Evaluating Network Vulnerability with the Mincuts Frequency Vector

Stéphane Bulteau, Gerardo Rubino

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Evaluating network vulnerability with the mincuts frequency vector

Stéphane Bulteau, Gerardo Rubino

N ° 3125

Mars 1997

THÈME 1

ISSN 0249-6399

INRIA
RENNES

Evaluating network vulnerability with the mincuts frequency vector

Stéphane Bulteau*, Gerardo Rubino †

Thème 1 — Réseaux et systèmes
Projet Model

Rapport de recherche n ° 3125 — Mars 1997 — 29 pages

Abstract: We consider the problem of evaluating the behavior of a communication network face to the possible disruption of some of its components. We are interested in the case when there is no available statistical information about the dependability properties of the network components. Instead of working with reliability metrics in a stochastic context, we analyze vulnerability measures in a deterministic framework. This approach allows us to propose a solution to other classes of problems (not easily handled in reliability theory). For instance, we can consider the problem of evaluating the capacity of a network to resist to external attacks. We can also address the problem of quantifying the network ability to satisfy some capacity constraints in transporting information. In the paper, we propose a definition of vulnerability allowing the numerical evaluation of these aspects of a communication system. We show that it verifies some intuitively desirable properties, which is not the case of previously proposed means of vulnerability analysis. Last, we discuss the algorithmic issues related with the evaluation of the proposed metric.

Key-words: communication networks, vulnerability, reliability, network design

(Résumé : tsvp)

* Email: sbulteau@irisa.fr
† Email: rubino@irisa.fr

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : (33) 02 99 84 71 00 – Télécopie : (33) 02 99 84 71 71

Evaluation de la vulnérabilité d'un réseau par le vecteur de coupes minimales

Résumé : Nous considérons le problème de l'évaluation du comportement d'un réseau de communication face à la défaillance possible de certains de ses composants. Nous nous intéressons au cas où nous ne disposons pas d'informations statistiques sur les composants du réseau. Au lieu de travailler avec des mesures de fiabilité, dans un contexte stochastique, nous étudions des mesures de vulnérabilité, dans un contexte déterministe. Cette approche permet de proposer une solution à d'autres types de problèmes, difficilement traités dans la théorie de la fiabilité. Par exemple, nous pouvons considérer le problème de l'évaluation de la résistance du réseau face à une aggression externe. On peut également évaluer l'habilité du réseau à satisfaire certaines contraintes de capacité dans le transport de l'information. Dans ce papier, nous proposons une définition de la vulnérabilité autorisant l'évaluation numérique de ces aspects d'un système de communication. Nous montrons qu'elle vérifie un certain nombre de propriétés intuitivement souhaitables, ce qui n'était pas le cas des mesures précédemment proposées. Finalement, nous discutons l'aspect algorithmique relatif à l'évaluation de la mesure proposée.

Mots-clé : réseau de communication, vulnérabilité, fiabilité, conception de réseau

1 Introduction

The behavior of a communication network when some of its components fail is unambiguously handled by the so-called *network reliability* theory. The framework is a stochastic one, in which the analyst builds a model around the concept of graph and includes the available statistical information about the dependability properties of the components (nodes, channels) and possibly of the users (offered traffic). This data together with the knowledge of the *structure* of the network leads to the definition of many useful *reliability metrics* and to the development of algorithmic solutions to the problem of how these metrics can be evaluated. More specifically, the network can be, for instance, represented by an undirected multi-graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges representing the bi-directional communication channels. In the sequel, we will speak simply about graphs, but all the results shown here are valid in case of more than one edge between the same pair of nodes. With each edge i we can associate a probability r_i, its *(elementary) reliability*. This means that each line is either operational (state coded by 1) or non operational (state coded by 0) and that the probability to find edge i in the operational state is r_i. Furthermore, we assume, as usual, that the different random variables "state of line i" are independent and, for simplicity, that nodes are perfect. The most widely studied reliability measure in such a context assumes that two particular nodes s (the *source*) and t (the *terminal*) are fixed and that we are interested in the communications between them. This leads to consider the event "there is at least a path between s and t having all its edges operational (an *operational path*)". The probability of this event is the reliability $R_{s,t}$ of the system, called *source-to-terminal reliability*. There are many available algorithms to compute this metric (see [1, 2]). If we are concerned with the possible communications between all pairs of nodes, then we deal with the *all-terminal reliability* R_{all}, which is the probability that there is at least one operational path relying any pair of vertices. An important problem with these metrics and with their extensions is that in almost all the contexts of interest, their evaluations are NP-hard problems.

Assume now that statistical information about the behavior of the components is not available. In this case, we see two alternatives to still perform an analysis of the system. One can build possible scenarios by setting the set of elementary reliabilities to different values and answer "what if" questions. This can give insight into the properties of the studied system, for instance allowing the user to identify weak points in the network topology. The other approach, which is the main subject of this paper, is to obtain useful information from the topology of the network only, by studying *vulnerability* metrics instead of reliability ones.

Let us consider the communications between nodes s and t. Intuitively speaking, a network is vulnerable with respect to source–terminal communications, if it is "easy" to disconnect those nodes, that is, if the fact that a "few" components of the network are down makes that there are no more operational paths between s and t. The problem relies of course in the meaning to assign to the words "easy" and "few". Consider, for instance, the two examples in Figure 1. Network 1b

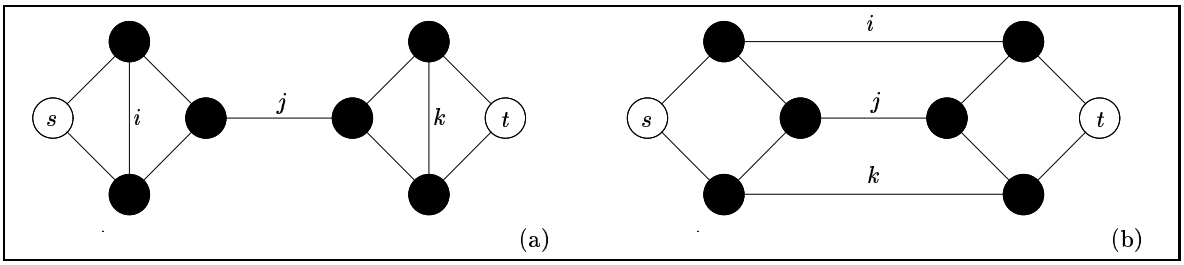

Figure 1: A first example

is a modification of 1a obtained by changing the position of lines i and k. Due to the bridge j in 1a, anyone will prefer network 1b, as far as communications between s and t are considered. The problems are mainly two: first, how to quantify the differences between the topologies in order, for instance, to compare two alternative options; second, how to do with less trivial cases. This is the goal of the paper.

We will denote by $V(\mathcal{G})$ a vulnerability measure of an undirected graph $\mathcal{G}$. If we consider only the communications between nodes s and t, we will speak about *source-to-terminal* vulnerability, or *2-terminal* vulnerability, and the associated measure will be denoted by $V_{\mathrm{s,t}}()$. In case of being concerned by communications between any pair of nodes, the measure is the *all-terminal* vulnerability, denoted by $V_{\mathrm{all}}()$.

The contents of this work, which is an extension of a previous work presented in [3], is the following. In next section, we discuss the main properties that a vulnerability index should have. In Section 3, we briefly recall previous attempts to work with the vulnerability concept. The problem here is that none of the metrics that have been proposed in the literature satisfy the minimal set of properties discussed in Section 2. Section 4 presents a new vulnerability measure and we show that it has the properties listed in Section 2. In Section 5, we prove that the measure verifies another property, which is particularly useful for the applications. In Section 6, it is discussed how one can extend the metric in a natural way, to handle other problems

involving supplementary data about the network. We give numerical examples in Section 7 and the last section is devoted to some concluding remarks.

2 Desirable properties for a vulnerability measure

A first point of this paper is the claim that a vulnerability measure should satisfy a minimum number of properties to be really meaningful. We list here what we think the most important ones are:

(i) *Ordering.* First, we must be able to use it to *compare* two different topologies, that is, the set of vulnerability values must be *ordered.*

(ii) *Monotonicity.* Second, the measure must have the following monotonicity property: if we denote by $\mathcal{G}+e$ the network obtained by adding the edge e to $\mathcal{G}$, and if $V()$ is the vulnerability measure, we should have

$$V(\mathcal{G}+e) \leq V(\mathcal{G}).$$

This follows from the underlying idea of what we want to represent, that is, the "resistance" of the topology when some of the components fail, its "robustness" or its "weakness", etc. Under these English words there is the idea that, given the fact that we are interested in the network support to allow communications between pair of nodes, deleting edges makes the system more "vulnerable", that is, worse than before.

(iii) *Globality.* Third, the measure must be *global* enough. What we mean is that, for instance, it must allow us to distinguish between the two networks in Figure 2 (and it should say that 2a is less vulnerable than 2b, because of the monotonicity property). In other words, even if both networks in Figure 2 have a similar "weakness" around the edge adjacent to the only node with degree one, we can naturally desire that the first one, due to its higher density, be less vulnerable than the second.

Formally, let x be an articulation point of $\mathcal{G}$, that is, when we delete x and its adjacent edges, the resulting graph denoted by $\mathcal{G}-x$ has at least 2 connected components $\mathcal{G}_1$ and $\mathcal{G}_2$. Assume that a new graph $\mathcal{G}'$ is defined by replacing $\mathcal{G}_1$ by $\mathcal{G}'_1$ in $\mathcal{G}$. We want that

$$\text{if } V(\mathcal{G}'_1) \geq V(\mathcal{G}_1), \text{ then } V(\mathcal{G}') \geq V(\mathcal{G}).$$

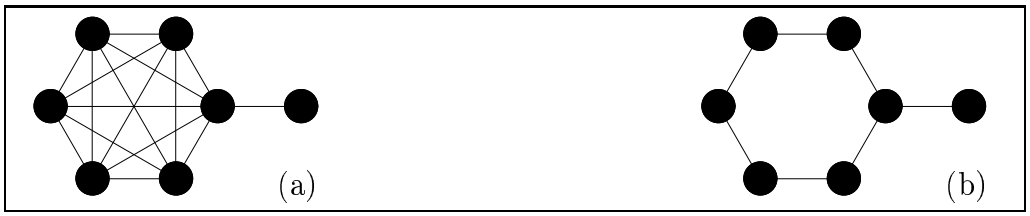

Figure 2: A second example

If we are more specific about the fact that we speak about 2-terminal or all-terminal vulnerability, then we can be more precise. For the all-terminal case, if $V_{\text{all}}(\mathcal{G}'_1) > V_{\text{all}}(\mathcal{G}_1)$, then we want that $V_{\text{all}}(\mathcal{G}') > V_{\text{all}}(\mathcal{G})$. In the 2-terminal case, we must take into account where the two fixed nodes s and t are. If s and t belong to $\mathcal{G}_2$, then we want that $V(\mathcal{G}') = V(\mathcal{G})$ whatever happens with $\mathcal{G}_1$. And if $s \in \mathcal{G}_1$ and $t \in \mathcal{G}_2$, then if $V_{s,x}(\mathcal{G}'_1) > V_{s,x}(\mathcal{G}_1)$ then we want that $V_{s,t}(\mathcal{G}') > V_{s,t}(\mathcal{G})$.

Let us observe that, probably, other variants of (iii) can be defined using different particular subgraphs, but we will limit ourselves in the paper to biconnected components (or, more precisely, to union of biconnected components as $\mathcal{G}_1$ above).

This set of properties seems to be minimal. A supplementary point is that it is clearly useful to be able to consider both the source-to-terminal case and the all-terminal one, as it is done in reliability theory. From this point of view, we consider that the following property is necessary in the 2-terminal case:

(iv) Given two graphs $\mathcal{G}_1$ and $\mathcal{G}_2$ and a pair of nodes marked in each, s_1, t_1 in $\mathcal{G}_1$, s_2, t_2 in $\mathcal{G}_2$, let us define the series graph $\mathcal{G}_s$ as the graph obtained by identifying, say, nodes t_1 and s_2, and the parallel graph $\mathcal{G}_p$ obtained by identifying, say, nodes s_1 and s_2, and nodes t_1 and t_2. We then want that

$$V_{s_1,t_2}(\mathcal{G}_s) \geq V_{s_1,t_1}(\mathcal{G}_1) \qquad \text{and} \qquad V_{s_1,t_2}(\mathcal{G}_s) \geq V_{s_2,t_2}(\mathcal{G}_2),$$

and that

$$V_{s,t}(\mathcal{G}_p) \leq V_{s_1,t_1}(\mathcal{G}_1) \qquad \text{and} \qquad V_{s,t}(\mathcal{G}_p) \leq V_{s_2,t_2}(\mathcal{G}_2).$$

Even if other possibilities exist that can be justified as these, we will show in next section that no previous proposal to measure the vulnerability of a network

satisfy (i) to (iii). All other proposals verify (i), since they all use integers or reals as vulnerability metrics. The problems are with the remaining, and from our point of view, important properties. It must also be added that most previous effort was concentrated on the all-terminal case only.

The goal of our research was to find a way of measuring vulnerability satisfying the given minimal set of properties. The result is described in Section 4. Not only the proposed index verifies properties (i) to (iv), but it has also other interesting supplementary characteristics (see Section 5 and Section 6). It can also handle both the source-to-terminal and the all-terminal cases, or the general $\mathcal{K}$-terminal case, where $\mathcal{K}$ is any subset of nodes. In the paper, we study the metric in the two main cases $V_{\mathrm{s,t}}()$ and $V_{\mathrm{all}}()$.

3 Previous work on the vulnerability concept

As we have seen in the introduction, the underlying idea under the concept of "vulnerability" is connectivity. For this reason, let us recall here the definition of *mincut* which will be central in the following. An s,t-cut is a set of edges, denoted by $(X,\overline{X})$, where X is a subset of nodes containing either s or t but not both and $\overline{X}$ is its complement: it is defined as the subset of edges having one extremity in X and the other one in $\overline{X}$. An s,t-mincut is an s,t-cut not containing (strictly) any other s,t-cut. A (min)cut is an s,t-(min)cut for some pair s,t.

For any subset of nodes $\mathcal{V}' \subseteq \mathcal{V}$, let us denote $\mathcal{E}_{\mathcal{V}'} = \{(u,v) \in \mathcal{E} \text{ s.t. } u,v \in \mathcal{V}'\}$. The pair $(\mathcal{V}', \mathcal{E}_{\mathcal{V}'})$ defines the graph induced by $\mathcal{V}'$ in $\mathcal{G}$. A key result about mincuts is the following: if $\Gamma = (X,\overline{X})$ is an s,t-cut in $\mathcal{G}$, then Γ is an s,t-mincut of $\mathcal{G}$ if and only if both $(X,\mathcal{E}_X)$ and $(\overline{X},\mathcal{E}_{\overline{X}})$ are connected.

From the vulnerability point of view, perhaps the most natural idea is to use the *edge connectivity* c of the underlying graph as a measure, also called the *breadth* of the graph, that is, the minimum cardinality of an edge disconnecting set. It is in fact an *invulnerability* metric, since we prefer high values rather than low ones (to have a measure of vulnerability, we can use, for instance, $1/c$). The problem with c is that it is not global enough: it insists too much on a local weakness of the network. For instance, with this definition, network 1a in Figure 1 and a series with extremities s and t would have the same vulnerability with respect to communications between s and t ($c = 1$ in both cases), and, nevertheless, we intuitively "feel" that they are not equivalent from the "vulnerability" point of view, and thus, we should want to differentiate them. In fact, we want that the measure says that network 1b is better than 1a also in the all-terminal case. In Figure 2, we also have the same value $c = 1$

when considering the all-terminal case, and network 2a appears more "robust" than network 2b.

When considering the parameter c as a measure, it is interesting to relate it to the reliability framework. Assume that every line has the same elementary reliability r. The network reliability (either source-to-terminal or all-terminal, or even more general reliability metrics) is then a polynomial in r. Writing $r = 1 - \varepsilon$ (since the usual situation is $\varepsilon \approx 0$), and using a Taylor expansion, R can be written

$$R = 1 - n_c \varepsilon^c + O(\varepsilon^{c+1})$$

where n_c is the number of mincuts of (minimal) size c (see for instance [1]). This expression can be very accurate when used to approximate the reliability of a network composed of highly reliable components (see [2]). It suggests that the number of mincuts could also be a possible relevant or useful parameter in our context. We can observe that it is also rather local; in the two graphs given in Figure 2, we have $n_c = 1$ (and $c = 1$ as well). One of the objectives of our proposal is to avoid this.

An interesting idea is to use this comparison with reliability to calibrate or to validate a vulnerability metric proposal. That is, to try to obtain that the more reliable a network is, the less vulnerable it is. But it is not that easy, because of the so-called *crossing reliabilities* problem [4]. Let us consider two networks $\mathcal{G}_1$ and $\mathcal{G}_2$ with the same number of nodes and edges. Assume that all the lines have the same elementary reliability r and let us denote by $R_1(r)$ and $R_2(r)$ the respective network reliabilities. For some values r', r'' of r, it is possible to have $R_1(r') < R_2(r')$ and $R_1(r'') > R_2(r'')$. The consequence is that in order to use the reliability as a reference, a value of r must be fixed. The natural choice is to consider r close to one. In that case, we are in the situation discussed before, where the relevant parameters are c and n_c, and, as we have shown, this is not good enough for our purposes.

Other attempts to capture the vulnerability concept have been proposed, based on the distance between nodes. For example, looking at the communication between every pair of nodes, Bollobás [5] suggests to use the *diameter*, that is, the maximum length of shortest paths between any two nodes. The diameter is not rich enough. For instance, in a series of m edges between two nodes x, y, the diameter is m, and it is also equal to m if we put, say, k paths in parallel between x and y, each with, for instance m edges. Even adding "vertical" edges between these parallel paths does not change the diameter of the graph. Consider now a graph $\mathcal{G}$ with an articulation point x such that by deleting x, we obtain three connected components, $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_3$ with diameters d_1, d_2 and d_3 respectively, such that $d_1 \leq \min(d_2, d_3)$. If you replace $\mathcal{G}_1$ by any graph with diameter $d \leq \min(d_2, d_3)$, you obtain the same vulnerability (even if $d > d_1$ or $d < d_1$).

Having observed that the diameter, as a vulnerability measure, is poor in many cases, Boesch and *al.* [6] analyze the *line-persistence*, defined as the minimum number of edges that must be removed in order to increase the diameter or to disconnect the network. As an invulnerability index, this parameter does not verify the property of monotonicity. The line-persistence of the complete graph with n nodes, K_n, is equal to 1, whereas the line-persistence of $K_n - e$ is $n - 2$.

More complex metrics have also been built starting from this type of parameters, with the objective of improving the accuracy. Following this line, Soi and Aggarwal [7] proposed to identify a set of graph parameters that could be *a priori* relevant to the vulnerability concept, and to divide them into two classes, $\mathcal{C}_1$ and $\mathcal{C}_2$. For each parameter p, they decide if the vulnerability metric should be increasing or decreasing when p increases. In the first case, $p \in \mathcal{C}_1$ and $p \in \mathcal{C}_2$ in the second. Then, some simple function of the selected parameters is chosen, such that it is non decreasing on variables in $\mathcal{C}_1$ and non increasing on variables in $\mathcal{C}_2$. For instance, a simplified version of their metric is

$$v = \frac{d}{c} + \frac{N}{M}$$

where N is the number of nodes, M is the number of edges and d is the diameter.

This type of approach can be of practical interest, but its inherent complexity makes difficult to obtain a function satisfying the set of suggested properties. For instance, let us show that property (iii) can be violated. Let us consider the two graphs a and b on Figure 3, with $v_a = 3 + \frac{6}{8} = v_b$. In each graph, the grey nodes are articulation points leading to two connected components. In both cases, there is a biconnected component composed by only one edge. The vulnerabilities of the other components are respectively $v'_a = 1 + \frac{5}{7} < 2 + \frac{5}{7} = v'_b$. Then, this measure does not verify the property (iii), that is, it is not global enough. Let us illustrate

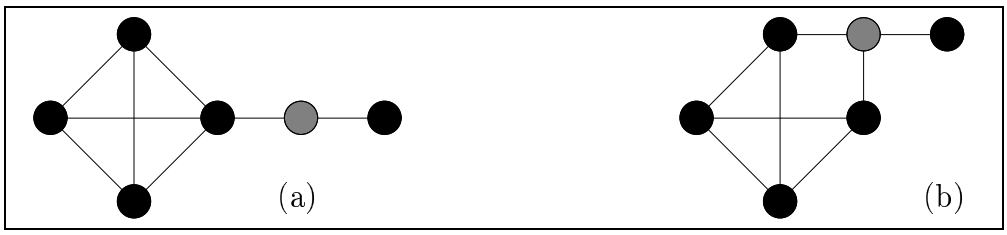

Figure 3:

another type of bad behavior of a function such as $v()$. Consider a *star* with $n + 1$

nodes (and thus, n edges). The index $d/c + N/M$ gives $v_s(n) = 3 + 1/n$. If we look at a *ring* with n nodes (and thus, n edges as well) we obtain $v_r(n) = 1 + \lfloor n/2 \rfloor$. According to this index, for n small, the ring is better (for instance, $v_s(3) = 10/3$ and $v_r(3) = 2$) while for $n \geq 6$, the less vulnerable topology of both is the star. This dependence on the parameter n seems not a very desirable property.

When a network becomes disconnected it could be desirable to capture the extent of disruption by measuring the size and number of the remaining connected components. A system which has been split into many small parts may represent a more severe disruption than one which has been split into a few large parts. Several parameters have been studied for combining the sizes of the disconnecting sets with the characteristics of the resulting components [8]. For instance, in [9] (see also [10]), the author proposes as a measure of *invulnerability* of $\mathcal{G}$ the number $INV(\mathcal{G})$ defined by

$$INV(\mathcal{G}) = \min_{\Gamma \text{ cut of } \mathcal{G}} \frac{|\Gamma|}{\#CC(\mathcal{G} - \Gamma) - 1}$$

where $\mathcal{G} - \Gamma$ is the graph obtained from $\mathcal{G}$ by deleting all the edges of Γ and, $\#CC()$ denotes the number of connected components. Observe that $\#CC(\mathcal{G} - \Gamma) \leq |\Gamma| + 1$, which implies that $INV(\mathcal{G}) \geq 1$. This metric is also rather local. In the examples of Figure 2, we obtain the value 1 in both graphs. We can observe that if we consider the source-terminal vulnerability, the interest is not in the number of created connected components but in the fact that s and t are connected or not. So, the analogous measure for the source-terminal vulnerability is simply the edge connectivity c.

Last, let us also mention, for completeness, a different approach followed in [11]. The authors propose to define the *degree of influence of edge e on the vulnerability* of a network by

$$\sum_{\substack{s,t \in V \\ s \neq t}} g(s,t;e)$$

where $g(s,t;e)$ is the maximum of the values that the different max flows take on edge e. If $f(s,t)$ is the value of a maximal flow between s and t, a normalized version of this metric is

$$\sum_{\substack{s,t \in V, \\ s \neq t}} \frac{g(s,t;e)}{f(s,t)}.$$

Observe that this index is not defined for the graph but for its edges. Later in the paper, we will see that our metric can also handle weighted graphs, and this

suggests, as a possible research direction, the possible use of the approach of [11] in such a context.

None of the metrics discussed before satisfies the properties (i) to (iii) presented in Section 2. Moreover, they are relevant only when we consider all-terminal vulnerability, with one exception: the edge-connectivity c. In the next section, we propose a measure which satisfies all these properties and which can be used to quantify either source-to-terminal vulnerability or all-terminal vulnerability. We also give analytical expressions to evaluate $V_{\mathrm{s,t}}$ and V_{all} in case of series and parallel configurations. Moreover, the new measure satisfies also a *coherence* property which is discussed in Section 5. Last, this measure allows to work with natural extensions obtained by adding supplementary data to the model (costs, capacities, ...) without losing the previous listed properties. We discuss this in Section 6.

4 A new measure of vulnerability

One of the conclusions of the previous section is that the pair (c, n_c) has some nice characteristics. Its main default is the locality, as discussed before. Our proposal consists of taking into account not only the mincuts of minimal size c and their number n_c, but all the mincuts in the graph. Let us denote by n_i the number of mincuts having i edges. Formally, we propose to use the vector $(n_0, n_1, \dots)$ as the measure of vulnerability; we set $n_0 = 0$ when the graph is connected, 1 otherwise. The rest of the paper consists of the analysis of this metric. For simplicity, it is convenient to see this vector as having an infinite number of components. Of course only the first ones are non zero: if the graph has M edges, we necessarily have $n_i = 0$ for all $i > M$.

Definition 4.1 *The vulnerability of graph $\mathcal{G}$ is the infinite vector $V(\mathcal{G}) = (n_0, n_1, \dots)$ where n_i is the number of mincuts of cardinality i. Recall that the mincuts considered here are either s,t-cuts for fixed s and t, or simply cuts, that is, x,y-cuts for at least one pair of nodes x, y. We say that n_i is the value at position i in $V(\mathcal{G})$, $i = 0, 1, \dots$ If $\mathcal{G}$ is connected, $n_0 = 0$. If not, $n_0 = 1$ and for all $i \geq 1$, $n_i = 0$.*

The first point is to choose the ordering on the set of vectors. We want the edge-connectivity c as large as possible, and for a given value c, the number n_c of mincuts of minimal size c as small as possible. This leads to propose the lexicographical order. Consider two graphs $\mathcal{G}_1$ and $\mathcal{G}_2$, and let us denote the respective vulnerabilities by $V(\mathcal{G}_1) = (n_0, n_1, n_2, \dots)$ and $V(\mathcal{G}_2) = (m_0, m_1, m_2, \dots)$. The relation $V(\mathcal{G}_1) < V(\mathcal{G}_2)$ means that we have $n_i = m_i$ for $i = 0, 1, \dots, k-1$ ($k \geq \min(c_1, c_2)$ if c_i is

the edge-connectivity of $\mathcal{G}_i$) and $n_k < m_k$. The relation $V(\mathcal{G}_1) \leq V(\mathcal{G}_2)$ means that either $V(\mathcal{G}_1) = V(\mathcal{G}_2)$ or $V(\mathcal{G}_1) < V(\mathcal{G}_2)$, etc. Resuming,

Definition 4.2 *Let $V(\mathcal{G}_1) = (n_0, n_1, n_2, \dots)$ and $V(\mathcal{G}_2) = (m_0, m_1, m_2, \dots)$ be the vulnerabilities of two graphs $\mathcal{G}_1$ and $\mathcal{G}_2$. We have $V(\mathcal{G}_1) < V(\mathcal{G}_2)$ if there exists $k \geq 0$ such that $n_k < m_k$ and for all $i < k$ (if any), $n_i = m_i$. We write $V(\mathcal{G}_1) \leq V(\mathcal{G}_2)$ if either $V(\mathcal{G}_1) < V(\mathcal{G}_2)$ or $V(\mathcal{G}_1) = V(\mathcal{G}_2)$, etc.*

So, this measure verifies property (i). Let us now look at the other basic properties. We need here a supplementary definition, taken from the network reliability area.

Definition 4.3 *An edge $e \in \mathcal{G}$ is s,t-relevant if and only if there exists at least one s,t-mincut Γ with $e \in \Gamma$, that is, if and only if e belongs to some minimal s,t-path. If not, e is s,t-irrelevant.*

This is immediately related to our problem by means of the following result.

Theorem 4.4 *An edge $e \in \mathcal{G}$ is s,t-irrelevant if and only if $V_{s,t}(\mathcal{G} - e) = V_{s,t}(\mathcal{G})$.*

Proof.

In the proof, we need to discuss about cuts in $\mathcal{G}$ and in $\mathcal{G} - e$, two graphs having the same node set. To ease the reading of the proof, we explicitly denote by $(X, \overline{X})_{\mathcal{G}}$ the cut defined by $(X, \overline{X})$ in $\mathcal{G}$, and by $(X, \overline{X})_{\mathcal{G}-e}$ the cut defined by the same pair of subset of nodes in $\mathcal{G} - e$. We also denote by $\mathcal{E}_{\mathcal{V}',\mathcal{G}}$ the set of edges of $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ having their extremities in $\mathcal{V}' \subseteq \mathcal{V}$. Thus, $(X, \mathcal{E}_{X,\mathcal{G}})$ is the graph induced by $X \subseteq \mathcal{V}$ in $\mathcal{G}$.

(i) Assume first that $e = \{u, v\}$ is an s,t-irrelevant edge in $\mathcal{G}$. We will prove that the set of s,t-mincuts of $\mathcal{G}$ and of $\mathcal{G} - e$ are identical.

Consider an s,t-mincut $(X, \overline{X})_{\mathcal{G}-e}$ of $\mathcal{G} - e$. Then either $u, v \in X$ or $u, v \in \overline{X}$. To see this, recall first that graphs $(X, \mathcal{E}_{X,\mathcal{G}-e})$ and $(\overline{X}, \mathcal{E}_{\overline{X},\mathcal{G}-e})$ are connected. Now, if $u \in X$ and $v \in \overline{X}$ (or if $u \in \overline{X}$ and $v \in X$), the set of edges $(X, \overline{X})_{\mathcal{G}-e} + e$, which is an s,t-cut in $\mathcal{G}$, is in fact an s,t-mincut in $\mathcal{G}$ since $\mathcal{E}_{X,\mathcal{G}-e} = \mathcal{E}_{X,\mathcal{G}}$ and $\mathcal{E}_{\overline{X},\mathcal{G}-e} = \mathcal{E}_{\overline{X},\mathcal{G}}$. But this is in contradiction with the fact that e is s,t-irrelevant in $\mathcal{G}$ because $e \in (X, \overline{X})_{\mathcal{G}}$. Now, since $u, v \in X$ or $u, v \in \overline{X}$, $(X, \overline{X})_{\mathcal{G}-e} = (X, \overline{X})_{\mathcal{G}}$ and $(X, \overline{X})_{\mathcal{G}}$ is also an s,t-mincut in $\mathcal{G}$.

Conversely, consider an s,t-mincut $\Gamma = (X, \overline{X})_{\mathcal{G}}$. Since $e = \{u, v\}$ is s,t-irrelevant in $\mathcal{G}$, $e \notin \Gamma$; so, $u, v \in X$ or $u, v \in \overline{X}$, and Γ is also an s,t-cut in $\mathcal{G} - e$.

We have to prove that Γ is an s,t-mincut in $\mathcal{G}-e$. If this is not the case, it contains some s,t-mincut Γ' in $\mathcal{G}-e$, which is an s,t-mincut in $\mathcal{G}$ as well, as we have shown below. But this implies that, since $\Gamma' \subset \Gamma$ also in $\mathcal{G}$, Γ is not minimal in $\mathcal{G}$, which is in contradiction with our starting point.

In conclusion, when e is an s,t-irrelevant edge in $\mathcal{G}$, then all the s,t-mincuts of $\mathcal{G}$ are s,t-mincuts of $\mathcal{G}-e$ and reciprocally. This proves that $V_{\mathrm{s,t}}(\mathcal{G}-e) = V_{\mathrm{s,t}}(\mathcal{G})$.

(ii) Assume now that $V_{\mathrm{s,t}}(\mathcal{G}-e) = V_{\mathrm{s,t}}(\mathcal{G})$. Let us denote, for fixed s,t,u,v,

$$MC_{\mathcal{G}} = \{\Gamma \mid \Gamma \text{ is an } s,t\text{-mincut in } \mathcal{G} \text{ separating } u \text{ and } v\},$$

$$\overline{MC}_{\mathcal{G}} = \{\Gamma \mid \Gamma \text{ is an } s,t\text{-mincut in } \mathcal{G} \text{ not separating } u \text{ and } v\}.$$

Let us assume that e is s,t-relevant and show that the vulnerabilities of $\mathcal{G}$ and $\mathcal{G}-e$ are different, which is in contradiction with the starting assumption.

Observe that there is a one-to-one correspondence between $MC_{\mathcal{G}}$ and $MC_{\mathcal{G}-e}$. Indeed,

$$\Gamma \in MC_{\mathcal{G}-e} \Longleftrightarrow \Gamma + e \in MC_{\mathcal{G}}. \tag{1}$$

Since there is at least one s,t-mincut in $\mathcal{G}$ containing e, we can define k as the min of the sizes of the s,t-mincuts in $\mathcal{G}$ containing e, which can be written

$$k = \min_{\Gamma \in MC_{\mathcal{G}}} |\Gamma|,\ k \geq 1.$$

If $k=1$, then e is a bridge in $\mathcal{G}$ and, in that case, $\mathcal{G}-e$ is s,t-disconnected, leading by definition to $V_{\mathrm{s,t}}(\mathcal{G}-e) = (1,0,0,\dots) \neq V_{\mathrm{s,t}}(\mathcal{G}) = (0,0,\dots)$.

Consider now the case of $k \geq 2$. Let us denote $V_{\mathrm{s,t}}(\mathcal{G}) = (n_0, n_1, \dots)$ and $V_{\mathrm{s,t}}(\mathcal{G}-e) = (m_0, m_1, \dots)$. We will show that for all $i < k-1$, $n_i = m_i$, and that $n_{k-1} \neq m_{k-1}$. Observe that, by definition of k, if $i<k$, every s,t-mincut Γ of size i in $\mathcal{G}$ necessarily belongs to $\overline{MC}_{\mathcal{G}}$. We will then show that, for all $i<k$,

$$\{\Gamma \in \overline{MC}_{\mathcal{G}} \text{ such that } |\Gamma| = i\} \equiv \{\Gamma \in \overline{MC}_{\mathcal{G}-e} \text{ such that } |\Gamma| = i\}.$$

If $\Gamma \in \overline{MC}_{\mathcal{G}-e}$, with $|\Gamma| = i$, then trivially $\Gamma \in \overline{MC}_{\mathcal{G}}$, with $|\Gamma| = i$.

Assume now that $\Gamma \in \overline{MC}_{\mathcal{G}}$ and $|\Gamma| = i < k$. We know that Γ is an s,t-cut in $\mathcal{G}-e$, separating u and v.

To prove that necessarily $\Gamma \in \overline{MC}_{\mathcal{G}-e}$, assume that the contrary holds. That means that Γ is not minimal in $\mathcal{G}-e$. Then, it contains some s,t-mincut Γ', with $|\Gamma'| < i$, which separates u and v (otherwise, we would obtain that $\Gamma' \subset \Gamma$ is an s,t-mincut in $\mathcal{G}$ and Γ is not minimal in $\mathcal{G}$). So, we have $\Gamma' \in MC_{\mathcal{G}-e}$. But then,

from (1), $\Gamma'+e \in MC_{\mathcal{G}}$ with $|\Gamma'+e| \leq i < k$, in contradiction with the definition of k. So, necessarily $\Gamma \in \overline{MC}_{\mathcal{G}-e}$, which leads to the following one-to-one correspondence:

$$\forall i < k, \quad \Gamma \in \{\Gamma' \in \overline{MC}_{\mathcal{G}} \text{ such that } |\Gamma'| = i\} \Longleftrightarrow \Gamma \in \{\Gamma' \in \overline{MC}_{\mathcal{G}-e} \text{ such that } |\Gamma'| = i\}. \tag{2}$$

From (1), we have that, for all $i < k-1$,

$$|\{\Gamma' \in MC_{\mathcal{G}-e} \text{ such that } |\Gamma'| = i\}| = |\{\Gamma' \in MC_{\mathcal{G}} \text{ such that } |\Gamma'| = i+1\}| = 0. \tag{3}$$

From (2) and (3), we have that, for all $i < k-1$,

$$m_i = |\{\Gamma' \in \overline{MC}_{\mathcal{G}-e} \text{ such that } |\Gamma'| = i\}| = |\{\Gamma' \in \overline{MC}_{\mathcal{G}} \text{ such that } |\Gamma'| = i\}| = n_i,$$

and

$$m_{k-1} - n_{k-1} = |\{\Gamma' \in MC_{\mathcal{G}-e} \text{ such that } |\Gamma'| = k-1\}|.$$

Since there is at least one s,t-mincut of size $k-1$ in $MC_{\mathcal{G}-e}$, we have $m_{k-1}-n_{k-1} > 0$. Then, we obtain, for all $i < k-1$, $n_i = m_i$, and $n_{k-1} < m_{k-1}$. ——— ■

We are now ready to state the first basic property of our measure.

Property 4.5 *The measure is* ***monotone****: if we add an edge to the graph without changing the set of nodes, the vulnerability does not increase. More specifically,*

- *if $\mathcal{G}$ is not $(s,t-)$connected, then if $\mathcal{G}+e$ is not $(s,t-)$connected neither, $V(\mathcal{G}+e) = V(\mathcal{G}) = (1,0,0,\dots)$, while if $\mathcal{G}+e$ is $(s,t-)$connected, $V(\mathcal{G}+e) = (0,\dots) < V(\mathcal{G}) = (1,0,0,\dots)$.*
- *If $\mathcal{G}$ is $(s,t-)$connected, then $V_{all}(\mathcal{G}+e) < V_{all}(\mathcal{G})$. In the source-to-terminal case, if e is s,t-relevant in $\mathcal{G}+e$, then $V_{s,t}(\mathcal{G}+e) < V_{s,t}(\mathcal{G})$ (and $V_{s,t}(\mathcal{G}+e) = V_{s,t}(\mathcal{G})$ otherwise).*

  Moreover, when all edges in $\mathcal{G}$ are s,t-relevant and if there are no isolated nodes, then for all $e = \{u,v\}$ with $u \neq v$, e is s,t-relevant in $\mathcal{G}+e$ (and thus $V_{s,t}(\mathcal{G}+e) < V_{s,t}(\mathcal{G})$).

Proof.

(i) The first part of this proposition comes directly from the definition of the vulnerability when the considered network $\mathcal{G}$ is not $(s,t-)$connected.

(ii) Case of source-to-terminal vulnerability of a connected network. Assume that e is s,t-relevant in $\mathcal{G}+e$. Then, we have seen in the last part of the proof of Theorem 4.4 that $V_{\mathrm{s,t}}(\mathcal{G}+e) < V_{\mathrm{s,t}}(\mathcal{G})$ (more specifically, the first difference between the components of the respective vulnerability vectors happens at position $k = \min_{\Gamma \in MC_{\mathcal{G}}} |\Gamma|$.

(iii) Case of all-terminal vulnerability of a connected network. As in the case of an s,t-relevant edge $e = \{u,v\}$, we can observe that there is a one-to-one correspondence between the mincuts in $\mathcal{G}$ separating u and v and the mincuts in $\mathcal{G}-e$ separating u and v. Moreover, every mincut that does not contain e in $\mathcal{G}-e$ is a mincut in $\mathcal{G}$. As in Theorem 4.4, we have that the size of a mincut in $\mathcal{G}$ which is not a mincut in $\mathcal{G}-e$ is greater or equal than k. The only difference lies in the fact that any edge e is relevant, so, the inequality is always strict.

(iv) A result in [12] which says that a necessary and sufficient condition for a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ to have no s,t-irrelevant edge is that the graph $\mathcal{G}' = (\mathcal{V}, \mathcal{E} + \{s,t\})$ obtained from $\mathcal{G}$ by adding an extra edge $\{s,t\}$ has no articulation point. It is then clear that by adding an edge e, we do not create any articulation point in $\mathcal{G}'+e$.

■

An immediate consequence of Property 4.5 is stated in the following corollary.

Corollary 4.6 *Let us consider the family of connected graphs sharing the same fixed set of nodes $\mathcal{V}$ (we do not allow here multiple edges). If $|\mathcal{V}| = n$, with respect to $V_{s,t}$ the most vulnerable is a series and the less vulnerable is the complete graph. In case of V_{all}, the most vulnerable graph is a tree and the less vulnerable is again the complete graph.*

The vulnerabilities of the "extremal" graphs with n nodes

Let us give explicitly here the vulnerabilities of the "extreme" graphs considered in the previous lemma. Denote by $\mathcal{G}_s$ a series with n nodes (then $n-1$ edges), where s and t are the "extremities" of the series, and by $\mathcal{G}_c$ the complete graph with n nodes (then $n(n-1)/2$ edges). A careful analysis of the two topologies leads immediately to the following expressions:

- $V_{\mathrm{s,t}}(\mathcal{G}_s) = (0, n-1, 0, 0, \dots)$
- $V_{\mathrm{s,t}}(\mathcal{G}_c) = (0, 0, \dots, 0, \alpha C_{n-2}^{\alpha-1}, 0, \dots, 0, i C_{n-2}^{i-1}, 0, \dots, 0, \frac{n+1}{2}, 0, \dots)$
- $V_{\mathrm{all}}(\mathcal{G}_s) = (0, n-1, 0, 0, \dots)$

- $V_{\text{all}}(\mathcal{G}_c) = (0, 0, \ldots, \overset{n}{\hat{n}}, 1, 0, \ldots, 0, \overset{i(n\nparallel i)}{C_n^i}, 0, \ldots, 0, \overset{\alpha(n\nparallel\alpha)}{C_n^\alpha}, 0, \ldots)$
  with $\alpha = \lfloor n/2 \rfloor$ and $q = 1 + (n \bmod 2)$.

Series-parallel configurations

Now, let us turn to series-parallel configurations.

Property 4.7 *Assume $\mathcal{G}$ is composed as shown in Figure 4. Then, we have $V_{s,t}(\mathcal{G}) = V_{s,t}(\mathcal{G}_1) + V_{s,t}(\mathcal{G}_2)$ and $V_{all}(\mathcal{G}) = V_{all}(\mathcal{G}_1) + V_{all}(\mathcal{G}_2)$.*

Proof. Every s,t-mincut in $\mathcal{G}$ is either an s,u-mincut in $\mathcal{G}_1$ or an u,t-mincut in $\mathcal{G}_2$, and reciprocally. Then, if n_i is the number of s,t-mincuts in $\mathcal{G}$ with size i, and if n_i^1 (resp. n_i^2) is the corresponding number of s,u-mincuts in $\mathcal{G}_1$ (resp. in of u,t-mincuts in $\mathcal{G}_2$), we have $n_i = n_i^1 + n_i^2$ which ends the proof for $V_{\text{s,t}}$. The case of V_{all} is similar. ■

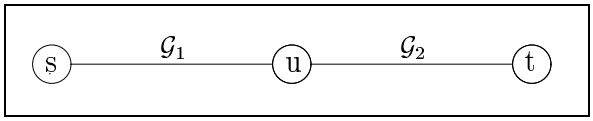

Figure 4: A series configuration

Observe that u in Figure 4 is an articulation point of $\mathcal{G}$. From the previous result about the vulnerability of a series, we deduce that the proposed measure verify property (iii).

Let us denote by $\bigotimes$ the convolution operator between two vectors: if $u = (u_0, u_1, \ldots)$ and $v = (v_0, v_1, \ldots)$, then $w = u \bigotimes v = (w_0, w_1, \ldots)$ with

$$w_n = \sum_{j+k=n} u_j v_j.$$

Property 4.8 *Assume $\mathcal{G}$ is composed as shown in Figure 5. Then, we have $V_{s,t}(\mathcal{G}) = V_{s,t}(\mathcal{G}_1) \bigotimes V_{s,t}(\mathcal{G}_2)$. In the all-terminal case, we have $V_{all}(\mathcal{G}) = V_{all}(\mathcal{G}_1 \bullet st) + V_{all}(\mathcal{G}_2 \bullet st) + (V_{s,t}(\mathcal{G}_1) \bigotimes V_{s,t}(\mathcal{G}_2))$ where "$\mathcal{G}_i \bullet st$" denotes the graph obtained by contracting the nodes s and t in one single node in $\mathcal{G}_i$. No edges are destroyed.*

Proof. Case source-to-terminal first. Every s,t-mincut in $\mathcal{G}$ is the union of an s,t-mincut in $\mathcal{G}_1$ and an s,t-mincut in $\mathcal{G}_2$, and reciprocally. Then, with the same notation as in the series case, we have

$$n_i = \sum_{j+k=i} n_j^1 n_k^2.$$

Case of the all-terminal measure. Every mincut in $\mathcal{G}$ either separates s and t or not. In the first case, this cut is the union of an s,t-mincut in $\mathcal{G}_1$ and an s,t-mincut in $\mathcal{G}_2$. In the second one, it is a mincut that contains only edges of $\mathcal{G}_1$ or edges of $\mathcal{G}_2$, because every path from a node of $\mathcal{G}_1$ to a node of $\mathcal{G}_2$ contains s or t. Then, it is a mincut in $\mathcal{G}_1 \bullet st$ or in $\mathcal{G}_2 \bullet st$. Reciprocally, the union of two s,t-mincuts, one in $\mathcal{G}_1$ and the other in $\mathcal{G}_2$, is a mincut in $\mathcal{G}$ and a mincut in $\mathcal{G}_1 \bullet st$ or in $\mathcal{G}_2 \bullet st$ is also a mincut in $\mathcal{G}$. ■

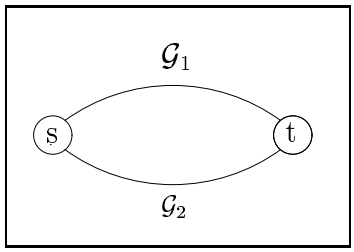

Figure 5: A parallel configuration

These properties allow to simplify the models (in a similar way as it is usually done in network reliability theory). Moreover, with the property of coherence that we will show in the next section, these properties make us possible to use series-parallel reductions in order to evaluate the network vulnerability. We will give a small example at the end of Section 5.

5 The property of coherence

In this section, we extend the framework to be able to set and prove the announced coherence property. To do this, we need to switch to *valued* graphs. We will proceed in two steps.

In the first step, we start from the following observation: if we consider a graph $\mathcal{G}$ with only two nodes s and t, and a single edge between them, then we have

$V_{\mathrm{s,t}}(\mathcal{G}) = V_{\mathrm{all}}(\mathcal{G}) = (0, 1, 0, \dots)$. From this, for any graph $\mathcal{G}$ we define the value $w(e)$ of an edge e by $w(e) = (0, 1, 0, \dots)$. Then, we also define the value of the cuts Γ of $\mathcal{G}$ by the vector $w(\Gamma) = (n_0, n_1, \dots)$ where $n_i = 0$ for all $i \neq |\Gamma|$ and $n_{|\Gamma|} = 1$. It follows that

$$V(\mathcal{G}) = \sum_{\text{all mincut } \Gamma} w(\Gamma).$$

We can now prove the following result.

Theorem 5.1 *For any mincut* Γ,

$$w(\Gamma) = \bigotimes_{e \in \Gamma} w(e).$$

Proof. Let $v = (0, 1, 0, \dots)$. It is immediately checked by recurrence on n, that the vector sequence

$$v_n = \bigotimes_{i=1}^{n} v$$

verifies $v_n = (0, 0, \dots, 0, 1, 0, \dots)$ where the only 1 is at the nth position. Since for all edge e we have $w(e) = v$, this proves the result. ■

We arrive now at the second step, which generalizes the previous setting. We will define the vulnerability measure of valued graphs $(\mathcal{G}, \mathrm{val})$ where val is an infinite vector of non-negative integers. First, we define the value of any cut by

$$\mathrm{val}(\Gamma) = \bigotimes_{e \in \Gamma} \mathrm{val}(e)$$

and then, the vulnerability vector by

$$V(\mathcal{G}, \mathrm{val}) = \sum_{\text{all mincut } \Gamma} \mathrm{val}(\Gamma).$$

Observe that by considering general mincuts or s, t-mincuts in the previous sum, we obtain the all-terminal measure, or the source-to-terminal one.

All what have been said before in this section can be summarized in the following result.

Theorem 5.2 *Given a graph* $\mathcal{G}$ *valued by the* w*'s (that is,* $w(e) = (0, 1, 0, \dots)$*), we have*

$$V(\mathcal{G}) = V(\mathcal{G}, w).$$

Remark 5.3 *From this theorem, the vulnerability of a graph $\mathcal{G}$ valued by the w's (that is, $w(e) = (0, 1, 0, \dots)$) verifies all the previous properties.*

We are now ready to state the so-called *coherence* property.

Property 5.4 *Let us consider a valued graph $\mathcal{G}$ where we denote $\mathcal{G} = (\mathcal{V}_\mathcal{G}, \mathcal{E}_\mathcal{G}, val)$, and let u be an articulation point in $\mathcal{G}$. If s and t belong to the same connected component $\mathcal{H} = (\mathcal{V}_\mathcal{H}, \mathcal{E}_\mathcal{H}, val)$ (the other one will be denoted $\mathcal{K} = (\mathcal{V}_\mathcal{K}, \mathcal{E}_\mathcal{K}, val)$), then we have*

$$V_{s,t}(\mathcal{G}, val) = V_{s,t}(\mathcal{H}, val).$$

Otherwise, we have

$$V_{s,t}(\mathcal{G}, val) = V_{s,u}(\mathcal{H}, val) + V_{u,t}(\mathcal{K}, val).$$

For the all terminal vulnerability, this property is equivalent to the series property and we have

$$V_{all}(\mathcal{G}, val) = V_{all}(\mathcal{H}, val) + V_{all}(\mathcal{K}, val).$$

Proof. If s and t belong to the same connected component, then all the edges in $\mathcal{E}_\mathcal{K}$ are s,t-irrelevant. Then, by deleting all edges in $\mathcal{E}_\mathcal{K}$, we obtain $V_{\mathrm{s,t}}(\mathcal{G}, \mathrm{val}) = V_{\mathrm{s,t}}(\mathcal{H}, \mathrm{val})$. In the other case, this is the result on the series graph, as in the case of all-terminal vulnerability. ■

Property 5.5 *Let us consider a valued graph $\mathcal{G}$ denoted $\mathcal{G} = (\mathcal{V}_\mathcal{G}, \mathcal{E}_\mathcal{G}, val)$. Let $\{u, v\}$ be a separating pair such that s and t belong to the same biconnected component with respect to $\{u, v\}$, which is denoted $\mathcal{H} = (\mathcal{V}_\mathcal{H}, \mathcal{E}_\mathcal{H}, val)$. We denote by $\mathcal{K} = (\mathcal{V}_\mathcal{K}, \mathcal{E}_\mathcal{K}, val)$ the complement of $\mathcal{H}$ in $\mathcal{G}$. We have $\mathcal{V}_\mathcal{H} \cup \mathcal{V}_\mathcal{K} = \mathcal{V}$, $\mathcal{V}_\mathcal{H} \cap \mathcal{V}_\mathcal{K} = \{u, v\}$, $\mathcal{E}_\mathcal{H} \cup \mathcal{E}_\mathcal{K} = \mathcal{E}$ and $\mathcal{E}_\mathcal{H} \cap \mathcal{E}_\mathcal{K} = \emptyset$. Define the reduced graph $\mathcal{G}^r = (\mathcal{V}_{\mathcal{G}^r}, \mathcal{E}_{\mathcal{G}^r}, val_{\mathcal{G}^r})$ by replacing $\mathcal{H}$ in $\mathcal{G}$ by a single edge between u and v, with value $val_{\mathcal{G}^r}(\{u, v\}) = V_{u,v}(\mathcal{H}, val)$ (we have $\mathcal{V}_{\mathcal{G}^r} = \mathcal{V}_\mathcal{K}$ and $\mathcal{E}_{\mathcal{G}^r} = \mathcal{E}_\mathcal{K} \cup \{u, v\}$). Figure 6 illustrates the transformation. We then have*

$$V_{s,t}(\mathcal{G}, val) = V_{s,t}(\mathcal{G}^r, val_{\mathcal{G}^r}).$$

For the all terminal vulnerability, this property is equivalent to Property 4.8 and we have

$$V_{all}(\mathcal{G}, val) = V_{all}(\mathcal{H} \bullet uv, val) + V_{all}(\mathcal{G}^r, val_{\mathcal{G}^r}).$$

with $val_{\mathcal{G}^r}(\{u, v\}) = V_{u,v}(\mathcal{H}, val)$

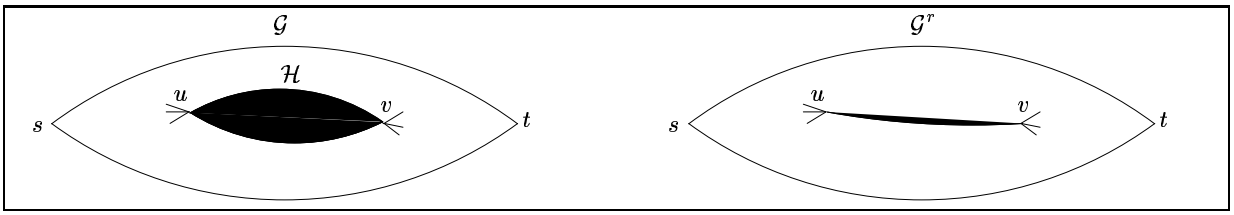

Figure 6: G and its reduced graph $\mathcal{G}^r$

Proof.

Let Γ be an s,t-mincut in $\mathcal{G}$ which does not separate nodes u and v (so, all nodes in $\mathcal{V}_\mathcal{H}$ are in the same connected component). This means that Γ is an s,t-mincut in $\mathcal{G}^r$, with the same value and not containing the edge $\{u,v\}$. Reciprocally, if Γ is an s,t-mincut in $\mathcal{G}^r$ not containing $\{u,v\}$, then it is an s,t-mincut in $\mathcal{G}$, not containing any edge of $\mathcal{H}$, and with the same value.

Let us denote by $\mathcal{C}$ the set of all s,t-mincuts of $\mathcal{G}$ separating u and v, by $\mathcal{C}_r$ the set of all s,t-mincuts of $\mathcal{G}^r$ containing $\{u,v\}$, by $\mathcal{C}_\mathcal{H}$ the set of all u,v-mincuts of $\mathcal{H}$ and by $\mathcal{C}_\mathcal{K}$ the set of all s,t-mincuts of $\mathcal{K}$ separating nodes u and v. If $\Gamma_K \in \mathcal{C}_\mathcal{K}$ then $\Gamma_K \cup \{u,v\} \in \mathcal{C}_r$. Reciprocally, let us choose $\Gamma_r \in \mathcal{C}_r$. Then, for any $\Gamma_\mathcal{H} \in \mathcal{C}_\mathcal{H}$ we have that $(\Gamma_r - \{u,v\}) \cup \Gamma_\mathcal{H} \in \mathcal{C}$.

To prove the theorem, we only need to prove that

$$\sum_{\Gamma \in \mathcal{C}} \mathrm{val}(\Gamma) = \sum_{\Gamma_r \in \mathcal{C}_r} \mathrm{val}_{\mathcal{G}^r}(\Gamma_r).$$

Observe that if $\Gamma \in \mathcal{C}$, then $\Gamma \cap \mathcal{E}_{\mathcal{H}} = \Gamma_{\mathcal{H}} \in \mathcal{C}_{\mathcal{H}}$ and $\Gamma \cap \mathcal{E}_{\mathcal{K}} = \Gamma_{\mathcal{K}} \in \mathcal{C}_{\mathcal{K}}$. Then,

$$\begin{aligned}
\sum_{\Gamma \in \mathcal{C}} \mathrm{val}(\Gamma) &= \sum_{\Gamma \in \mathcal{C}} \Big(\mathrm{val}(\Gamma_{\mathcal{K}}) \bigotimes \mathrm{val}(\Gamma_{\mathcal{H}}) \Big) \text{ where } \Gamma = \Gamma_{\mathcal{H}} + \Gamma_{\mathcal{K}}, \\
&= \left(\sum_{\Gamma_{\mathcal{K}} \in \mathcal{C}_{\mathcal{K}}} \mathrm{val}(\Gamma_{\mathcal{K}}) \right) \bigotimes \left(\sum_{\Gamma_{\mathcal{H}} \in \mathcal{C}_{\mathcal{H}}} \mathrm{val}(\Gamma_{\mathcal{H}}) \right) \\
&= \left(\sum_{\Gamma_{\mathcal{K}} \in \mathcal{C}_{\mathcal{K}}} \mathrm{val}_{\mathcal{G}^r}(\Gamma_{\mathcal{K}}) \right) \bigotimes V_{u,v}(\mathcal{H}) \\
&= \left(\sum_{\Gamma_{\mathcal{K}} \in \mathcal{C}_{\mathcal{K}}} \mathrm{val}_{\mathcal{G}^r}(\Gamma_{\mathcal{K}}) \right) \bigotimes \mathrm{val}_{\mathcal{G}^r}(\{u, v\}) \\
&= \sum_{\Gamma_r \in \mathcal{C}_r} \mathrm{val}_{\mathcal{G}^r}(\Gamma_r)
\end{aligned}$$

which ends the proof. ■

These theorems have a main consequence. They show that the definition is coherent and supports hierarchical composition of networks. From the opposite point of view, they make possible to use the decomposition into triconnected components, leading to the evaluation of the vulnerability of smaller networks.

Remark 5.6 *Observe also that this property (together with Theorem 5.2) implies that the properties shown in Section 4 remain valid in the more general setting of weighted graphs.*

Let us illustrate these properties on the small example shown in Figure 7, which has several triconnected components. On this example, we want to evaluate the vulnerability between the two white points. To do this, we show in the center of Figure 8 the reduced graph, where the three edges denoted by V_1, V_2 and V_3, are associated with the three triconnected components also shown in the same Figure. Then, by performing two series reductions, we obtain the network shown in Figure 9. After five last simplifications (parallel, series, parallel, series, parallel), we arrive at a single edge between the two marked nodes, weighted by the vulnerability of the original graph. The obtained vulnerability vector is

$$(0, 0, 0, 2, 4, 4, 6, 12, 12, 8, 4, 0, \dots).$$

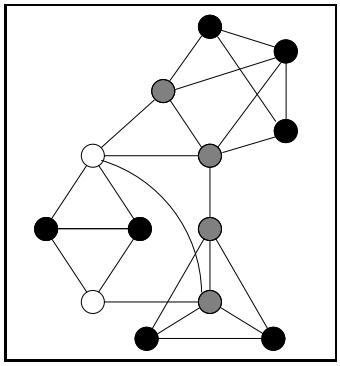

Figure 7: A biconnected graph with separation pairs, taken from [13]

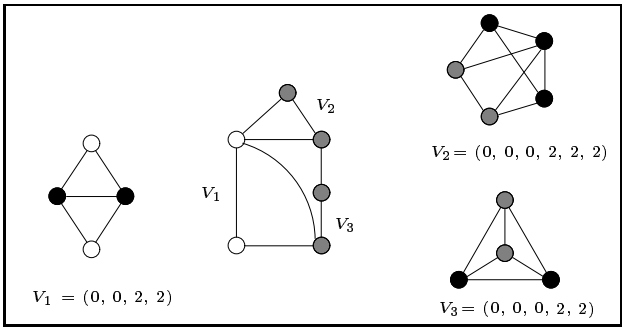

Figure 8: The vulnerability of three of the triconnected components of the graph of Figure 7 and the reduced associated graph

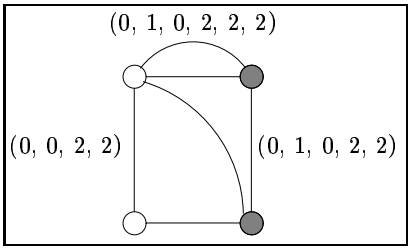

Figure 9: The graph obtained after two series reductions

6 Considering capacities or costs

In Section 4 we studied the vulnerability of a network with no data on edges. However, it is often important in some applications to be able to take into account not only the structure of the network, but also supplementary information, such as capacities, costs, etc. We show here that the preceding results can immediately been extended to this more general context with almost no additional conceptual nor computational cost.

We are given again an undirected valued graph $(\mathcal{G}, \mathrm{val})$ where val takes its values in $\mathbb{N}^\infty$.

Resistance to external "clever attacks"

Let us consider the case of a military application, in which the user wants to evaluate the resistance of a network face to possible attacks. For this, each edge has a destruction cost associated with, assumed to be an integer. If j is the destruction cost of edge e, we assign $\mathrm{val}(e) = (0, 0, \dots, 0, 1, 0, \dots)$ where the only 1 is at the $(j+1)$th position. The sum and the convolution are as previously, then the framework on weighted graphs can be applied without any change. We use here the fact that, since the attack is assumed to be "clever", the attacker can identify the weakest parts of our network, trying to minimize the cost of the attack.

Support to flow transportation under capacity constraints

Another example is the case of a transport network where the value of each edge is some measure of its capacity. Now, the value of a cut is the sum of the capacities of its edges. The lower the value of a cut is, that is the lower the maximal flow is, the more vulnerable the network is, since it is easier to diminish the max flow capacity. In other words, we are in the case of a typical flow problem, but once again we ask ourselves what happens with the capacity of the network to transport the flow when some of the edges are no more there. This problem has been considered in many papers, in a stochastic framework, assuming we know the reliability of each component of the system. Here, we provide a tool which is able to compare different architectures under the flow transportation point of view, in a deterministic context.

From Remark 5.6, we have that the measure, applied to this class of weighted graphs, verifies all the properties shown in the previous sections.

7 Algorithmic issues and numerical examples

The generation of all cutsets in undirected graphs has been studied by many papers [12, 14, 15, 16]. The most efficient of these approaches seems to be the technique developed by Provan and Shier in [16]. It requires $O(|\mathcal{E}|)$ work per minimal cut listed. This approach does not require the elimination of irrelevant edges as in [12], for instance. The algorithm is based on a pivotal decomposition on a node v and its pivot set $I(S,v)$. A pivot node relative to the set $S \subset \mathcal{V}$ is any node $v \notin S$ which is a successor of a node in S. The associated pivot set is $I(S,v) = \{u \in \overline{S} \mid \text{every } (u,t)\text{-path in } \langle \overline{S} \rangle \text{ contains } v\}$. The main procedure, defined for two subsets of nodes S and T, is the following:

Procedure $LIST(S,T)$

PIVOT$(S,T,v,I(S,v))$;
if $I(S,v) = \emptyset$ **then** output the cut $(S,\overline{S})$
else
LIST$(S,T \cup \{v\})$
LIST$(S \cup I(S,v),T)$

Then, $LIST(\emptyset,\emptyset)$ correctly lists all the s,t-mincuts, where the only successor of $\emptyset$ is s.
The procedure PIVOT, relative to sets S and T, is based on the biconnected components. It may be implemented as follows:

1. Construct the graph $\tau = (\mathcal{V}_\tau, \mathcal{E}_\tau)$ whose vertex set $\mathcal{V}_\tau$ consists of $\overline{S}$ together with a vertex b_i for each biconnected component B_i of $\langle \overline{S} \rangle$. The edge set $\mathcal{E}_\tau$ contains all pairs (v,b_i) with $v \in B_i$. It is easy to see that τ is a tree.

2. In the tree τ, identify the set M of those vertices v, which are successors of nodes in S, that are maximally distant from t: that is, the nodes v for which the set $\mathcal{V}(v)$ of vertices in $\overline{S}$ separated from t by v contains no other successor of S. (Note that if any pivot element v satisfying $I(S,v) \subseteq \overline{T}$ exists, then one which lies in M must exist.)

3. For each $v \in M$ check whether $\mathcal{V}(v) \subseteq \overline{T}$. If this holds for some v, then return v and $I(S,v) = \mathcal{V}(v)$; otherwise return $I(S,v) = \emptyset$.

The algorithm has been used in order to evaluate the vulnerability of several networks. For instance, it needs less than 10 seconds (of Sparc 4) on the graph with 19 nodes and 34 edges, proposed in [17], represented on Figure 11. In a much

more stressing case, consider the graph shown in Figure 10 having 32 nodes and 61 edges. Our implementation uses around 4 hours (always on a Sparc 4) to evaluate its vulnerability (1,859,660 (s,t)-mincuts).

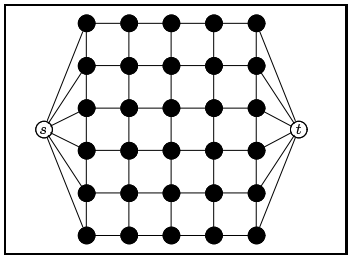

Figure 10: A stressing test-case

Let us point out again the interest in performing series-parallel simplifications. For instance, in the case of the well known example shown in Figure 11, the series-parallel reductions lead to the first graph in Figure 14. The algorithm runs ≈ 35 times faster after performing the series-parallel reductions.

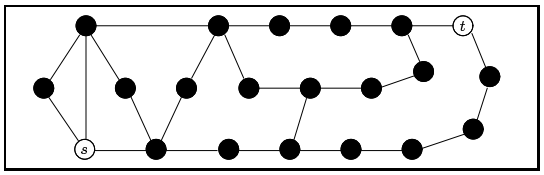

Figure 11: A version of the Arpanet topology

The algorithm runs ≈ 35 times faster after performing the series-parallel reductions.

Comparing again with the reliability context

Consider the following sample of graphs taken from papers published in the network reliability area. Assume that every line in the graphs has the same elementary reliability equal to 0.9.

Table 13 shows the value of the reliability of the 7 previous networks with elementary reliability equal to 0.9 in each edge, and their vulnerability. If we class them according to their reliability or to their vulnerability, we obtain exactly the same order.

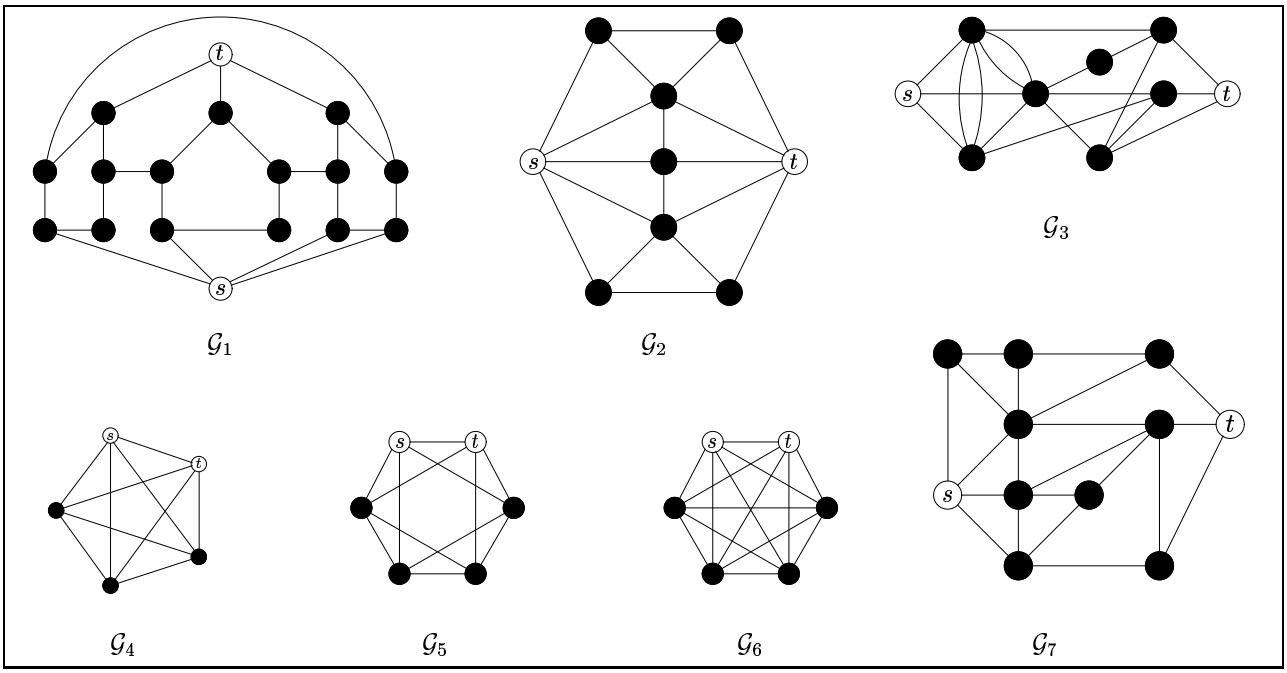

Figure 12: 7 networks from literature with edge reliability 0.9

Graphs	reliability	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9	n_{10}	n_{11}	n_{12}	n_{13}
$\mathcal{G}_1$	0.998062	0	0	1	11	73	235	397	347	145	23	0	0	0
$\mathcal{G}_2$	0.999971	0	0	0	0	2	8	16	20	16	8	2	0	0
$\mathcal{G}_3$	0.997917	0	0	2	0	9	2	3	10	8	16	4	0	0
$\mathcal{G}_4$	0.999795	0	0	0	2	0	6	0	0	0	0	0	0	0
$\mathcal{G}_5$	0.999793	0	0	0	2	0	8	0	4	0	0	0	0	0
$\mathcal{G}_6$	0.999980	0	0	0	0	2	0	0	8	6	0	0	0	0
$\mathcal{G}_7$	0.998663	0	0	1	3	5	12	21	25	26	22	13	5	0

Figure 13: Comparison between reliability and vulnerability of 7 networks

Consider now the two networks $\mathcal{G}_4$ and $\mathcal{G}_5$ shown in Figure 12. Assume that we assign elementary reliabilities of 0.9 to all the edges. Then, the source-to-terminal reliability of the networks are equal to 0.9997948 for the first one, and to 0.9997928 for the second. So, the first one is (slightly) less reliable than the second. If the elementary reliabilities are set to 0.99, then the difference between the system reliabilities is less than 10^{-12}, and, again, the first one is (very slightly) better than the second. Both graphs have edge-connectivity (with respect to the pair s, t) equal to 4, and both have exactly 2 s,t-mincuts of size 4. Our vulnerability measure gives $(0, 0, 0, 0, 2, 0, 6, \dots)$ for the first graph and $(0, 0, 0, 0, 2, 0, 8, \dots)$ for the second, which is consistent with the results obtained in the stochastic framework. Again, we can see that parameters c and n_c are not enough to make a difference, as discussed in Section 3.

In Figure 14 we illustrate the framework in which we consider destruction costs (and the first interpretation). When all the costs are equal, we obtain that the first network is less vulnerable than the second. When the cost of edge e is equal to 2, we obtain that the first network becomes more vulnerable than the second.

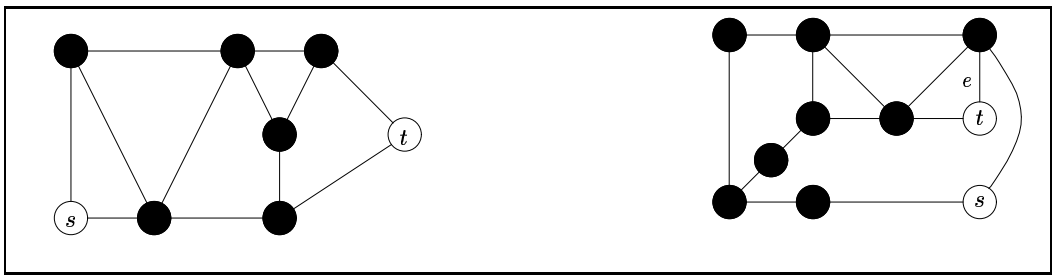

Figure 14: Network in Figure 11 after series-parallel reductions, and a comparable topology

The following table gives the values of the vulnerability vectors.

Graphs	n_0	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8
Reduced ARPANET	0	0	2	5	5	4	3	0	0
Comparable topology with cost(e)=1	0	0	3	4	7	8	8	0	0
Comparable topology with cost(e)=2	0	0	2	5	4	5	8	6	0

8 Conclusions

We have studied the behavior of a communication network using vulnerability metrics in a deterministic framework. We have proposed a new measure, based on minimal cuts. This measure verifies desirable properties, such as the monotonicity property, and several properties of interest for its evaluation. Moreover, our approach has made it possible to take into account certain supplementary data on network components. For example, we have considered the cases where edges are valued by their resistance to an external attack, or by capacities. Our research effort is being done in this direction, to further explore the possibility of using the same approach in richer models. Also, we think that more work is necessary in the algorithmic aspects.

References

[1] I. B. Gertsbakh. *Statistical Reliability Theory.* Marcel Dekker, Inc., New York and Bassel, 1989.

[2] G Rubino. Network reliability evaluation. In K. Bagchi and J. Walrand, editors, *State-of-the art in performance modeling and simulation*, pages 275–302. Gordon and Breach Books, 1996. For a copy, send a mail to `rubino@irisa.fr`.

[3] S. Bulteau and G. Rubino. A new approach to vulnerability evaluation of communication networks. In *Proceedings of the International Teletraffic Congress (ITC) 15*, Washington, D.C., U.S.A., 1997.

[4] A. K. Kel'mans. The graph with the maximum probability of remaining connected depends on the edge-removal probability. *Graph Theory Newsletter*, 9:2–3, 1979.

[5] B. Bollobás. A problem of the theory of communication networks. In G. Katona and P. Erdos, editors, *Theory of Graphs*, pages 29–36. Akad. Kiado, Budapest, 1968.

[6] F.T. Boesch, F. Harary, and J.A. Kabell. Graphs as models of communication network vulnerability: connectivity and persistence. *Networks*, 11:57–63, 1981.

[7] I.M. Soi and K.K. Aggarwal. Reliability indices for topological design of computer communication networks. *IEEE Transactions on Reliability*, 30:438–444, 1981.

[8] C.A. Barefoot, R. Entringer, and H. Swart. Vulnerability in graphs - a comparative survey. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1:12–22, 1987.

[9] D. Gusfield. Connectivity and edge-disjoint spanning trees. *Information Processing Letters*, 16:87–89, 1983.

[10] W.H. Cunningham. Optimal attack and reinforcement of a network. *Journal of ACM*, 32:549–561, 1985.

[11] M. Sengoku, S. Shinoda, and R. Yatsuboshi. On a function for the vulnerability of a directed flow network. *Networks*, 18:73–83, 1988.

[12] S. Tsukiyama, Z. Shirakawa, H. Ozaki, and H. Ariyoshi. An algorithm to enumerate all cutsets of a graph in linear time per cutset. *Journal of ACM*, 27:619–631, 1980.

[13] J. E. Hopcroft and R. E. Tarjan. Dividing a graph into triconnected components. *SIAM Journal of Computing*, 2:135–158, 1973.

[14] U. Abel and R. Bicker. Determination of all minimal cut-sets between a vertex pair in an undirected graph. *IEEE Transactions on Reliability*, 31:167–171, 1982.

[15] M. Bellmore and P.A. Jensen. An implicit enumeration scheme for proper cut generation. *Technometrics*, 12:775–788, 1970.

[16] J.S. Provan and D.R. Shier. A paradigm for listing (s,t)-cuts in graphs. *Algorithmica*, 15:351–372, 1996.

[17] L. Fratta and U. Montanari. A recursive method based on case analysis for computing network terminal reliability. *IEEE Transactions on Communications*, 26:1166–1177, 1978.

Unit´e de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unit´e de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unit´e de recherche INRIA Rhône-Alpes, 655, avenue de l'Europe, 38330 MONTBONNOT ST MARTIN
Unit´e de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unit´e de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
http://www.inria.fr
ISSN 0249-6399