

Network Structural Vulnerability: A Multi-Objective Attacker Perspective

Luca Faramondi^{1,2}, Gabriele Oliva^{1,2,*}, Stefano Panzieri³, Federica Pascucci³, Martin Schlueter⁴,
Masaharu Munetomo⁴, and Roberto Setola^{1,2}

Abstract—In this paper we provide a novel framework to assess the vulnerability/robustness of a network with respect to pairwise nodes' connectivity. In particular, we consider attackers that aim, at the same time, at dealing the maximum possible damage to the network in terms of the residual connectivity after the attack and at keeping the cost of the attack (e.g., the number of attacked nodes) at a minimum. Differently from previous literature, we consider the attacker perspective using a multi-objective formulation and, rather than making hypotheses on the mindset of the attacker in terms of a particular tradeoff between the objectives, we consider the entire Pareto front of non-dominated solutions. Based on that, we define novel global and local robustness/vulnerability indicators and we show that such indices can be the base for the implementation of effective protection strategies. Specifically, we propose two different problem formulations and we assess their performances. We conclude the paper by analyzing, as case studies, the IEEE 118 power network and the US airline network as it was in 1997, comparing the proposed approach against centrality measures.

Index Terms—Critical Infrastructures, Network Robustness, Critical Node Detection, Attacker Behavior

I. INTRODUCTION

Critical Infrastructures (e.g., telecommunication or transportation networks) are exposed to the threat of cascading failures, that may lead to the complete or partial halt of the services provided to the community, with dramatic and often life-threatening consequences [1], [2].

In order to reduce the risk and mitigate the consequences it is mandatory to identify effective formalisms to represent dependencies (e.g., see [3]), to devise effective protection strategies and, in particular, to prioritize the protection of the different sites and components. To this end, it is fundamental to identify adequate metrics and indicators, by evaluating comparatively the criticality and the vulnerability associated to different elements, especially in highly heterogeneous contexts. A typical strategy to obtain such metrics is to simulate the effect of negative events in order to provide insights on the most critical elements, for which protection has to be raised. In particular, a well established approach is to focus

on intentional attacks, considering a rational attacker that aims at maximizing the damage. Among other approaches, it is worth mentioning methods to estimate the resilience of infrastructure networks, based on (constrained) optimization problems [4]–[12], bi-level optimization frameworks [13], [14] and network spectral analysis [15], [16].

Since the pioneering works about complex networks in the first 2000s (e.g., [17], [18]), it has become clear that attacks that take into account the topological structure of a network may have dramatic consequences. In fact, knowing the topology of the network, an attacker is able to select more effectively the target sites, increasing the damage dealt while keeping the number of attacks at a minimum (see [19]–[23] for recent works on the topic). In particular, the *Critical Node Disruptor* (CND) problem [4]–[6] showed its effectiveness. Within the CND problem, an attacker targets some of the nodes in the network (removing them and all their incident links) with the aim to minimize the *pairwise connectivity* (PWC) [24], that is, the number of pairs of nodes that are connected via a path after the attacked nodes have been removed. Specifically, the CND problem assumes that up to k nodes can be attacked. Such an approach, however, requires a large number of Boolean decision variables [6] and a number of constraints that can be non-polynomial in the number of nodes of the network [5]; these factors limit the applicability of such a methodology. In [25] a dual problem is addressed, namely *Cardinality Constrained Critical Node Detection Problem*, which constraints the largest connected component to be smaller than a user-defined value; the objective is to minimize the number of attacked nodes required to fulfill this constraint. In [8] the authors argue that the attacker decision process is intrinsically a multi-objective problem. They suggest improvements where not only the pairwise connectivity, but also the variance in cardinality among the connected components is minimized, i.e., the dimension of the “islands” obtained after removing the k nodes. Such an approach, however, suffers the same drawbacks of the standard CND. Moreover, the two objectives are “scalarized”; such a scalarization is highly dependent on the specific priority between the objectives for the attacker, and thus it has limited validity, especially when the attacker behavior is not known a priori. A similar path is followed in [9], where the size of each connected component obtained as a result of the attack is constrained to be below a given bound. Other related approaches in the literature include frameworks based on the concept of *critical links*, i.e., those links that, if removed cause a relevant degradation of some connection-related index such as the average inverse geodesic

¹ Unit of Automatic Control, Department of Engineering, Università Campus Bio-Medico di Roma, via Álvaro del Portillo 21, 00128, Rome, Italy.

² Consorzio Nazionale Interuniversitario per i Trasporti e la Logistica (NITEL), via Spalato 11, 00198, Rome, Italy.

³ University Rome Tre, Department of Engineering, Via della Vasca Navale 79, 00146, Rome, Italy.

⁴ Information Initiative Center, Hokkaido University, 5 Chome Kita 8 Jonishi, Kita Ward, Sapporo, Hokkaido Prefecture 060-0808, Japan.

* Corresponding author. Email g.oliva@unicampus.it

This research was partially supported by the SECUREWATER Project, which was funded by the Italian Ministry of Foreign Affairs and International Cooperation.

length [26] (i.e., the sum of the inverse of the shortest paths among any pair of nodes). In [10], the authors provide a formulation where the attacker is not constrained to target a fixed number of nodes, and aims at dividing the network in a predetermined number of components while having two conflicting objectives: minimize the number of attacked nodes and minimize the size of the largest component; such an approach is further extended in [12] by considering a convex combination of three objectives. The approaches in [10] and [12], however, considering a scalarized objective function, suffer of the mentioned drawbacks.

A. Contribution

In this paper we introduce a framework for assessing the structural vulnerability of a network in terms of pairwise connectivity after an attack. In a nutshell, the main contributions of this paper are as follows: 1) We develop a novel multi-objective framework to solve the Critical Node Detection problem. Our formulation has remarkably less variables and constraints with respect to the state of the art, yet it is more rich and descriptive, as it does not impose scalarization of the different objectives; 2) We provide novel metrics to assess the robustness of the network as a whole and the criticality of its nodes, based on the Pareto front that represents the set of most effective tradeoffs in the objectives. Specifically, we show that the area underlying the Pareto front of the set of solutions is a global measure of robustness/vulnerability, while the frequency of attack of a given node of the network in the solutions in the Pareto front is a measure of criticality of that node; 3) We show that the node criticality index developed in this paper is an effective guide for the decision maker in deciding how to allocate resources in order to protect the different nodes; the result of the proposed strategy is that the attacker has no more particular preference in attacking the most critical nodes.

Let us now discuss in more details the contributions of this paper and how such contributions position themselves with respect to the state of the art. As discussed above, previous literature typically focuses on optimizing a convex combination of some objectives, but in this way the result has little generality as it is tailored to a particular attacker (e.g., an attacker with large economic resources or an attacker with limited budget). In the proposed approach we aim at considering all possible combinations of the objectives. Thus, instead of inspecting the behavior of a particular attacker, we adopt a multi-objective perspective and we seek the set of most effective attack patterns, i.e., the set of non-dominated solutions. By analyzing such patterns at once, and by looking for recurring schemes within such strategies, we devise novel global and local robustness/vulnerability metrics, i.e., we characterize the robustness of the whole network and the comparative robustness of its elements. Specifically, we take the standpoint of an attacker that aims at disrupting some of the nodes in the network, in order to achieve two conflicting objectives:

- 1) minimize the degree of connectivity in the network;
- 2) minimize the cost of the attack.

To model the degree of connectivity in the network, we take into account the pairwise connectivity (see Section II-C). As for the cost of the attack, we assume each node in the network has a specific cost which, for instance, may depend on the monetary cost of attacking that specific node, on the actual degree of security of the target, or on a combination of the above factors. Based on such an attacker model, we develop a *multi-objective optimization* (MOO) problem.

Notice that most approaches in the MOO literature attempt to provide a single solution based on the set of solutions in the *Pareto front* (i.e., the set of solutions such that no other solution is better with respect to all the optimization criteria) according to different techniques such as linear combinations [27] or other nonlinear techniques [28], [29]. Other approaches, instead, involve the decision maker in the process, by considering also his/her preferences [27], by demanding the choice of the best solution to the decision-maker [30], or considering interactive procedures [31].

In this paper, instead of determining which nodes are critical with respect to a specific balancing of the objectives, we focus on an holistic approach by providing both global and local robustness/criticality metrics that depend on the entire set of solutions in the Pareto front, thus encompassing a broad range of attacker behaviors.

The Pareto front is thus the starting point to define two novel indices that characterize the global robustness of the network and the criticality of the nodes: I) *Global robustness index*: we take the area under the curve that connects the solutions in the Pareto front as a measure of the overall robustness of the network. In fact, the larger is such an area, the higher is the value of the objectives associated to the solutions in the Pareto front; hence, high values of the global robustness index correspond to networks where the attacker is not able to deal large damage, or deals large damage only at a great cost. Conversely, when the area is small, the attacker is able to deal large damage with a small effort. II) *Node criticality index*: nodes that are critical to the connectivity of the network are likely to be selected as target by the attacker in several solutions belonging to the Pareto front. Based on such an intuition, we assess the criticality of a node in terms of the fraction of solutions in the Pareto front in which such a node is attacked. Notice that the area under the Pareto front is not a novel concept in the multi-criteria optimization literature, see for instance [32], [33]. Such an index, however, is typically used as a measure of the quality of stochastic approximation algorithms, since the smaller is such an area, the smaller, overall, is the cost of the solutions in the Pareto front. Applying such an index as a measure of robustness can be regarded as a novel aspect of our approach. Furthermore, by identifying recurring attacked nodes in the solution space of the Pareto front, a novel measure for the criteria criticality is introduced. Given the complexity of solving the MOO problem exactly, especially for large instances, we resort to an approximation technique. We use the MIDACO optimization software which implements an extension of the evolutionary Ant Colony Optimization meta-heuristic [34] and which has been developed especially for highly non-linear real-world applications. See [35] or [36] for a focus of the performance of

MIDACO software with respect to the state of the art. In order to validate the proposed approach, we compare our metrics with respect to classical centrality measures and we consider as case studies two realistic networks, the IEEE118 power network [37] and the US airline network as it was in 1997 [38].

B. Paper Outline

The outline of the paper is as follows: in Section II we provide some preliminary definitions; in Section III we provide two interchangeable multi-objective formulations that model the attacker's behavior; in Section IV we define the proposed robustness/vulnerability metrics; results and discussions are collected in Section V with the aim to validate the proposed framework; some conclusive remarks are collected in Section VI; finally, we give the proofs of theorems and propositions in the Appendix.

II. PRELIMINARIES

A. General Preliminaries

In the following we denote by $|X|$ the cardinality of a set X . Moreover, we denote vectors via boldface letters, and we use \mathbf{k}_m to indicate a vector in \mathbb{R}^m whose components are all equal to k . Finally we denote the sign of $x \in \mathbb{R}$ by $\text{sign}(x)$; moreover, we denote by $\text{sign}(X)$ the entry-wise sign of a matrix X , i.e., a matrix $\text{sign}(X)$ having (i, j) -th entry that corresponds to $(\text{sign}(X))_{ij} = \text{sign}(X_{ij})$.

B. Graph-related definitions

Let $G = \{V, E\}$ be a graph with n nodes $V = \{v_1, v_2, \dots, v_n\}$ and e edges $E \subseteq V \times V$, where $(v_i, v_j) \in E$ captures the existence of a relation between node v_i and node v_j . A graph is *complete* if there is an edge between any two nodes. We denote a complete graph with n nodes by K_n .

A *path* over an undirected graph $G = \{V, E\}$, starting at a node $v_i \in V$ and ending at a node $v_j \in V$, is a subset of links in E that connects v_i and v_j .

An undirected graph is *connected* if for each pair of nodes v_i, v_j there is a path over G that connects them. A *connected component* is a connected subgraph $G_i = \{V_i, E_i\}$ of G (i.e., $V_i \subseteq V$ and $E_i \subseteq E$) such that, over G , no node in V_i is connected to a node in $V \setminus V_i$. The *adjacency matrix* of a graph G is an $n \times n$ matrix A such that $A_{ij} = 1$ if $(v_j, v_i) \in E$ and $A_{ij} = 0$ otherwise.

C. Pairwise Connectivity

We now discuss an index, namely *pairwise connectivity* (PWC) [4], [10], that captures the overall degree of connectivity of a graph.

Definition 1. The PWC is the number of distinct node pairs connected by a path over G , i.e.,

$$PWC(G) = \frac{1}{2} \sum_{v_i, v_j \in V, v_i \neq v_j} p(v_i, v_j), \quad (1)$$

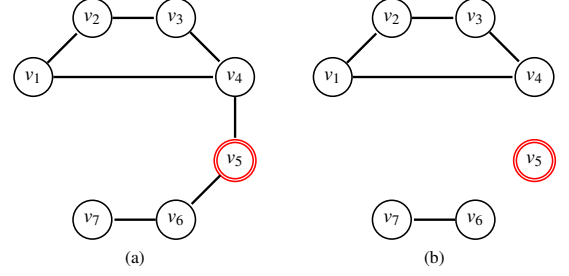


Fig. 1. A sample graph before and after an attack that disconnects node v_5 (in red). The original graph G (panel (a)) is connected, hence all pairs of nodes are connected by a path and $nPWC(G) = 1$. The graph G' after the attack (panel (b)) is disconnected in three connected components (one component corresponds to the isolated node v_5), and the resulting normalized pairwise connectivity is $nPWC(G') = 7/21$.

where $p(v_i, v_j)$ is 1 if the pair (v_i, v_j) is connected via a path in G , and is zero otherwise.

Figures 1a and 1b report the PWC for a sample graph before and after the removal of all links that are incident on a specific node, respectively; it can be noted that the removal of just few edges causes a massive reduction of PWC.

We point out that $PWC(G)$ is monotone non-increasing with respect to edge removals, since the removal of an edge can not increase the number of pairs of nodes connected by a path. Moreover, we note that, if G_{con} is a connected and undirected graph then all its pairs of nodes are connected by a path and it holds $PWC(G_{\text{con}}) = n(n-1)/2$. Therefore, we define the *normalized pairwise connectivity* $nPWC(G)$ as the fraction of unique connected pairs of nodes with respect to the total number of pairs of nodes, i.e.:

$$nPWC(G) = \frac{PWC(G)}{PWC(G_{\text{con}})} = \frac{1}{n(n-1)} \sum_{v_i, v_j \in V, v_i \neq v_j} p(v_i, v_j); \quad (2)$$

clearly, it holds $nPWC(G) \in [0, 1]$. The above index is a convenient way to represent the degree of connectivity in a graph G that is not connected, as it is straightforward to note that $nPWC(G) = 1$ if and only if G is connected, while, when $nPWC(G) < 1$, such an index can be regarded as a measure of the degree of connectivity of G , i.e., the larger is $nPWC(G)$, the closer G is to a connected graph. Note that, even when G is not completely connected, the $nPWC(G)$ is proportional to the fraction of node pairs that are connected by at least one path.

D. Multi-Objective Optimization

Given a vector $\mathbf{x} \in \{0, 1\}^n$ representing n decision variables, an MOO problem can be expressed as follows

$$\min f(\mathbf{x}) = \min [f_1(\mathbf{x}), f_2(\mathbf{x}), \dots, f_k(\mathbf{x})]^T, \quad \text{subject to } \mathbf{x} \in \mathcal{F}, \quad (3)$$

where $k \geq 2$ and the i -th objective is given by $f_i(\mathbf{x}) : \mathbb{R}^n \rightarrow \mathbb{R}$, while $f(\mathbf{x}) : \mathbb{R}^n \rightarrow \mathbb{R}^k$ is the *multi-objective function*. The set \mathcal{F} represents the set of *admissible solutions* for the problem at hand. Moreover, the *multi-objective space* is defined as $\mathcal{Z} = \{\mathbf{z} \in \mathbb{R}^k : \exists \mathbf{x} \in \mathcal{F}, \mathbf{z} = f(\mathbf{x})\}$.

Within a MOO problem, therefore, the aim is to select an admissible solution \mathbf{x} that minimizes at the same time all the different objectives f_i . Let us consider a solution \mathbf{x}^* for which all the objectives $f_i(\mathbf{x}^*)$ are simultaneously minimized, and let us denote the associated multi-objective vector $f(\mathbf{x}^*)$ by \mathbf{z}^{id} . Notice that, when there is no conflict among the objectives, we can solve Problem (3) by solving k scalar problems, thus obtaining \mathbf{z}^{id} as the *ideal* multi-objective vector. Due to the conflicting nature of the objectives $f_i(\mathbf{x})$, however, it is realistic to assume that $\mathbf{z}^{id} \notin \mathcal{Z}$. In most practical cases, therefore, there is a need to overcome the above naive definition of an optimal solution; a typical approach in the literature is to resort to the theory of *Pareto optimality* [39].

Let \mathbf{z}^a and $\mathbf{z}^b \in \mathcal{Z}$; we say that \mathbf{z}^b is *Pareto-dominated* by \mathbf{z}^a ($\mathbf{z}^a \leq_P \mathbf{z}^b$) if: (i) $\mathbf{z}_i^a \leq \mathbf{z}_i^b$ for each $i = 1, 2, \dots, k$ and (ii) $\mathbf{z}_j^a < \mathbf{z}_j^b$ at least for a value of $j \in \{1, \dots, k\}$.

A solution vector $\mathbf{x}^* \in \mathcal{F}$ is a *Pareto optimal solution* if there is no other solution $\mathbf{x} \in \mathcal{F}$ such that $f(\mathbf{x}) \leq_P f(\mathbf{x}^*)$.

The *Pareto front* \mathcal{P} is the set of all possible Pareto optimal solutions \mathbf{x}^* for the problem at hand, while we denote by $\mathcal{P}_f \subseteq \mathcal{Z}$ the set of values $f(\mathbf{x}^*)$, in the multi-objective space, which correspond to each $\mathbf{x}^* \in \mathcal{P}$.

Figure 2 shows an example of Pareto front with respect to $k = 2$ objectives; we show via boxes the points belonging to \mathcal{P}_f and via circles the dominated multi-objective vectors. As an example, point C is dominated from both points A and B , thus is not in the Pareto front.

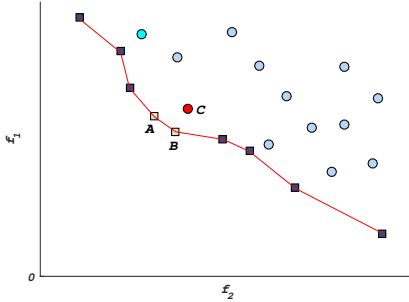


Fig. 2. Example of Pareto front with respect to a problem with $k = 2$ objectives. The points belonging to \mathcal{P}_f are shown with boxes while dominated multi-objective vectors are shown via circles.

III. MODELING ATTACKER'S BEHAVIOR

In this section we provide two complementary ways to represent an attack to the network; then, we provide two formulations to model the behavior of an attacker that has to select which nodes to target in order to simultaneously maximize the damage dealt to the network in terms of reduction of pairwise connectivity and minimize the cost of the attack. These formulations will be the cornerstone for the definition of metrics that characterize the vulnerability/robustness of the different nodes and of the network as a whole. Before proceeding, we reiterate that, in the literature, formulations addressing similar problems consider a scalar convex combination of different objectives, while in this paper we focus on the simultaneous optimization of concurrent objectives (minimizing

the cost and maximizing the damage dealt in terms of PWC reduction). Moreover, in the literature the typical approach is to consider formulations with a large number of constraints (e.g., in [12] $O(|V|^2|E|)$ constraints are required) that are *linear* in the choice variables, i.e., the typical approach is to consider (Mixed) Integer Linear Programming formulations. Conversely, in this paper we aim at providing formulations that are suitable to be solved by an approximated solver (e.g., based on ant-colony optimization or other methodologies). To this end, aside for their multi-objective nature, the proposed formulations differ from traditional approaches. In particular, the first formulation consists of a constrained optimization problem, but with a limited number (i.e., $O(|V| + |E|)$) of *nonlinear* constraints; instead, the second formulation consists of an unconstrained (except for the requirement that the variables must be Boolean) problem. We point out that the first formulation is more descriptive of the inner structure of the problem, while the second one is particularly suitable to be solved by an approximated solver; in fact, the absence of constraints implies that any randomly generated solution will correspond to an admissible solution, thus preventing the solver from performing expensive feasibility checks.

A. Encoding the Attack as a Partition Matrix

Let a graph $G = \{V, E\}$ with n nodes and suppose that a subset V_n of the nodes is attacked. Within the partition matrix approach, we model the attack by focusing on the nodes that are not targeted by the attacker. Specifically, we define n , possibly empty, *partitions* V_1, \dots, V_n of the node set V , i.e., subsets of V such that $V_i \cap V_j = \emptyset$ for all $i, j \in \{1, \dots, n\}$, $i \neq j$ and $V = \bigcup_{i=1, \dots, n} V_i$. Specifically, partition V_n represents the set of attacked nodes, while partitions V_1, \dots, V_{n-1} represent nodes corresponding to the $n - 1$ (possibly empty) connected components of the graph $G' = \{V, E'\}$ obtained as a result of the attack, i.e., such that $E' = \{(v_i, v_j) \in E : v_i \notin V_n \text{ and } v_j \notin V_n\}$. In other terms, E' is the subset of the edges of E that are not incident to the attacked nodes.

We notice that some associations of the nodes in V to the partitions might not correspond to a meaningful attack configuration, since the nodes associated to different partitions should not be connected by a path in the graph G' (otherwise, they would belong to the same component). In order to focus on meaningful attacks, in the following we provide a condition to determine whether an associations of the nodes to the partitions corresponds to a *well-defined attack*, which we define as follows.

Definition 2 (Well-defined attack). *Let $G = \{V, E\}$ be an undirected graph with n nodes and suppose that the nodes in V have been partitioned in V_1, \dots, V_n , where V_n represents the attacked nodes. Moreover, let $G' = \{V, E'\}$ be the graph obtained from G as a result of the attack. The partitions V_1, \dots, V_n correspond to a well defined attack if: (a) each $v_a \in V$ is associated to exactly one partition V_1, \dots, V_n ; (b) for all $v_a, v_b \in V$ with $a \neq b$ and for all $i, j \in \{1, \dots, n - 1\}$ with $i \neq j$ it holds*

$$v_a \in V_i, v_b \in V_j, \Rightarrow (v_a, v_b) \notin E. \quad (4)$$

In other words, a well defined attack is such that each node is associated to at most one partition (otherwise it is attacked) and no two nodes in different partitions are connected by an edge (otherwise, the two nodes would be in the same partition).

The partitions V_1, \dots, V_{n-1} are the cornerstone for the representation of the attack; specifically, we consider the Boolean variables y_{ij} such that $y_{ij} = 1$ if node v_i belongs to the partition V_j and $y_{ij} = 0$, otherwise, and we denote by $Y \in \{0, 1\}^{n \times (n-1)}$ the $n \times (n-1)$ partition matrix having y_{ij} at its (i, j) -th entry.

Let us now provide a condition to verify whether a partition matrix Y corresponds to a well-defined attack; as discussed later, such a condition directly translates into one of the constraints of the proposed formulation.

Proposition 1. Let $G = \{V, E\}$ be an undirected graph with n nodes and let $Y \in \{0, 1\}^{n \times (n-1)}$ be a partition matrix. Matrix Y corresponds to a well-defined attack if and only if the vector

$$\mathbf{x}(Y) = \mathbf{1}_n - Y\mathbf{1}_{n-1} \quad (5)$$

is boolean, i.e., $\mathbf{x}(Y) \in \{0, 1\}^n$ and for all $(v_a, v_b) \in E$ it holds

$$\left(1 - \sum_{i=1}^{n-1} y_{ai}y_{bi}\right) \left(\sum_{i=1}^{n-1} y_{ai}\right) \left(\sum_{i=1}^{n-1} y_{bi}\right) = 0. \quad (6)$$

Proof. See Appendix.

B. Encoding the Attack as an Attack Vector

Let us now provide a different way to represent an attack focusing on the attacked nodes; to this end, let us now provide the following definition.

Definition 3 (Attack Vector). Let $G = \{V, E\}$ be an undirected graph and let us define for each $v_i \in V$ a Boolean variable x_i such that $x_i = 1$ if node v_j is attacked and $x_i = 0$, otherwise. The attack vector $\mathbf{x} \in \{0, 1\}^n$ is the stack of all variables x_i .

We point out that the attack vector \mathbf{x} can be the basis to express the PWC in a closed form, as demonstrated by the following theorem.

Theorem 1. Let us consider a graph $G = \{V, E\}$ with n nodes and an attack vector $\mathbf{x} \in \{0, 1\}^n$. Moreover, let us denote by G' the graph obtained from G as a result of the attack (i.e., obtained by removing the edges that are incident on the attacked nodes). It holds

$$\text{PWC}(G') = \frac{1}{2} \mathbf{1}_n^T (\tilde{A}(\mathbf{x}) - I_n) \mathbf{1}_n \quad (7)$$

where

$$\tilde{A}(\mathbf{x}) = \text{sign} \left(\sum_{h=1}^{n-1} \hat{A}^h(\mathbf{x}) \right),$$

\hat{A} is an $n \times n$ matrix such that

$$\hat{A}_{ij}(\mathbf{x}) = (1 - x_i)(1 - x_j)A_{ij}, \quad (8)$$

and A_{ij} is the (i, j) -th entry of the adjacency matrix associated to the graph G .

Proof. See Appendix.

The above theorem provides an operative procedure for calculating the PWC. The following proposition characterizes the computational complexity of such a procedure.

Proposition 2. Let us consider a graph $G = \{V, E\}$ with n nodes and an attack vector $\mathbf{x} \in \{0, 1\}^n$. Moreover, let us denote by G' the graph obtained from G as a result of the attack. The $\text{PWC}(G')$ can be computed according to Eq. (7) with a computational complexity $O(n^{3.373})$.

Proof. See Appendix.

The following remark collects the main features of the attack vector and compares them with those of the partition matrix; a summary of such a comparison is provided in Table I.

Remark 1. We point out that a given attack to G is univocally determined by the attack vector \mathbf{x} , while there are several partition matrices that correspond to the same set of attacked nodes. Moreover, each attack vector $\mathbf{x} \in \{0, 1\}^n$ corresponds to a meaningful attack, and there is no need to check for well-definedness as in the case of partition matrices Y (in the latter case there is a need to check for $|V| + |E|$ constraints, i.e., we need to verify that each node belongs just to one partition and that each edge in the graph G' obtained as a result of the attack has endpoints belonging to the same component). We also point out that the attack vector requires only $|V|$ Boolean variables, compared to $O(|V|^2)$ Boolean variables necessary to encode an attack in the case of partition matrices. Finally, we note that any partition matrix Y encoding a well-defined attack can be converted into an attack vector via Eq. (5).

TABLE I
MAIN FEATURES OF TWO ALTERNATIVE APPROACHES TO ENCODE ATTACKS AND TO COMPUTE THE PWC AFTER THE ATTACK.

	Partition Matrix Y	Attack Vector \mathbf{x}
Meaning	node v_i in partition V_j	node attacked or not attacked
Variables	$ V ^2$ Booleans	$ V $ Booleans
Constraints	$ V + E $	none
Additional Features	more descriptive	can be used to compute PWC
Suggested Usage	Gain insights on the inner structure of the problem	Approximated solution

C. Multi-Objective Formulation of Attacker's Behavior

We now provide two interchangeable multi-objective formulations for modeling the attacker behavior that are based on the partition matrix Y and on the attack vector \mathbf{x} , respectively. To this end, let us consider an undirected graph $G = \{V, E\}$, and let us encode an attack to G by means of an attack vector \mathbf{x} or a partition matrix Y . In the latter case, let us denote by $\mathbf{x}(Y)$ the attack vector obtained from Y via Eq. (5). In any case, let us denote by G' the graph obtained by G as a result of the attack.

We reiterate that the attacker has two conflicting objectives, in that it aims at minimizing the connectivity of the network after the attack and at keeping the cost of the attack to

a minimum. Specifically, we model the connectivity of the network in terms of the $nPWC$ of the graph after the attack, i.e., we consider the objective $f_1 = nPWC(G')$. Note that, in the following, we use f_i^p and f_i^a to denote the i -th objective computed based on the partition matrix Y or the attack vector \mathbf{x} , respectively. In particular, if we consider the partition matrix Y , the first objective corresponds to

$$f_1^p(Y) = nPWC(G') = \frac{1}{n(n-1)} \mathbf{1}_n^T (\tilde{A}(\mathbf{x}(Y)) - I_n) \mathbf{1}_n,$$

where $\mathbf{x}(Y)$ is the attack vector obtained from Y via Eq. (5). Similarly, if we encode the attack via an attack vector \mathbf{x} , the first objective corresponds to

$$f_1^a(\mathbf{x}) = \frac{1}{n(n-1)} \mathbf{1}_n^T (\tilde{A}(\mathbf{x}) - I_n) \mathbf{1}_n.$$

where the last equation follows from the definition of $nPWC$ and from Theorem 1. Moreover, we consider a second objective f_2 that represents the cost associated to attacking each node v_i , normalized by the sum of the attack cost $c_i \geq 0$ of the nodes $v_i \in V$.

Let $\mathbf{c} \in \mathbb{R}^n$ be the stack vector collecting the attack costs c_i . If we consider a partition matrix Y we model the cost of the attack in terms of an objective $f_2^p(Y) = \mathbf{c}^T \mathbf{x}(Y) / \mathbf{1}_n^T \mathbf{c}$, while we write $f_2^a(\mathbf{x}) = \mathbf{c}^T \mathbf{x} / \mathbf{1}_n^T \mathbf{c}$ if we consider an attack vector \mathbf{x} . Notice that the normalization term $\mathbf{1}_n^T \mathbf{c}$ is introduced so that the objectives are comparable, as they both assume values in $[0, 1]$.

We now provide the two formulations. In the case of a model based on the partition matrix Y , we formulate the attacker in terms of the following MOO problem.

Formulation 1 (Partition Matrix Formulation).

$$\begin{aligned} \min_{Y \in \{0,1\}^{n \times (n-1)}} & [f_1^p(Y), f_2^p(Y)]^T \\ \text{s.t.} & \\ & (1 - \sum_{i=1}^{n-1} y_{ai} y_{bi}) (\sum_{i=1}^{n-1} y_{ai}) (\sum_{i=1}^{n-1} y_{bi}) = 0, \quad \forall (v_a, v_b) \in E \\ & \sum_{j=1}^{n-1} y_{ij} \in \{0, 1\}, \quad \forall v_i \in V. \end{aligned} \quad (9)$$

Note that the first set of constraints enforces that the endpoints of the edges in G' belong to the same partition, while the second set of constraints guarantee that each node belongs to at most one partition (otherwise, it is attacked); overall, the simultaneous enforcing of the first and second set of constraints guarantees that, by Proposition 1, Y corresponds to a well-defined attack.

Conversely, when we consider an attack vector \mathbf{x} we model the attacker's perspective in terms of the following MOO problem

Formulation 2 (Attack Vector Formulation).

$$\min_{\mathbf{x} \in \{0,1\}^n} [f_1^a(\mathbf{x}), f_2^a(\mathbf{x})]^T. \quad (10)$$

Notice that, as discussed above, the latter formulation is

particularly adequate for solving the problem in an approximate way, since the absence of constraints implies that it is straightforward to generate admissible solutions. However, we point out that in both formulations, there is no need to specify a hierarchy between the objectives nor to gain prior information about the psychology of the attacker. It should be further noted that, for the problem at hand, $\mathbf{z}^{id} = [0 \ 0]^T$ corresponds to an ideal attack where the network is completely disconnected without attacking any node; therefore, it is evident that $\mathbf{z}^{id} \notin \mathcal{F}$.

We point out that there are, in principle, $2^{n \times (n-1)}$ possible choices for Y , but not all such solutions are admissible. However, since the set of all possible $\mathbf{x}(Y)$ coincides with the set of all possible attack vectors \mathbf{x} , there are at least 2^n admissible solutions. Similarly, in the case of attack vector formulation, since any choice of $\mathbf{x} \in \{0,1\}^n$ is admissible, it follows that in this case there are 2^n admissible solutions. In both formulations, therefore, the set of admissible solution grows exponentially with the number of nodes, thus calling for an approximated way to find the Pareto front, as discussed in the next section.

IV. EVALUATING NETWORK ROBUSTNESS

Having introduced the proposed model of the attacker's behavior, In this section we develop two novel indices to measure the robustness/criticality of a network as a whole and of its nodes. We remark that such indices do not dependent upon the particular MOO formulation considered, i.e. they can be either based on the attack vector \mathbf{x} or on the vector $\mathbf{x}(Y)$ that is obtained from the partition matrix Y . Therefore, without loss of generality, we express the indices as a function of the attack vector \mathbf{x} .

A. Global Robustness Index

Suppose that the above MOO problem has been solved, identifying the Pareto front composed of m solutions; we reiterate that \mathcal{P} and \mathcal{P}_f denote, respectively, the set of solutions in the Pareto front and the set of solutions in the objective space, i.e., the values assumed by the objective functions f_1 and f_2 associated to each solution in the Pareto front. We characterize the global robustness of the network in terms of the area under¹ the linear interpolation of the points $\mathbf{z}_1, \dots, \mathbf{z}_m \in \mathcal{P}_f$ in the objective space² which correspond to the solutions in \mathcal{P} . Let us denote by $z_{i,1}$ and $z_{i,2}$ the value of a point \mathbf{z}_i in the objective space according to the first objective ($nPWC$) and the second objective (attack cost), respectively, and let us assume that the points in \mathcal{P}_f are ordered by ascending value of attack cost³. Notice that, for any graph G , a solution where no node is attacked can not be dominated and thus belongs to the Pareto front. Similarly, there is always a subset of the nodes which, if attacked, reduce the PWC to

¹We consider Cartesian axes intersecting at the origin $[0,0]^T$.

²In the pseudocode of Algorithm 1, we model this procedure via the function *GetParetoFrontObjectiveSpace*(G, \mathbf{c}).

³In the pseudocode of Algorithm 1, we model this procedure via the function *sort*(\mathcal{P}_f).

zero; this choice, again, corresponds to a solution that belongs to the Pareto front.

We define the Global Robustness Index Γ as the area under the polygonal chain connecting the points in the Pareto front via trapezoidal integration, i.e.,

$$\Gamma = \frac{1}{2} \sum_{i=0}^m (z_{i,2} + z_{i+1,2})(z_{i+1,1} - z_{i,1}). \quad (11)$$

The pseudocode of such a procedure is reported in Algorithm 1.

Algorithm 1 Global Robustness Index Calculation

```

procedure GlobalRobustnessIndex(graph  $G$ , attack costs  $\mathbf{c}$ )
  ▷ Approximated Pareto front (in the objective space)
   $\mathcal{P}_f \leftarrow \text{GetParetoFrontObjectiveSpace}(G, \mathbf{c})$ ;
  ▷ Sort  $\mathbf{z}_i = [z_{i,1}, z_{i,2}]^T \in \mathcal{P}_f$  by ascending attack cost  $z_{i,2}$ 
   $\{\mathbf{z}_1, \dots, \mathbf{z}_m\} \leftarrow \text{sort}(\mathcal{P}_f)$ 
  ▷ Compute  $\Gamma$  via Trapezoidal Integration
   $\Gamma \leftarrow \frac{1}{2} \sum_{i=0}^m (z_{i,2} + z_{i+1,2})(z_{i+1,1} - z_{i,1})$ .
return  $\Gamma$ 

```

As discussed in the introduction, the larger is Γ , the more the solutions in the Pareto front, overall, have high cost. Thus, large values of Γ imply that the attacker is not able to deal large damage, or can deal a large damage only at a high cost. Conversely, a small value of Γ implies that the solutions in the Pareto front result in small values for both the objectives, i.e., the attacker is likely to deal large damage, even when the attack has a negligible cost.

We notice that, for a fixed number n of nodes, it is nontrivial to find the graph having the maximum possible Γ , since such an index is strongly dependent on the attack costs. However, in the case of equal costs, we now show that the complete graph has the largest possible Γ , thus providing a term of comparison in order to evaluate the robustness of sparser graphs.

Theorem 2. *Let G be an undirected graph with n nodes and suppose all costs c_i are equal. It holds*

$$\Gamma \leq \gamma = \frac{1}{n^2(n-1)} \sum_{k=0}^{n-2} (n-k-1)^2$$

and $\Gamma = \gamma$ for $G = K_n$.

Proof. See Appendix.

B. Node Criticality Index

We estimate the criticality of a node in terms of the frequency with which it is a target for an attack in the solutions belonging to the Pareto front. Therefore, we define the *node criticality index* χ_i for a node v_i as $\chi_i = |\mathcal{P}_i|/|\mathcal{P}|$, where \mathcal{P} is the set of solutions in the Pareto front⁴ and \mathcal{P}_i is the subset of solutions in the Pareto front where node v_i is attacked, i.e., $\mathcal{P}_i = \{\mathbf{x}(Y) \in \mathcal{P} \mid x_i(Y) = 1\}$ in the case of Formulation 1 or $\mathcal{P}_i = \{\mathbf{x} \in \mathcal{P} \mid x_i = 1\}$ in the case of Formulation 2.

⁴In the pseudocode of Algorithm 2, we model this procedure via the function $\text{GetParetoFront}(G, \mathbf{c})$.

Algorithm 2 Node Criticality Index Calculation

```

procedure GlobalRobustnessIndex(graph  $G$ , attack costs  $\mathbf{c}$ )
  ▷ Approximated Pareto front
   $\mathcal{P} \leftarrow \text{GetParetoFront}(G, \mathbf{c})$ ;
  for  $i = 1, \dots, n$  do
    ▷ Compute sets  $\mathcal{P}_i$  featuring  $x_i = 1$  or  $x_i(Y) = 1$ .
     $\mathcal{P}_i \leftarrow \{\mathbf{x} \in \mathcal{P} \mid x_i = 1 \text{ or } x_i(Y) = 1\}$ .
    ▷ Compute Node Criticality Index  $\chi_i$ 
     $\chi_i = \frac{|\mathcal{P}_i|}{|\mathcal{P}|}$ .
  return  $[\chi_1, \dots, \chi_n]^T$ 

```

The pseudocode for the computation of such index is given in Algorithm 2.

The above index assigns larger criticality to those nodes v_i that are often attacked in the solutions in the Pareto front, while the criticality of a node is small if it is attacked in few of the solutions in the Pareto front. Notice that, in spite of other network indexes as node degree, betweenness, or the eigenvector centrality, the criticality index can be considered as an holistic parameter able to capture the global relevance of a node in the network in the presence of the concurrent failure of an arbitrary number of nodes. Moreover, as discussed in the next subsection, the above index is useful to design an effective defensive strategy.

C. Defense Strategy based on Node Criticality Index

As noted above, the node criticality index can be the basis to guide the decision-maker in the protection of the different sites. In fact, if the nodes are protected in a way such that the cost of the attack becomes proportional to the node criticality index, then we expect the global robustness index to improve.

Let us consider a scenario where a decision-maker calculates the indices χ_i considering equal attack costs and then implements protection strategies spending a (monetary, etc.) effort on each node that is proportional to its criticality χ_i . Specifically, we assume that, by doing so, the attack costs are no more equal, but instead it holds

$$c_i = \frac{\chi_i}{\sum_{i=1}^n \chi_i}, \quad (12)$$

i.e., the cost of attacking a node v_i is proportional to the node criticality index χ_i for equal attack costs. The effect

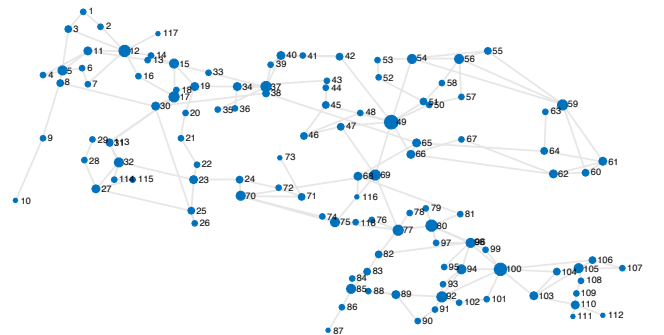


Fig. 3. IEEE 118 Bus Test Case topology [37]. The node size is proportional to its degree.

of such a strategy is twofold. From one side it improves the global robustness index Γ raising up the Pareto front, i.e. reducing the negative effects of an attack. On the other side it contributes to “equalize” the criticality index associated to the different nodes, i.e., it reduces the attractiveness of the most relevant nodes. As a consequence, the attacker is likely to have no preferential targets, since all nodes tend to have similar relevance to him/her. We point out that such an attacker/defendant approach has some points of contact with a min-max Stackelberg game [40], [41], where the defendant moves first and subsequently the attacker performs his choice on the base of the strategy adopted by the defender; within such a framework, a popular defense strategy is to minimize the maximum negative consequences of any attack. Framing our defensive approach in the context of Stackelberg games represents a promising future work direction.

V. CASE STUDIES

In this section we numerically demonstrate the effectiveness of the proposed approach by considering two remarkably different network topologies as case studies, namely the IEEE118 [37] power network and the USAir97 network [38], i.e., the US airline network as it was in 1997.

A. Case Study: IEEE118 Power Network

In this first case study, we apply the proposed framework considering the IEEE 118 power network⁵ [37], [42] (see Figure 3), i.e., a graph with $n = 118$ nodes and $|E| = 179$ links. We now discuss the solvability of the problems modeled in Formulations 1 and 2 via an approximated solver. Specifically, we compare two different multi-objective optimization solvers: NSGA-II [43] and MIDACO [35], [36].

We point out that the two solvers considered have remarkably different features. NSGA-II implements an evolutionary solution selection process, via operations like cross-over and mutation. Conversely, MIDACO is based on a mixed-integer extension of the Ant Colony Optimization (ACO) metaheuristic, combined to multi-kernel Gauss probability functions; within MIDACO the constraints are handled with the oracle penalty method (see [44] for more details).

In Figure 4 we compare the performances achieved by approximating the solution of the two formulations using NSGA-II and MIDACO. In particular, since the area of the Pareto front found by the two solvers tends to be reduced as new non-dominated solutions are found, we evaluate the performances in terms of Global Robustness index Γ over a 24 hours iteration on a machine equipped with a 2×2.66 GHz 6-Core Intel Xeon CPU and 32 GB RAM, and we compare them with the Γ found after 45 days of calculations on the same machine, using the attack vector formulation and MIDACO solver. The results highlight that MIDACO is remarkably more effective than NSGA-II on this type of application; moreover, the approximated solution based on the attack vector formulation converges remarkably faster than the one

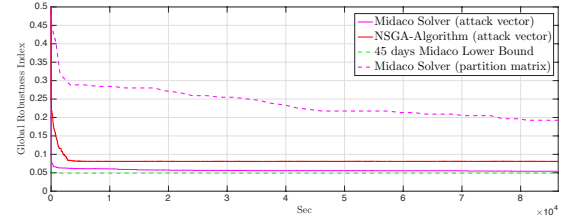


Fig. 4. MIDACO and NSGA-II comparison considering both constrained and unconstrained formulations over IEEE118 Network.

based on the partition matrix formulation. Also, notice that during the simulation NSGA-II algorithm was not able to obtain admissible solutions while approximating the solution of the partition matrix formulation. A potential reason for this behavior might be the large-scale dimension (118 variables) of the application, to which NSGA-II is not well suited. Based on the above experimental results, in the remainder of this section we carry out the computations using the formulation based on attack vectors and MIDACO. However, we reiterate that the proposed approach is essentially independent on the particular solver adopted.

Let us now discuss the insights that can be gained from the proposed indices. In Figure 5 we analyze the indices developed in the previous section in the case of the IEEE118 network and we show the effectiveness of the defense strategy based on the node criticality indices. According to Figure 5a, where we show the criticality indices for equal attack costs, we note that few nodes exhibit significantly larger criticality with respect to the others. In more detail, we observe that three nodes have a criticality index above 0.6 and only two nodes (number 49 and number 100) above 0.7. A valuable insight suggested by the proposed approach, therefore, is that such nodes, being frequently attacked in the solutions belonging to the Pareto front, need to be appropriately protected. By inspecting the topology of this network, we note that the removal of the nodes identified as most critical, indeed, causes the disconnection of the graph in several partitions. In particular, node 100, if removed, disconnects 10 nodes from the network. However, the high criticality associated to node 49 is less intuitive to identify, because its removal, alone, does not generate disconnected components. In fact, we reiterate that, in the proposed approach, the criticality of a node is evaluated in an holistic perspective considering different attackers' strategies. Thus, the focus of the proposed methodology is on the nodes that are preferred by the attacker, rather than on the damage dealt by the deletion of a single node. This claim is supported by the results in Table II, where we show the Kendall's correlation coefficient⁶ [45] among the rankings obtained according to the proposed node criticality indices and to traditional network descriptors, such as degree, betweenness or eigenvector centrality. According to the table, it can be

⁵Notice that we analyze this network only as a benchmark, without considering its physical characteristics in terms of generators, loads, and power flows.

⁶ The Kendall's correlation coefficient τ can be interpreted as a measure of the degree of shuffling of two vectors containing the same elements; in this view, $\tau = 1$ implies that the rankings are almost the same, while $\tau = -1$ models a situation where the rankings are in reverse order. The closer is τ to (minus) one, therefore, the more the two rankings are (anti-) correlated, while the closer is τ to zero the more the two rankings are independent.

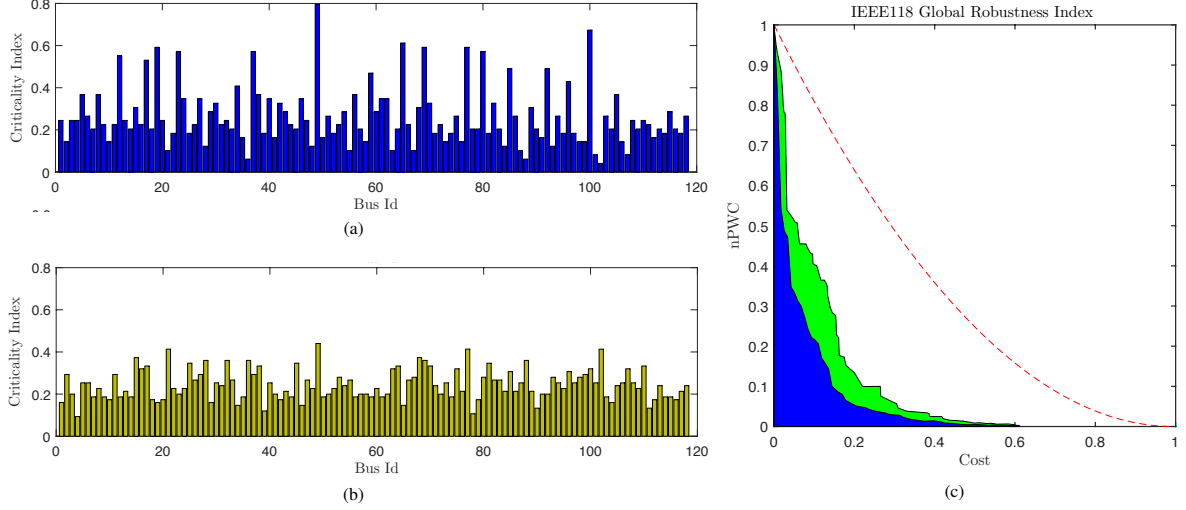


Fig. 5. Proposed indices over the IEEE118 network. Panel (a): node criticality index in the case of equal attack costs. Panel (b): node criticality index when the attack costs are proportional to the node criticality indices calculated for equal attack costs. Panel (c): area under the Pareto front obtained for equal attack costs (in blue) and for costs that are proportional to the node criticality indices (union of the blue and green areas). For comparison reasons the Pareto front of the complete graph K_{118} is reported with a red dashed line.

TABLE II
KENDALL'S RANK CORRELATION COEFFICIENT τ BETWEEN THE RANKINGS OBTAINED ACCORDING TO THE PROPOSED INDEX χ_i AND TO TRADITIONAL CENTRALITY MEASURES (I.E., DEGREE, BETWEENNESS AND EIGENVECTOR CENTRALITY) FOR THE IEEE118 CASE STUDY.

τ	χ_i	Betweenness	Degree	Eigenvector Centrality
χ_i	1	0.0563	-0.0618	-0.0380
Betweenness	*	1	-0.1838	-0.0378
Degree	*	*	1	0.1261
Eigenvector Centrality	*	*	*	1

noted that the proposed metric exhibits almost no correlation with other metrics, thus suggesting that the proposed index represent, indeed, novel information that is not easily captured by other approaches. Let us now demonstrate the effectiveness of the defense strategy discussed in Section IV-C, based on the node criticality index. Specifically, we assume to invest on protection measures proportionally to χ_i , consequently, the attack cost is not uniform for all the node but, as illustrated in Eq. (12), it is higher for the node with high criticality index. In this configuration, the attacker is dissuaded to attack nodes with high attack cost. Specifically, the new criticality indices are reported in Figure 5b. Moreover, in Figure 5c we show the areas under the Pareto fronts obtained for equal attack cost (in blue) and for attack costs proportional to the nodes criticality indices (in green). According to the figure, we observe a relevant increase in Γ as a result of the adopted protection strategy; in particular the Global Robustness index moves from $\Gamma = 0.0607$ in the case of equal costs to $\Gamma = 0.1014$ (i.e., +67.05%) in the case of costs proportional to the original node criticality indices. Notice that such a large increase in the network robustness is achieved at invariant overall costs, i.e., $\sum_{i=1}^n c_i$ remains constant; the proposed defense strategy, in fact, considers a smarter allocation of the available defense resources. Moreover, as emphasized by comparing the critical indices in Figures 6a and 6b, it is evident that in the latter case

the peaks are reduced and the nodes exhibit similar levels of criticality. This suggests that the proposed defense strategy has the effect to reduce the differences in the attractiveness of the nodes, thus greatly reducing the interest of the attacker to target the most relevant nodes.

B. Case Study: US Airline Network as it was in 1997

In order to provide insights on the key differences between the proposed indices and traditional topological descriptors, and in order to inspect the effectiveness of the proposed approximation strategy, we now consider as a case study the US Airline Network as it was in 1997 [38]. Within this network, reported in Figure 6, the $n = 332$ nodes represent the US airports and the $m = 2126$ edges represent a direct flight route between two airports. This network, in addition to being larger than the IEEE 118 network, is also characterized by a different topological configuration: as shown in Figure 6, such a network consists of a core of *hubs*, i.e. nodes with an high degree, while the remaining nodes have rather few connections.

In order to highlight the effectiveness of the proposed approach, we now compare the node criticality indices against the major topological descriptors of the importance of the nodes (i.e., degree, eigenvector centrality and betweenness). Specifically, in Table III we list the 20 most relevant nodes according to the degree, betweenness, eigenvector centrality and node criticality indices (in the case of equal attack costs); we point out that the ranking of the nodes is remarkably different. Such a difference is also highlighted by Figure 7, where we report the distribution of the indices for the different nodes in the network.

In order to validate the proposed defensive strategy, we compare in Figure 8a the Pareto fronts and the Global Robustness indices obtained when the nodes in the network are protected in a way that is proportional to the degree,

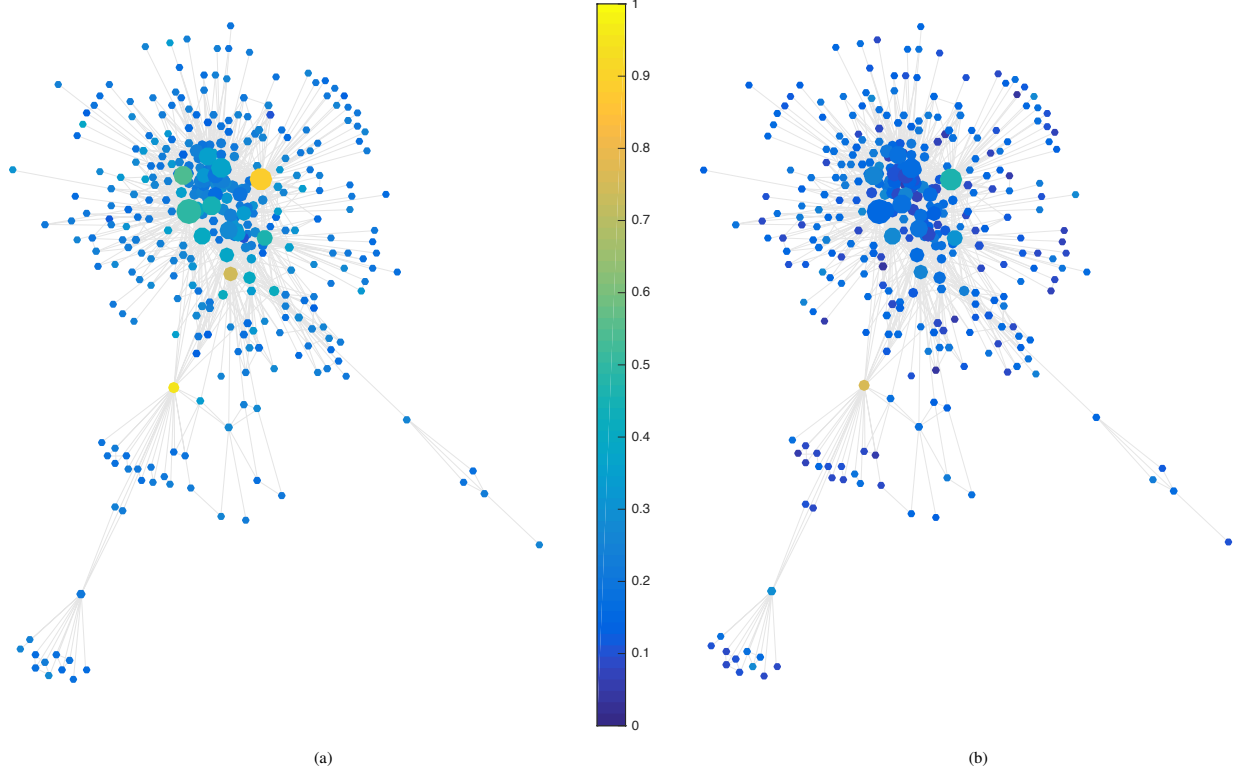


Fig. 6. The US Airline Network as it was in 1997 [38]. The node size is proportional to its degree. The nodes color are related to the critical indices computed considering equal attack costs (panel (a)), and attack costs proportional to the critical indices (panel (b)).

TABLE III

TOP 20 RELEVANT NODES OF USAir97 NETWORK IN TERMS OF NODE DEGREE, BETWEENNESS, EIGENVECTOR CENTRALITY, AND CRITICAL INDEX.

Node ID	Airport	Degree	Node ID	Airport	Betweenness	Node ID	Airport	Eigenvector Centrality	Node ID	Airports	Critical Index
52	Chicago	139	52	Chicago	11376.6251	52	Chicago	0.02070093	13	Anchorage	0.94736842
64	Dallas	118	13	Anchorage	9288.35878	64	Dallas	0.01906758	64	Dallas	0.87719298
18	Atlanta	101	64	Dallas	8366.77448	18	Atlanta	0.01879669	273	Seattle	0.73684211
282	StLouis	94	265	SanFrancisco	5146.29694	282	StLouis	0.01758506	234	Pittsburgh	0.54385965
234	Pittsburgh	94	273	Seattle	5069.27588	234	Pittsburgh	0.01751466	52	Chicago	0.49122807
49	Charlotte	87	282	StLouis	4453.66299	49	Charlotte	0.01695598	265	SanFrancisco	0.45614035
71	Denver	85	18	Atlanta	3904.95499	73	Detroit	0.01647662	282	StLouis	0.43859649
199	Minneapolis	78	234	Pittsburgh	3785.08517	199	Minneapolis	0.01607747	280	Spokane	0.42105263
73	Detroit	70	124	Honolulu	3720.73827	71	Denver	0.01584247	124	Honolulu	0.42105263
265	SanFrancisco	68	28	Bethel	3566.33333	215	Newark	0.01583406	238	Portland	0.40350877
215	Newark	67	199	Minneapolis	3558.45699	55	Cincinnati	0.01545844	199	Minneapolis	0.40350877
231	Philadelphia	62	49	Charlotte	2964.93655	231	Philadelphia	0.01518815	73	Detroit	0.40350877
125	Houston	62	262	SaltLakeCity	2662.49699	222	Orlando	0.01497688	262	SaltLakeCity	0.38596491
55	Cincinnati	61	71	Denver	2496.46029	211	Nashville	0.01442441	90	Erie	0.38596491
232	Phoenix	60	238	Portland	2381.67659	125	Houston	0.01438586	18	Atlanta	0.36842105
262	SaltLakeCity	59	172	LosAngeles	1918.64971	37	Boston	0.01425788	212	NatronaCounty	0.35087719
172	LosAngeles	59	73	Detroit	1753.1415	22	Baltimore-Washington	0.0140217	184	McGheeTyson	0.35087719
273	Seattle	57	232	Phoenix	1407.5583	172	LosAngeles	0.01380031	134	JamesMCoDayton	0.35087719
222	Orlando	56	117	Guam	1308.5	232	Phoenix	0.01356733	101	FresnoAirTerminal	0.35087719
211	Nashville	56	125	Houston	920.726191	57	Cleveland-Hopkins	0.01353207	66	TruaxFie	0.35087719

eigenvector centrality, betweenness⁷ and node criticality indices. Specifically, Figure 8a shows the Pareto front and the value of Γ obtained as a result of each defense strategy. According to the figure, we observe that protecting the nodes based on the node criticality indices is more effective than resorting to classical topological descriptors; in fact, the area underlying the Pareto front, i.e., the global robustness index Γ , is rather unchanged in the case of protection strategies

⁷Since the betweenness of leaf nodes, i.e., nodes with degree equal to one, is equal to zero, in order to avoid attack costs equal to zero, we replace their betweenness with one, which is small compared to the betweenness of non-leaf nodes. However the results obtained are quite similar to those obtained for the original betweenness.

based on degree and eigenvector centrality ($\Gamma = 0.1802$ for the unitary attack costs, while $\Gamma = 0.1984$ for the degree and $\Gamma = 0.1882$ in the case of eigenvector centrality), and is remarkably reduced while considering the betweenness (i.e., $\Gamma = 0.1147$); conversely, we notice a relevant improvement in the case of costs that are proportional to the original criticality indices (i.e., we obtain $\Gamma = 0.2225$). Such results are also highlighted by Figure 8b, where we report the variations in percentage of the global robustness index with respect to the original configuration (i.e., with respect to the case of equal attack costs). In particular we point out that, despite the betweenness distribution and critical index distribution share

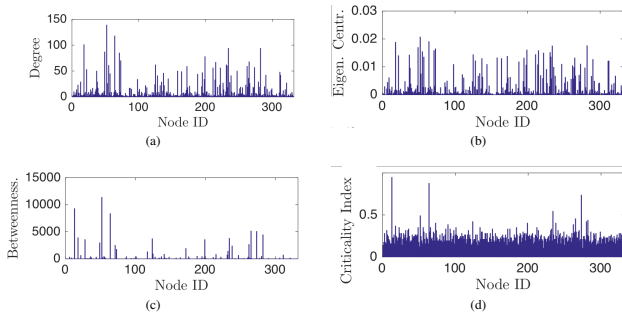


Fig. 7. Node degree, eigenvector centrality, betweenness, and critical index (in the case of unitary attack costs) for the USAir97 Network.

13 out of 20 most relevant nodes (see Table III), the adoption of a protection strategy based on the betweenness causes a degradation of the network robustness.

A rationale for this can be inferred observing Figure 7. Classical indexes, by focusing on the particular role of a node in the network, tend to give emphasis to the hubs, thus attributing large part of the protection budget to the those that seems very relevant nodes, leaving not adequately protected the other nodes (this is particularly evident in the case of the betweenness, where some node are thousands of times more important than others). On the contrary, the node criticality index exhibits an holistic perspective: even if it emphasizes the criticality of particular nodes, it attributes a non-negligible relevance to each node in the network (see Figure 7); hence, a protection strategy based on such an index has the ability to protect, to some extent, all the nodes.

In more detail, we analyze in Figure 6 the results of the proposed defense strategy, where we use a colormap to represent the criticality of each node in the network, considering equal attack costs (left) and attack costs proportional to the node criticality indices (right); the degree of each node is represented by the width of the node (the larger is the node, the larger is its degree). In the left panel of Figure 6 we observe the presence nodes with an high critical index, and we point out that such a criticality is not necessarily associated to large degree. Let us highlight an insight provided by the proposed methodology that would have not been understood by using traditional metrics. In fact, we observe that the most critical node according to the node criticality indices is the Anchorage airport (see Table III), which is not a large hub (i.e. it has comparatively small degree), but it is essential for each flight between the USA and Alaska. As shown by the colormap on the right, the proposed defense strategy has the effect to uniform the attractiveness of the different nodes, i.e., from the attacker perspective the nodes became of almost equal relevance (the only exception is the node 13—Anchorage due to its peculiar position in the network). As mentioned before, this represents an effective choice for the defendant, since it reduces the potential impact of any attack (this is also supported by the increase in Γ as a result of the protection strategy). We reiterate that the proposed methodology is able to emphasize elements that are not adequately captured by traditional metrics such as degree, betweenness or the eigenvector centrality.

C. Effectiveness of the Proposed Approximation Scheme

To conclude this section, we provide a simulation campaign aimed at demonstrating the effectiveness of our approximation the Pareto front. To this end, let χ^N be the vector of critical indices computed by the optimization solver after N evaluations.

In Figure 9 we compare the node criticality indices obtained as a function of the number of evaluations/iterations within MIDACO solver; specifically, we show for selected iterations the resulting criticality indices and we compare them in the rightmost plot. In more detail, the comparison is done by computing for each vector χ^N of critical indices, an index

$$\phi^N = \frac{1}{n} \|\chi^N - \chi^{1M}\|^2,$$

that is the difference in square Euclidean norm between χ^N and the vector χ^{1M} corresponding to the criticality indices obtained for one million evaluations; the index is normalized by $n = 332$, so that $\phi^N \in [0, 1]$, where $\phi^N = 1$ means that the two vectors are completely different and $\phi^N = 0$ means they are the same vector. According to the figure, the index ϕ^N tends to zero as N grows, and assumes quite small values after just $N = 1000$ evaluations; this suggests that the proposed approach is quite effective in approximating the ideal criticality indices in reasonable time.

To conclude, we point out that the proposed approximated way of computing the Pareto front is quite effective, and the availability of the theoretical Pareto front, obtained by solving exactly either of the proposed formulations, is not mandatory in order to gain meaningful insights on the criticality of the nodes and of the networks as a whole, and in order to implement effective protection strategies.

VI. CONCLUSIONS

In this paper we provide a multi-objective optimization framework to assess the level of robustness/vulnerability of a network and its nodes with respect to attacks aiming at dealing large damage while keeping the cost of the attack as small as possible. Without making assumptions on the psychology of the attacker, we follow a multi-objective approach and we consider the Pareto front of the possible solutions, looking for the attack patterns that correspond to different trade-offs between the conflicting objectives of the attacker. Based on such a framework, we develop novel indices, namely Global Robustness Index and Node Criticality Indices, that characterize the robustness of the network as a whole and the criticality of the nodes, respectively. Specifically, we characterize the overall robustness of the network in terms of the area underlying the Pareto front, and the criticality of each node in terms of the fraction of times a solution in the Pareto front corresponds to an attack strategy where such a node is attacked. Since the exact knowledge of the Pareto front might not be easily obtained in practical scenarios, we consider an approximated ant-colony solver, namely MIDACO solver and we show its effectiveness by comparing it with a popular solver, namely NSGA-II, and by verifying experimentally that the approximated Pareto front exhibits fast convergence

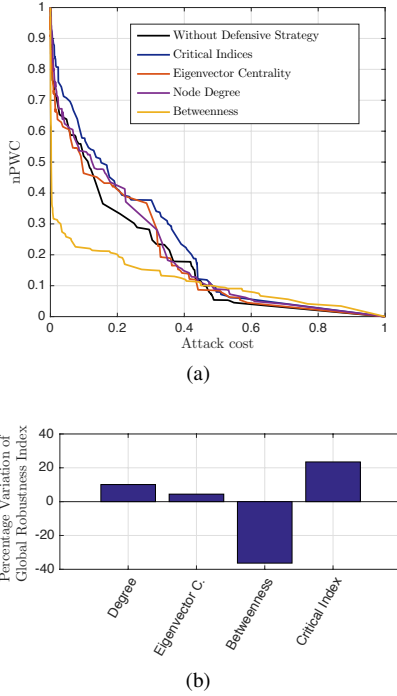


Fig. 8. Panel (a): comparison of Pareto fronts considering attack costs proportional to node degree, betweenness, eigenvector centrality, and critical index. Panel (b): percentage of variation of the global robustness index by adopting different protection plans respect to the unitary cost case.

to the real one, thus justifying the proposed approximation scheme. Moreover, we show that the proposed node criticality index can be useful guide for prioritizing the protection of the different nodes in the network; in fact, the experimental results in this paper suggest that, by protecting the nodes in a way that is proportional to their node criticality index, we are able to concretely increase the overall robustness of the network with respect to any attack's strategy. Notice that this property is obtained by reducing the attractiveness of the most critical nodes, hence minimizing the maximum impact of any attack strategy with prescribed attack cost. We validate the proposed approach with respect to two real world networks, namely the IEEE 118 power network and the network of air flights in USA as it was in 1997. Future work will aim at applying the proposed methodology to multi-layer or hierarchical networks and to adopt this framework as a support for the optimal re-design of the network. Moreover we will inspect the possibility to model the damage dealt by the attacker in terms of the reduction of flow over the network (e.g., for power or gas networks). A last envisaged future research direction is to frame the proposed defense strategy in the context of Stackelberg games [40], [41].

APPENDIX: PROOFS

Proof (Proof of Proposition 1). \Rightarrow Suppose that Y corresponds to a well defined attack. By definition, Y corresponds to an association of the nodes to the partitions where each node is associated to at most one partition, hence we conclude that $\mathbf{x}(Y) \in \{0,1\}^n$. Note that, for all $(v_a, v_b) \in E$ it holds $\sum_{i=1}^{n-1} y_{ai}y_{bi} = 1$ if v_a and v_b are not attacked and $\sum_{i=1}^{n-1} y_{ai}y_{bi} = 0$, otherwise; moreover, for all $v_a \in V$ it holds

$\sum_{i=1}^{n-1} y_{ai} = 1$ if v_a is not attacked and $\sum_{i=1}^{n-1} y_{ai} = 0$, otherwise. Since we assumed the attack is well defined, no two nodes in different partitions are connected by a link; in other words one of the following two events must occur: (i) v_a and v_b are in the same partition; (ii) either v_a or v_b (or both) are attacked. Overall, we note that such condition is verified if and only if Eq. (5) holds true.

\Leftarrow Suppose that $\mathbf{x}(Y) \in \{0,1\}^n$ and that Y satisfies the constraint in Eq. (6). In this case, we note that each node is associated to just one partition (or is attacked), hence it holds $x_\ell(Y) = 1 - \sum_{i=1}^{n-1} y_{\ell i}$, i.e., $x_a(Y) = 1$ if and only if v_a is attacked. As a consequence, Eq. (5) can be rearranged as

$$\left(1 - \sum_{i=1}^{n-1} y_{ai}y_{bi}\right) (1 - x_a(Y))(1 - x_b(Y)) = 0. \quad (13)$$

By Definition 2, the partition matrix Y encodes a well-defined attack if and only if $\sum_{i=1}^{n-1} y_{ai}y_{bi} = 1$ or either v_a or v_b (or both) are attacked, i.e., if and only if Eq. (13) is satisfied. We conclude therefore that conditions (5) and (6) are necessary and sufficient for Y to encode a well-defined attack. This completes our proof. \square

Proof (Proof of Theorem 1). We point out that, by Eq. (8), it holds $\hat{A}_{ij}(\mathbf{x}) = 1$ if and only if there is a link $(v_i, v_j) \in E$ and neither v_i nor v_j have been attacked. Therefore, matrix $\hat{A}(\mathbf{x})$ represents the adjacency matrix associated to G' , i.e., the adjacency matrix after the attack has been carried out and all links incident to the nodes having $x_i = 1$ have been removed. It is well known [46] that the (i, j) -th entry of the h -th power of the adjacency matrix of a graph G' is equal to the number of paths of length h between v_i and v_j over G' . Therefore, since a path has at most length $n - 1$, the entry $\tilde{A}_{ij}(\mathbf{x})$ for $i \neq j$ is equal to one if there is a path from v_i to v_j and is equal to zero otherwise. Note that, for $n > 1$, there must be at least one path of length 2 between any node v_i and itself; hence, the diagonal entries $\tilde{A}_{ii}(\mathbf{x}) = 1$ for all v_i . Therefore, the sum of the entries of matrix $\tilde{A}(\mathbf{x}) - I_n$ corresponds to the number of pairs of nodes connected by a path, counting each pair twice. Hence, we conclude that $PWC = \frac{1}{2} \sum_{i=1}^n \sum_{j=1, j \neq i}^n \tilde{A}_{ij}(\mathbf{x}) = \frac{1}{2} \mathbf{1}_n^T (\tilde{A}(\mathbf{x}) - I_n) \mathbf{1}_n$, which is the thesis. This completes our proof. \square

Proof (Proof of Proposition 2). The complexity of square $n \times n$ matrix multiplication is known to be $O(n^{2.373})$ [47]. Since the computation of the PWC via Eq. (7) is done by performing $n - 1$ matrix multiplications, the computational complexity is $O(n^{3.373})$. This completes our proof. \square

Proof (Proof of Theorem 2). Notice that, over a complete graph, the removal of all the links incident to any node corresponds to the loss of $n - 1$ connections, and the resulting PWC becomes $PWC(K_{n-1})$. Similarly, the removal of all the links incident to any m nodes correspond to a resulting PWC that is $PWC(K_{n-m})$. If all costs are equal to c , it holds

$$\mathcal{P}_f = \left\{ \left[\frac{PWC(K_{n-i})}{PWC(K_n)} \quad \frac{i}{n} \right]^T \text{ s.t. } i = 0, \dots, n-1 \right\}.$$

Since the removal of any m nodes results in a complete graph

with $n - m$ nodes, we can conclude that the resulting n PWC when m nodes are removed is the largest possible n PWC for all graphs with n nodes. Therefore, in the case of equal costs, the value of Γ for K_n is an upper bound for any other graph with n nodes. By Eq. (11), for a complete graph K_n we have that

$$\begin{aligned}\gamma &= \frac{1}{2} \sum_{k=0}^{n-2} \left(\frac{PWC(K_{n-k})}{PWC(K_n)} + \frac{PWC(K_{n-k-1})}{PWC(K_n)} \right) \left(\frac{k+1}{n} - \frac{k}{n} \right) = \\ &= \frac{1}{2nPWC(K_n)} \sum_{k=0}^{n-2} (PWC(K_{n-k}) + PWC(K_{n-k-1})).\end{aligned}$$

Note that it holds $PWC(K_{n-k}) + PWC(K_{n-k-1}) = 2(n-k-1)^2$ hence, it holds $\gamma = \sum_{k=0}^{n-2} (n-k-1)^2 / (n^2(n-1))$. This completes our proof. ■

REFERENCES

- [1] A. Atputharajah and T. K. Saha, "Power system blackouts-literature review," in *2009 International Conference on Industrial and Information Systems (ICIS)*. IEEE, 2009, pp. 460–465.
- [2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
- [3] R. Filippini and A. Silva, "I@ML: An infrastructure resilience-oriented modeling language," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 1, pp. 157–169, 2015.
- [4] A. Arulselman, C. W. Commander, L. Eleftheriadou, and P. M. Pardalos, "Detecting critical nodes in sparse graphs," *Computers & Operations Research*, vol. 36, no. 7, pp. 2193–2200, 2009.
- [5] M. Di Summa, A. Grosso, and M. Locatelli, "Branch and cut algorithms for detecting critical nodes in undirected graphs," *Computational Optimization and Applications*, vol. 53, no. 3, pp. 649–680, 2012.
- [6] Y. Shen, N. P. Nguyen, Y. Xuan, and M. T. Thai, "On the discovery of critical links and nodes for assessing network vulnerability," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 3, pp. 963–973, 2013.
- [7] T. N. Dinh, Y. Xuan, M. T. Thai, P. M. Pardalos, and T. Znati, "On new approaches of assessing network vulnerability: hardness and approximation," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 609–619, 2012.
- [8] M. Ventresca, K. R. Harrison, and B. M. Ombuki-Berman, "An experimental evaluation of multi-objective evolutionary algorithms for detecting critical nodes in complex networks," in *European Conference on the Applications of Evolutionary Computation*. Springer, 2015, pp. 164–176.
- [9] M. Lalou, M. A. Tahraoui, and H. Kheddouci, "Component-cardinality-constrained critical node problem in graphs," *Discrete Applied Mathematics*, 2015.
- [10] L. Faramondi, G. Oliva, F. Pascucci, S. Panzieri, and R. Setola, "Critical node detection based on attacker preferences," in *Control and Automation (MED), 2016 24th Mediterranean Conference on*. IEEE, 2016, pp. 773–778.
- [11] L. Faramondi, G. Oliva, R. Setola, F. Pascucci, A. E. Amideo, and M. P. Scaparra, "Performance analysis of single and multi-objective approaches for the critical node detection problem," in *International Conference on Optimization and Decision Science*. Springer, 2017, pp. 315–324.
- [12] L. Faramondi, R. Setola, S. Panzieri, F. Pascucci, and G. Oliva, "Finding critical elements in infrastructure networks," *International Journal of Critical Infrastructure Protection*, 2017 (to Appear).
- [13] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.
- [14] M. P. Scaparra and R. L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Computers & Operations Research*, vol. 35, no. 6, pp. 1905–1923, 2008.
- [15] Z.-M. Lu and X.-F. Li, "Attack vulnerability of network controllability," *PLoS one*, vol. 11, no. 9, p. e0162289, 2016.
- [16] O. Lordan, J. M. Sallan, P. Simo, and D. Gonzalez-Prieto, "Robustness of the air transport network," *Transportation Research Part E: Logistics and Transportation Review*, vol. 68, pp. 155–163, 2014.
- [17] R. Albert, H. Jeong, and A. L. Barabási, "Error and attack tolerance of complex networks," *nature*, vol. 406, no. 6794, pp. 378–382, 2000.
- [18] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, p. 056109, 2002.
- [19] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 6, p. 065101, 2011.
- [20] S. Bernardi and J. Campos, "A min-max problem for the computation of the cycle time lower bound in interval-based time petri nets," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 5, pp. 1167–1181, 2013.
- [21] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Percolation of localized attack on complex networks," *New Journal of Physics*, vol. 17, no. 2, p. 023049, 2015.
- [22] Y. Berezin, A. Bashan, M. M. Danziger, D. Li, and S. Havlin, "Localized attacks on spatially embedded networks with dependencies," *Scientific reports*, vol. 5, 2015.
- [23] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.
- [24] F. Sun and M. A. Shayman, "On pairwise connectivity of wireless multihop networks," *International Journal of Security and Networks*, vol. 2, no. 1-2, pp. 37–49, 2007.
- [25] W. Pullan, "Heuristic identification of critical nodes in sparse real-world graphs," *Journal of Heuristics*, vol. 21, no. 5, pp. 577–598, 2015.
- [26] P. Crucitti, V. Latora, and M. Marchiori, "Locating critical lines in high-voltage electrical power grids," *Fluctuation and Noise Letters*, vol. 5, no. 02, pp. L201–L208, 2005.
- [27] C. L. Hwang and A. S. M. Masud, *Multiple objective decision making methods and applications: a state-of-the-art survey*. Springer Science & Business Media, 2012, vol. 164.
- [28] A. P. Wierzbicki, "A mathematical basis for satisficing decision making," *Mathematical modelling*, vol. 3, no. 5, pp. 391–405, 1982.
- [29] M. Zeleny and J. L. Cochrane, *Multiple criteria decision making*. University of South Carolina Press, 1973.
- [30] R. S. Motta, S. M. B. Afonso, and P. R. Lyra, "A modified NBI and NC method for the solution of N-multiobjective optimization problems," *Structural and Multidisciplinary Optimization*, vol. 46, no. 2, pp. 239–259, 2012.
- [31] K. Miettinen, F. Ruiz, and A. P. Wierzbicki, "Introduction to multi-objective optimization: interactive approaches," in *Multiobjective Optimization*. Springer, 2008, pp. 27–57.
- [32] F. Castillo, A. Kordon, and G. Smits, "Robust Pareto front genetic programming parameter selection based on design of experiments and industrial data," in *Genetic Programming Theory and Practice IV*. Springer, 2007, pp. 149–166.
- [33] M. Kotanchek, G. Smits, and E. Vladislavleva, "Pursuing the Pareto paradigm: tournaments, algorithm variations and ordinal optimization," in *Genetic Programming Theory and Practice IV*. Springer, 2007, pp. 167–185.
- [34] M. Dorigo, "St & tle t. ant colony optimization," 2004.
- [35] M. Schlüter, M. Gerdts, and J.-J. Rückmann, "A numerical study of MIDACO on 100 MINLP benchmarks," *Optimization*, vol. 61, no. 7, pp. 873–900, 2012.
- [36] M. Schlueter, S. O. Erb, M. Gerdts, S. Kemble, and J.-J. Rückmann, "MIDACO on MINLP space applications," *Advances in Space Research*, vol. 51, no. 7, pp. 1116–1131, 2013.
- [37] R. D. Christie, "IEEE power systems test case archive," <http://ee.washington.edu/research/pstca>, 1999, [Online; accessed 13-September-2016].
- [38] V. Batagelj and A. Mrvar, "Pajek datasets," 2006.
- [39] Y. Censor, "Pareto optimality in multiobjective problems," *Applied Mathematics and Optimization*, vol. 4, no. 1, pp. 41–59, 1977.
- [40] V. Bier, S. Oliveros, and L. Samuelson, "Choosing what to protect: Strategic defensive allocation against an unknown attacker," *Journal of Public Economic Theory*, vol. 9, no. 4, pp. 563–587, 2007.
- [41] V. M. Bier, N. Haphuriwat, J. Menoyo, R. Zimmerman, and A. M. Culp, "Optimal resource allocation for defense of targets based on differing measures of attractiveness," *Risk Analysis*, vol. 28, no. 3, pp. 763–770, 2008.
- [42] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.
- [43] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE transactions on evolutionary computation*, vol. 6, no. 2, pp. 182–197, 2002.

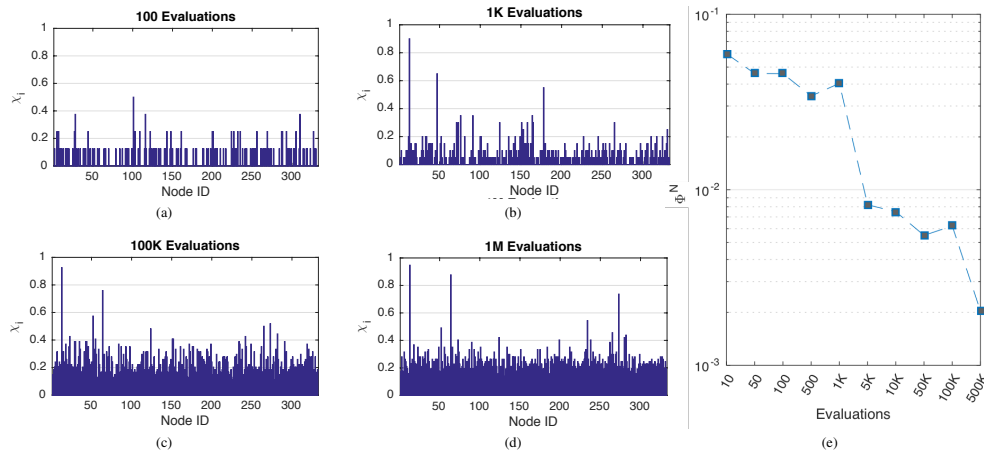


Fig. 9. Criticality indices obtained for different numbers of evolutions/iterations of the adopted solver and normalized square norm of the difference between the different vectors and the one for one million iterations.

- [44] M. Schlüter and M. Gerds, "The oracle penalty method," *Journal of Global Optimization*, vol. 47, no. 2, pp. 293–325, 2010.
- [45] M. G. Kendall, "A new measure of rank correlation," *Biometrika*, vol. 30, no. 1/2, pp. 81–93, 1938.
- [46] N. Biggs, *Algebraic graph theory*. Cambridge university press, 1993.
- [47] A. M. Davie and A. J. Stothers, "Improved bound for complexity of matrix multiplication," *Proceedings of the Royal Society of Edinburgh: Section A Mathematics*, vol. 143, no. 02, pp. 351–369, 2013.



Federica Pascucci received the MS in Computer Science and Automation Engineering (2000) from the University of Roma Tre and the PhD in System Engineering (2004) from the University of Rome "La Sapienza". Since 2005, she is with the Department of Engineering of the University of Roma Tre as Assistant Professor. She was visiting scholar at the University of Örebro (2003) and at the University of Cyprus (2013). She is the principal investigator in several EU funded projects. Her research interests include wireless sensor networks, indoor localization, cyber physical systems, industrial control systems, and critical infrastructure protection. She has published more than 80 journal and conference papers, receiving three best conference paper awards.



Luca Faramondi received the Laurea degree in Computer Science and Automation (2013) and the PhD degree in Computer Science and Automation (2017) from the University Roma Tre of Rome. He is currently PostDoc Fellow at Complex Systems & Security Laboratory at the University Campus Bio-Medico of Rome. He is involved in several national and European projects about the Critical Infrastructure and Indoor Localization. His research interests include the identification of network vulnerabilities, cyber physical systems, and optimization at large.



Martin Schlueter is employed as post-doctoral researcher at the University of Hokkaido (Japan). He obtained his Ph.D. in applied mathematics from the University of Birmingham (UK) in 2012. In collaboration with the European Space Agency (ESA) and Astrium (Airbus) he developed the MIDACO optimization software, which holds several best-known record solutions to interplanetary space mission trajectory benchmarks.



Gabriele Oliva (M'11) received the Laurea degree and the Ph.D in Computer Science and Automation Engineering in 2008 and 2012, respectively, both at University Roma Tre of Rome, Italy. He is currently assistant professor in Automatic Control at the University Campus Bio-Medico of Rome, Italy. His main research interests include distributed systems, distributed optimization, and applications of graph theory in technological and biological systems.



than 100 journal papers and conference papers.

Masaharu Munetomo received the B.A. degree in Electrical Engineering (1991) the M.A. degree in Information Engineering (1993) and the Ph.D in Information Engineering (1996) at the Hokkaido University, Japan. Since 2012, he serves as full professor at the Graduate School of Information Science and Technology, Hokkaido University, Japan, where he is the director of the Information Initiative Center. His main research interests include Evolutionary Computation and Cloud Computing. He is involved in several research projects and he authored more



Stefano Panzieri received the "Laurea" degree in Electronic Engineering in 1989 and the Ph.D. in Systems Engineering in 1994, both from the University of Roma "La Sapienza". Since February 1996 he is with the Engineering Department of University of "Roma Tre", as Associate Professor. He is the director of the Automatic Laboratory of the Engineering Department. His research interests are in the field of industrial control systems, robotics and sensor fusion.



Roberto Setola received the Laurea degree in Electronic Engineering (1992) and the PhD in Control Engineering (1996) from the University of Naples "Federico II". He is Professor at the University Campus Bio-Medico, where he directs the Automation Research Unit and the Master Program in Homeland Security. He was responsible for the Italian Government Working Group on Critical Information Infrastructure Protection (CIIP) and a member of the G8 Senior Experts' group for CIIP. He has been the coordinator of several EU projects and he authored seven books and more than 150 scientific papers. His main research interests are the simulation, modeling and control of complex systems and Critical Infrastructure Protection.