as a new metric for the topological analysis of regulatory networks," *BMC bioinformatics*, vol. 9, no. 1, p. 227, 2008.

[48] A. Zeng and W. Liu, "Enhancing network robustness against malicious attacks," *Physical Review E*, vol. 85, no. 6, p. 066130, 2012.

[49] X.-Q. Cheng, F.-X. Ren, H.-W. Shen, Z.-K. Zhang, and T. Zhou, "Bridgeness: a local index on edge significance in maintaining global connectivity," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2010, no. 10, p. P10011, 2010.

[50] A. Schrijver, "On the history of the transportation and maximum flow problems," *Mathematical Programming*, vol. 91, no. 3, pp. 437–445, 2002.

[51] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. McGraw-Hill Book Co., 2001.

[52] K.-C. Pien, K. Han, W. Shang, A. Majumdar, and W. Ochieng, "Robustness analysis of the european air traffic network," *Transportmetrica A: Transport Science*, vol. 11, no. 9, pp. 772–792, 2015.

[53] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[54] B. Wang, H. Tang, C. Guo, and Z. Xiu, "Entropy optimization of scale-free networks robustness to random failures," *Physica A: Statistical Mechanics and its Applications*, vol. 363, no. 2, pp. 591–596, 2006.

[55] J.-W. Wang and L.-L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability," *Physica A: Statistical Mechanics and its Applications*, vol. 388, no. 7, pp. 1289–1298, 2009.

[56] L. Li, Q.-S. Jia, H. Wang, R. Yuan, and X. Guan, "A systematic method for network topology reconfiguration with limited link additions," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1979–1989, 2012.

[57] J. Zhang, X. Xu, L. Hong, S. Wang, and Q. Fei, "Networked analysis of the Shanghai subway network, in China," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 23, pp. 4562–4570, 2011.

[58] M. E. J. Newman and M. Girvan, "Mixing patterns and community structure in networks," in *Proceedings of the XVIII Sitges Conference on Statistical Mechanics in Barcelona, Spain*, ser. Lecture Notes in Physics, R. Pastor-Satorras and J. Rubi, Eds. Springer-Verlag, Berlin, Germany, 2002, to appear in 2003.

[59] M. E. J. Newman, "A measure of betweenness centrality based on random walks," arXiv.org e-Print archive, techreport cond-mat/0309045, 2003.

[60] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer, "Evaluating temporal robustness of mobile networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 105–117, 2013.

[61] M. Piraveenan, M. Prokopenko, and L. Hossain, "Percolation centrality: Quantifying graph-theoretic impact of nodes during percolation in networks," *PloS one*, vol. 8, no. 1, p. e53095, 2013.

[62] Y. Xin and W. Yang, "Topological and spectral perturbations in complex networks," *Chinese Physics Letters*, vol. 29, no. 12, p. 128901, 2012.

[63] R. Vodák, M. Bl, and J. Sedonk, "Network robustness and random processes," *Physica A: Statistical Mechanics and its Applications*, vol. 428, pp. 368–382, 2015.

[64] X. Tang, J. Liu, and M. Zhou, "Enhancing network robustness against targeted and random attacks using a memetic algorithm," *EPL (Europhysics Letters)*, vol. 111, no. 3, p. 38005, 2015.

[65] S. Fortunato, "Community detection in graphs," *Physics Reports*, vol. 486, pp. 75–174, 2010.

[66] S. E. Schaeffer, "Graph clustering," *Computer Science Review*, vol. 1, no. 1, pp. 27–64, 2007.

[67] L. Ma, M. Gong, Q. Cai, and L. Jiao, "Enhancing community integrity of networks against multilevel targeted attacks," *Physical Review E*, vol. 88, no. 2, p. 022810, 2013.

[68] E. Sáenz-de Cabezn and H. P. Wynn, "Measuring the robustness of a network using minimal vertex covers," *Mathematics and Computers in Simulation*, vol. 104, pp. 82–94, 2014.

[69] F. D. Malliaros, V. Megalooikonomou, and C. Faloutsos, "Estimating robustness in large social graphs," *Knowledge and Information Systems*, vol. 45, no. 3, pp. 645–678, 2015.

[70] J.-C. Delvenne and A.-S. Libert, "Centrality measures and thermodynamic formalism for complex networks," *Physical Review E*, vol. 83, no. 4, p. 046117, 2011.

[71] A. N. Langville and C. D. Meyer, *Google's PageRank and Beyond: The Science of Search Engine Rankings*. Princeton University Press, 2011.

[72] E. Estrada, "Characterization of 3D molecular structure," *Chemical Physics Letters*, vol. 319, no. 5, pp. 713–718, 2000.

[73] S. Yi-Lun, "Local natural connectivity in complex networks," *Chinese Physics Letters*, vol. 28, no. 6, p. 068903, 2011.

[74] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 41, no. 6, pp. 1244–1252, 2011.

[75] D. Liu, H. Wang, and P. Van Mieghem, "Spectral perturbation and reconstructability of complex networks," *Physical Review E*, vol. 81, no. 1, p. 016101, 2010.

[76] M. Youssef, R. Kooij, and C. Scoglio, "Viral conductance: Quantifying the robustness of networks with respect to spread of epidemics," *Journal of Computational Science*, vol. 2, no. 3, pp. 286–298, 2011.

[77] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout-root causes and dynamics of recent major blackouts," *IEEE Power and Energy Magazine*, vol. 4, no. 5, pp. 22–29, 2006.

[78] J. Herskovitz, "Taiwan quake exposes weakness of undersea data lines," *Reuters*, Dec. 2006. [Online]. Available: http://www.itpro.co.uk/100966/taiwan-quake-exposes-weakness-of-undersea-data-lines

[79] V. Ramiro, J. Piquer, T. Barros, and P. Sepúlveda, "The Chilean internet: Did it survive the earthquake?" *WIT Transactions on State-of-the-art in Science and Engineering*, vol. 58, p. 19, 2012.

[80] T. Parfitt, "Georgian woman cuts off web access to whole of Armenia," *The Guardian*, Apr. 2011. [Online]. Available: https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access

[81] E. Jenelius, T. Petersen, and L.-G. Mattsson, "Importance and exposure in road network vulnerability analysis," *Transportation Research Part A: Policy and Practice*, vol. 40, pp. 537–560, 08 2006.

[82] J. G. Wardrop, "Road paper. some theoretical aspects of road traffic research." in *ICE Proceedings: engineering divisions*, vol. 1. Thomas Telford, 1952, pp. 325–362.

[83] D. C. Novak, J. L. Sullivan, and D. M. Scott, "A network-based approach for evaluating and ranking transportation roadway projects," *Applied geography*, vol. 34, pp. 498–506, 2012.

[84] A. Tizghadam and A. Leon-Garcia, "Autonomic traffic engineering for network robustness," *IEEE Journal on Selected Areas in Communications*, vol. 28, pp. 39–50, 01 2010.

[85] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing*. Kluwer Academic Publishers, 1998.

[86] A. Tizghadam and A. Leon-Garcia, "Autonomic traffic engineering for network robustness," *IEEE journal on selected areas in communications*, vol. 28, no. 1, pp. 39–50, 2010.

[87] Y. Cheng, M. T. Gardner, J. Li, R. May, D. Medhi, and J. P. Sterbenz, "Analysing GeoPath diversity and improving routing performance in optical networks," *Computer Networks*, vol. 82, pp. 50–67, 2015.

[88] F. Feng and L. Wang, "Robustness measure of chinas railway network topology using relative entropy," *Discrete Dynamics in Nature and Society*, vol. 2013, 2013.

[89] S. Pahwa, M. Youssef, P. Schumm, C. Scoglio, and N.Schulz, "Optimal intentional islanding to enhance the robustness of power grid networks," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 17, pp. 3741–3754, 09 2013.

[90] Y. Ko, M. Warnier, R. E. Kooij, and F. M. Brazier, "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety science*, vol. 59, pp. 126–134, 2013.

[91] Y. Ko, M. Warnier, P. Van Mieghem, R. E. Kooij, and F. M. Brazier, "The impact of the topology on cascading failures in a power grid model," *Physica A: Statistical Mechanics and its Applications*, vol. 402, pp. 169–179, 2014.

[92] M. Shinozuka, S. E. Chang, T. chung Cheng, M. Feng, T. D. ORourke, M. A. Saadeghvaziri, X. Dong, X. Jin, Y. Wang, and P. Shi, *Resilience of Integrated Power and Water Systems*. MCEER Earthquake Engineering to Extreme Events, 2003, pp. 65–67. [Online]. Available: http://mceer.buffalo.edu/publications/resaccom/04-SP01/06_shino.pdf

[93] K. Zhao, A. Kumar, and J. Yen, "Achieving high robustness in supply distribution networks by rewiring," *IEEE Transactions on Engineering Management*, vol. 58, no. 2, pp. 347–362, 2011.

[94] É. E. Plagányi, I. Van Putten, O. Thébaud, A. J. Hobday, J. Innes, L. Lim-Camacho, A. Norman-Lpez, R. H. Bustamante, A. Farmery, A. Fleming *et al.*, "A quantitative metric to identify critical elements within seafood supply networks," *PloS one*, vol. 9, no. 3, p. e91833, 2014.

[95] S. Tagore and R. K. De, "Detecting breakdown points in metabolic networks," *Computational biology and chemistry*, vol. 35, no. 6, pp. 371–380, 2011.

[96] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys*, vol. 45, no. 4, p. 47, 2013.

[97] G. Kossinets, "Effects of missing data in social networks," *Social networks*, vol. 28, no. 3, pp. 247–268, 2006.

[98] L. Lü, Y.-C. Zhang, C. H. Yeung, and T. Zhou, "Leaders in social networks, the delicious case," *PloS one*, vol. 6, no. 6, p. e21202, 2011.

[99] Y. Chen, G. Paul, R. Cohen, S. Havlin, S. P. Borgatti, F. Liljeros, and H. E. Stanley, "Percolation theory applied to measures of fragmentation in social networks," *Physical Review E*, vol. 75, no. 4, p. 046107, 2007.

[100] C. Correa, T. Crnovrsanin, and K.-L. Ma, "Visual reasoning about social networks using centrality sensitivity," *IEEE transactions on visualization and computer graphics*, vol. 18, no. 1, pp. 106–120, 2012.

[101] X.-Q. Cheng, F.-X. Ren, H.-W. Shen, Z.-K. Zhang, and T. Zhou, "Bridgeness: a local index on edge significance in maintaining global connectivity," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2010, no. 10, p. P10011, 2010.

Fernando Morales was born in Chile in 1990. He received his M.Sc. degree in 2017 from Universidad de Chile. His research interests include complex networks, internet protocols, and network robustness.

Elisa Schaeffer was born in Finland in 1976. She received her M.Sc. degree in 2017 in Computer Science and Engineering at Universidad de Chile. Her research interests include all aspects of complex networks, often modeled in terms of graph theory, particularly structural characterization, algorithmic aspects, and optimization.

Ivana Bachmann was born in Chile in 1990. He received his M.Sc. degree in 2017 in Computer Science at Universidad de Chile, and is currently a PhD. candidate in Computer Science at the same university. In 2014, she joined NIC Chile Research Labs as a research assistant. Her research interests include modeling and robustness of complex networks and their applications.

Javiera Figols was born in Chile in 1990. She is part of the M.Sc. in Applied Mathematics degree from Universidad de Chile. Her research interests include graph theory and computational complexity.

Javier Bustos-Jiménez was born in Chile in 1976. He received his D.Sc. degree in 2006 from Universit Nice Sophia Antipolis (thesis developed in OASIS team at INRIA). In 2012 he joined NIC Chile Research Labs as Director. His research interests include complex networks, internet protocols, network privacy/security, and data science.