Chapter

A Strategy to Improve Infrastructure Survivability via Prioritizing Critical Nodes Protection

Luca Faramondi, Giacomo Assenza, Gabriele Oliva, Ernesto Del Prete, Fabio Pera and Roberto Setola

Abstract

From an engineering point of view, the survivability of a system is defined as its ability to continue to operate despite a natural or human-made disturbance; for example a serious mechanical fault, a human error, or a malicious cyber or physical attack. In the context of critical infrastructures, due to their relevance for the public wellness, it is mandatory to improve the robustness of such systems in order to ensure the availability of essential services such as the distribution of water, gas and electrical power. Nowadays, due to the increasing number of cyber incidents, the definition of protection strategies, able to improve the survivability level of this infrastructure, is at the heart of the scientific debate. In this chapter we propose a procedure based on three steps aimed at improving infrastructure survivability. In the first stage we propose some approaches to identify the criticality degree of each subsystem composing the infrastructure, in the second stage we propose a method to aggregate multiple criticality evaluations performed by subject matter experts by providing a unique holistic indicator. Finally, on the basis of such indicator, we propose a protection strategy to improve the robustness of the entire system.

Keywords: critical nodes, network robustness, protection strategy, optimization problem, cooperative games

1. Introduction

The physical and cyber protection of critical infrastructures (CIs) is crucial to ensure the availability of multiple essential services. Concerning the physical security aspects, critical infrastructures are, in most cases, complex and geographically distributed systems hence hard to protect. Regardless of the specific scenario, a CI can be represented as a set of sub-systems able to interact and cooperate in order to provide services that are essential for the economy, society and public wellness. For example, in gas distribution systems, the cooperation of metering and regulation stations is fundamental to guarantee the proper functioning of the entire infrastructure. In power grids and water distribution infrastructures, the availability of

electrical power and water, depends respectively on the joint action of singular sub-systems such as bus or water supply stations. Analogously, the correct operation of a plant depends on the right operativeness of several elements as illustrated by the 4STER European project.

Critical infrastructure are characterized by a high level of interconnection and interdependency where the operation of a subsystem is essential for the functioning of others. In such a context, the disruption of a subsystem can easily escalate creating waterfall effect impacting multiple services and geographic areas. Therefore, in order to guarantee the functioning of the entire infrastructure it is necessary to protect adequately each sub-system from fault or exogenous events potentially capable of compromising normal operativity levels. As reported in [1], on the 28th September 2003, in Italy and some areas of Switzerland, about 56 million people lost power due to a storm-tossed tree branch that hit Swiss power lines. About 30,000 people remained trapped in trains, several hundred passengers were stranded on underground transit systems, and there were significant knock-on effects across other critical infrastructures. Similarly, the 2005 Hurricane Katrina [2] caused widespread power outages throughout Louisiana, Mississippi, Alabama, Florida, Kentucky and Tennessee due to the cascading effects initiated by a local event. Another example is the 2011 Great East Japan earthquake [3] and the resulting tsunami: 1.5 million households did not have access to their water supply, 4.4 million households were left without electricity, and all the local railway services were halted, and communications were suspended.

Domino effects over the entire infrastructure due to local fault are not caused only by accidental faults or natural disasters, but could also be intentionally caused by malicious actors. For example, with the increasing reliance of CI on Information & Communication Technology (ICT) malicious actors can perform attacks via cyberspace triggering service disruptions significant economic losses and even kinetic effects. This has been particular concerning in relation to the energetic sector with a significant increase of cyber threats capable of causing outages and blackout in power systems.

The first example of how a cyber attack can affect the operativity of CI causing mechanical damage was provided by the Aurora project [4]. This was a test performed by the Idaho National in which the simulation of a cyberattack led to the destruction of a 27-ton generator. Another Significant example is represented by the Stuxnet worm. The worm was able to modify the rotation speed of particular motors installed inside the centrifuges used for the uranium enrichment in plant in Iran. Similarly, recent blackouts in Ukraine in 2015 and 2016 were respectively caused by Blackenergy3 and CrashOverride, two malware specially designed to cause blackouts via cyber intrusion [5].

In addition, we have to consider impacts on workers' safety. Power plants, water plants, gas plants can provoke accidents and enormous damages. Seveso plants can be used for the storage of hazardous materials: an attack aimed at these plants can also cause a domino effect. The capability to adjust machine parameters in order to improve performance or simply in order to change behavior can make other people with criminal intent adjust parameters so that workers and others can be put at risk of harm. Example of parameters can be speeds, forces, torques that can be put at dangerous levels. In addition, graphical interfaces used for human-machine interaction can be altered so that people could see a situation not corresponding to reality (not reported error codes or messages, different values of parameters or measures). In order to identify hazards associated to the use of a machine or a set of machines, procedures like HAZOP, HAZID, accident reviews must be taken into consideration. Anyway, security and safety must be considered as part of the normal working processes and not always this happens.

The main common aspect about these cited events is that a local event is able to compromise the functionality of the entire plants due to a domino effect. The identification of the most critical sub-systems is a crucial point for the definition of effective protection strategies able to improve the survivability of the systems. To this end, it is fundamental to identify adequate metrics and indicators to quantify the criticality rate associated to each sub-system, especially in highly heterogeneous contexts.

1.1 Related works

From the literature, one of the typical strategies to obtain such metrics is to simulate the effects of negative events, such as local faults, in order to provide insights on the most critical elements, for which protection needs 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 while keeping low the effort required for his/her malicious action. Starting from the seminal works of Arulsevan et al. [6] it has become paramount that attacks that take into account the topology of the infrastructure, can select more effectively the target sites, increasing the damage dealt (e.g., in terms of disconnection of large portions of the infrastructure by causing services interruption). In [7–10] multiple approaches for the identification of critical nodes in infrastructure networks are presented. All these methods consists in optimization problems able to discover the nodes whose removal from the network compromise the connectivity of the entire system. All these approaches requires initial assumptions about the attacker budget and preferences despite this information are not available in general in a real context. Moreover, the results of these approaches are able to highlight the most critical node in a network but not provide a metric capable of quantifying the degree of criticality for each node of the infrastructure. In more details, the approach presented in [7] proposes a method, able to identify the most critical nodes, based on the result of an optimization problem characterized by the presence of assumptions about the strategy of an attacker in terms of available budget and dimension of disconnected components. Similar assumptions are considered also in the approach presented in [8, 9], the authors propose a method which aims at minimizing the attack cost against the infrastructure with constraints about the features of the network. Finally, assumptions about the attacker preferences are also required in the formulation presented in [10]. In general, centrality measures, such as the node degree or betweenness centrality are often adopted as criticality measures, while in [11] the authors propose a critical index for the elements of a CI by analyzing the solutions of a multi objective optimization problem without any assumption about the attacker behaviour. However, the adoption of a unique metric or indicator about the criticality rate of each node of the system is quite unrealistic due to the complex nature of the infrastructures. Two approaches able to consider multiple metrics with the aim to compute a final aggregated criticality holistic indicator are presented in [12, 13]. The proposed approaches take into account multiple indicators based on multiple data source (topology data, field-related data, expert evaluations, etc.) but not provide a final step necessary to define a defensive strategy and evaluate its effectiveness.

1.2 Contribution and outline of the chapter

In this chapter we want to propose a procedure able to define a defensive strategy for CIs based on multiple node criticality measures. In more details, the procedure is based on three steps, as depicted in **Figure 1**: In the first stage (Section 2) we provide some specific criticality measure for CIs based on the connectivity of the system. The identification of the criticality measures is a fundamental stage in

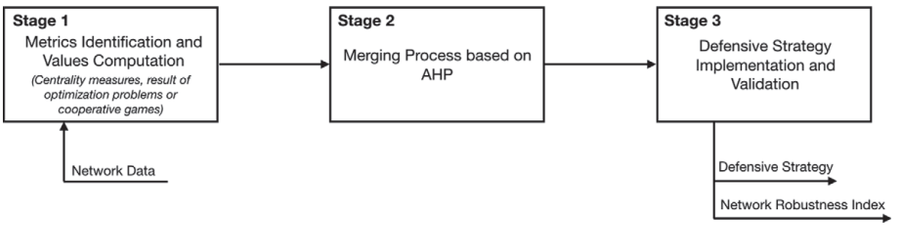

Figure 1.
Flow chart of the proposed three-steps procedure.

the defensive strategy definition process. In literature, graph centrality measures are often adopted as criticality measures for infrastructure but these approaches (e.g. Node degree or node betweenness) are quite ineffective as proved in [11]. In the second stage (Section 3) a methodology to merge multiple criticality metrics, based on the well-known Analytic Hierarchy Process [14], is described in order to overcome the limit about the application of a single metric in a complex environment. Moreover, such methodology allows considering also the criticality evaluations given for a subset of infrastructure nodes. The definition of the defensive strategy is provided in the last step (Section 4) and its effectiveness is proved by analyzing the global robustness of the network with respect to multiple robustness evaluation methods. Finally, in (Section 5), the application of the three-step procedure is illustrated with respect to the case study network with the aim of proving the effectiveness of the proposed strategy.

1.3 Notation

Let us denote by $|X|$ the cardinality of a set X; moreover, we represent 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, while by I_n we identify the $n \times n$ identity matrix. Finally, we denote the sign of $x \in \mathbb{R}$ by $sign(x)$ and by $sign(X)$ the entry-wise sign of a matrix X. Let $G = \{V, E\}$ denote a *graph* with a finite number n of nodes $v_i \in V$ and e edges $(v_i, v_j) \in E \subseteq V \times V$, from node v_i to node v_j. A graph is said to be *undirected* if $(v_i, v_j) \in E$ whenever $(v_j, v_i) \in E$ (see **Figure 2**). 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. A *path* over an undirected graph $G = \{V, E\}$, starting at a node $v_i \in V$ and ending at a node

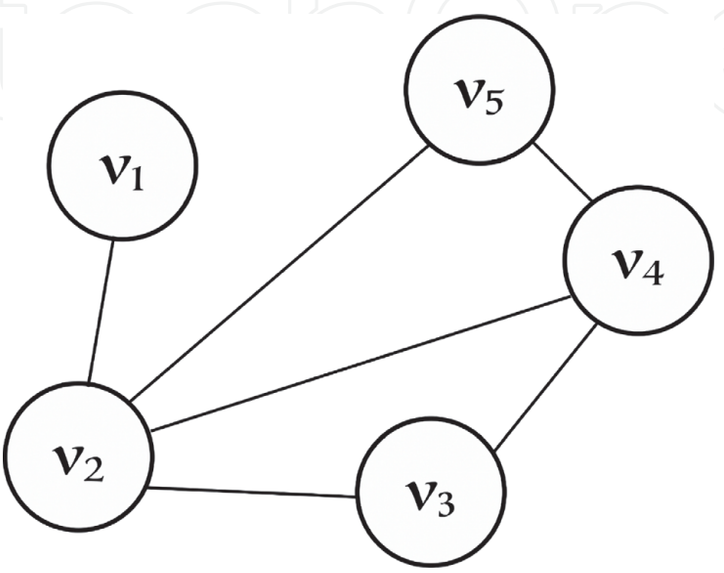

Figure 2.
Example of a graph $G = \{V, E\}$ with $|n| = 5$ nodes and $|E| = 6$ edges.

$v_j \in V$, is a subset of links in E that connects v_i and v_j without creating loops. An undirected graph $G = \{V, E\}$ is *connected* if each node can be reached by each other node by means of the links in E.

For the sake of clarity, we report here the notation adopted in the rest of the chapter.

c_i	Removal cost for node v_i
$PWC(G)$	Pairwise connectivity of G
$NPWC(A, x)$	Normalized pairwise connectivity for a graph with adjacency matrix A and without considering nodes v_i s.t.$\mathbf{x}_i = 0$
$\mathcal{P}$	Pareto Front
χ_i	Critical index for node v_i
P	Set of players in the cooperative game
$\Gamma(P, g)$	Cooperative game for players in P evaluated via characteristic function g
ϕ_i	Shapley value for player i
M_i	i-th metric
m	Number of metrics
$r_a^{(i)}/r_b^{(i)}$	Relative utility ratio among alternatives i and j according to metric i
R_{ab}^i	Matrix of utility ratios among alternatives a and b according to metric i
B	Defensive budget
w_i	Relevance of metric i
$\prod$	Global robustness index

2. Node criticality metrics based on network connectivity

As mentioned above the first step of the proposed approach for the identification of a defensive strategy is the identification of metrics of interests able to evaluate the network criticalities from multiple points of view. Despite in literature this process is often reduced to a simple centrality measure computation, in this section we propose two other applicable approaches, based on the infrastructure connectivity, to compute the criticality of each sub-systems of a CI. For the sake of clarity, in this context we represent the entire infrastructure via undirected graph $G = \{V, E\}$ where V is the set of n nodes v_i, (each node represents a sub-system of the CI) and $E \subseteq V \times V$ is the set of e undirected edges (v_i, v_j). An edge connects two nodes if a real physical connection exists between the two corresponding sub-systems.

Both the approaches for the critical node identification, presented in this section are based on the concept of connectivity. In our models, when a node is attacked and is unable to operate, we remove the node and the incident edges from the graph. The deletion of particular critical nodes could compromise the connectivity of the other elements of the network. Notice that, for each node v_i we consider a removal cost $c_i > 0$. With the aim to measure the degree of connectivity of the graph G, we adopt the Pairwise Connectivity (PWC), it is an index that captures the overall degree of connectivity of a graph on the basis of the couples of nodes connected by means of edges in G.

$$PWC(G) = \sum_{(v_i, v_j) \in V \times V, v_i \neq v_j} p(v_i, v_j), \tag{1}$$

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. Noting that the maximum number of couples of nodes in a graph with n nodes is $\frac{n(n-1)}{2}$, the *normalized pairwise connectivity* (NPWC) is defined as:

$$NPWC(G) = \frac{2PWC(G)}{n(n-1)} \in [0,1]. \tag{2}$$

Remark 1 $NPWC(G)$ is a measure of connectivity of the graph G, in fact, it is easy to note that

$$G \text{ connected} \Leftrightarrow NPWC(G) = 1. \tag{3}$$

When $NPWC(G) < 1$, the graph is not connected, but the larger $NPWC(G)$ is, the more G is "close" to be a connected graph. □

We now provide a more descriptive definition of a NPWC by taking into account a subset of attacked nodes. Let A be the adjacency matrix of an undirected graph $G = \{V, E\}$ and let $\mathbf{x} \in \mathbb{R}^n$ be a column vector whose entries $x_i = 0$ if the i-th node has been removed due to an attack or a fault and $x_i = 1$ otherwise, we define the connectivity as:

$$NPWC(A, \mathbf{x}) = \frac{\mathbf{1}_n^T \left[sign\left(\sum_{i=0}^{n-1} \hat{A}^i \right) - I_n \right] \mathbf{1}_n}{n(n-1)} \tag{4}$$

where $\hat{A}_{ij} = A_{ij} x_i x_j$, $\mathbf{1}_n$ is a column vector composed by n entries equal to 1.

2.1 A critical index based on optimization problem

The definition of the Critical Index χ_i for a node v_i, come directly from the solutions of a multi-objective problem defined by assuming the point of view of a malicious attacker.

In Eq. (5) the behavior of an attacker is defined as a multi-objective optimization problem characterized by two conflicting objectives: the reduction of the connectivity in terms of NPWC and the simultaneous minimization of the required attack effort in terms of removal cost. We reiterate that if an attacker want to disconnect a node v_i from the graph then (s)he must pay a cost c_i.

Problem 1

$$\begin{aligned} \min_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x}) = \quad & \min \left[f_1(\mathbf{x}), f_2(x) \right]^T, \end{aligned} \tag{5}$$

where $\mathbf{x}$ represents the vector of decision variables, whose entries x_i are equal to 0 if the node v_i is involved in the attack, 1 otherwise and where

$$f_1 = NPWC(A, \mathbf{x}) \tag{6}$$

and

$$f_2 = \frac{\mathbf{c}^T (\mathbf{1}_n - \mathbf{x})}{\mathbf{1}^T \mathbf{c}} \tag{7}$$

where $\mathbf{c} = [c_1 \dots c_n]^T$ is the vector whose entries represent the cost necessary to remove each node from the graph.

As described in [11], in general, a multi-objective problem is characterized by the presence of multiple optimal solutions $\mathbf{x}^{(j)}$ collected in the Pareto front set $\mathcal{P}$. Each solution is associated to a couple of values $\left[f_1(\mathbf{x}^{(j)}), f_2(\mathbf{x}^{(j)}) \right]$ according to the two objective functions. In other words, each optimal solution $\mathbf{x}^{(j)}$ represents a different attack strategy with damages caused on the network $f_1(\mathbf{x}^{(j)})$ and different attack effort $f_2(\mathbf{x}^{(j)})$ as depicted in **Figure 3**.

In [11], the Critical Index χ_i is defined as in Eq. (8):

$$\chi_i = \frac{\sum_{\forall \mathbf{x}^{(j)} \in \mathcal{P}} \mathbf{x}_i^{(j)}}{|\mathcal{P}|} \tag{8}$$

where $|\mathcal{P}|$ represents the number of solutions in the Pareto front. In other words it is defined as the ratio between the frequency with which a node v_i is involved in the attacks listed in the Pareto front and its cardinality. If the critical index χ_i is close to 0 this implies that the node is rarely involved in attack plans, instead, the closer it is to 1, more frequently the node is involved in optimal attack strategies.

2.2 A critical index based on a cooperative game

An alternative approach for the identification of the most critical nodes in a network is presented in [15]. Analogously to the critical index based on the results of the multi-objective optimization problem, the proposed method is based on the concept of NPWC. Differently from the previous critical index, this measure come from the game theory and is based on the solution of a cooperative game.

A cooperative game, sometimes called a value game or a profit game, is a competition among groups of players. Formally, a cooperative game is defined by a set of players P and a characteristic function $v : 2^N \Rightarrow \mathbb{R}^+$ which associate to all possible coalitions of players a utility rate. The function describes how much collective payoff a set of players can gain by forming a coalition.

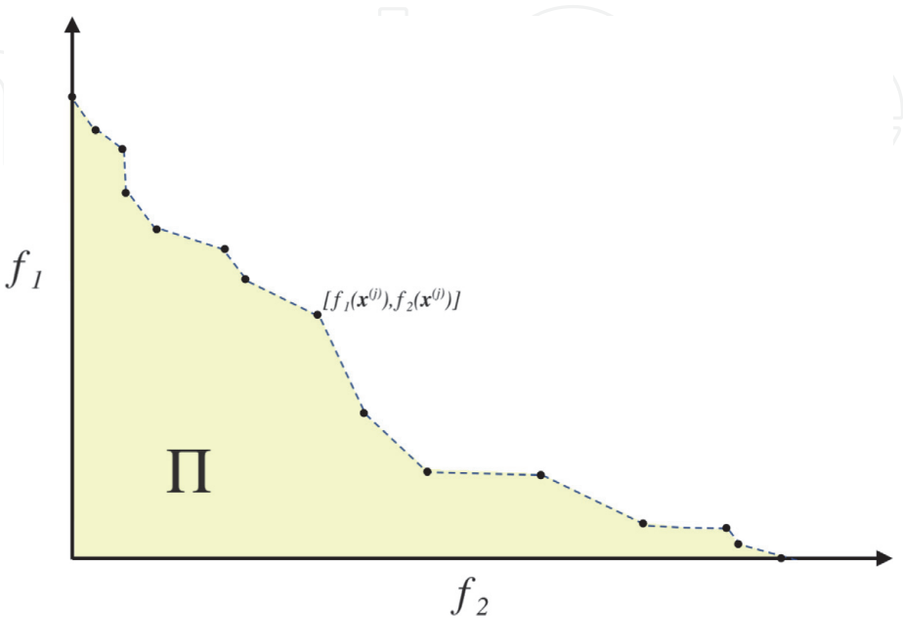

Figure 3.
Pareto front: the optimal solutions set for multi-objective optimization problem.

Let P be the set of players, and $g : 2^P \Rightarrow \mathbb{R}^+$ a function that satisfies the following properties:

- $g(\varnothing) = 0$
- Superadditive property: if $S, T \in 2^P \ \ s.t. \ \ S \cap T = \varnothing,$ then $v(S \cup T) \geq g(S) + g(T)$

The cooperative game $\Gamma(P,g)$ is defined by the couple (P,g) where the elements of P are the players of the game and the characteristic function of the game $g(S)$ estimates the utility of each coalition $S \in 2^P$.

Cooperative games can be solved via multiple approaches, the Shapley value [16] is one of the possible concepts of solution. The Shapley value assigns to each player $i \in P$, a reward ϕ_i. The larger is the contribution given by i in all the possible coalitions of players, based on the function g, the larger is the reward ϕ_i for the player i.

The Shapley value is a column vector Φ whose entries are ϕ_i are defined according to Eq. (9).

$$\phi_i = \frac{1}{n!} \sum_{S \subseteq P\{i\}} |S|!(n-|S|-1)!(g(S \cup \{i\}) - g(S)) \tag{9}$$

With the aim to adopt these concepts to provide a critical index able to quantify the criticality of each node of the network, a cooperative game $\Gamma(N, nPWC)$ is defined. The set of players is represented by the set of nodes N while the characteristic function g is $NPWC$ (Eq. (3)). Notice that, in [15], it is demonstrated that the NPWC satisfy the two fundamental properties of a characteristic function.

The solution of the proposed game will assign a reward to each node in V proportional to its contribution to the connectivity expressed in terms of $NPWC$, hence the Shapley value can be considered a valid node criticality metric.

3. A multi-criteria vulnerability detection index

As briefly introduced in Section 1, a research of the most critical nodes based on a single metric is practically worthless and extremely simplistic. In this section we propose an approach able to provide a holistic indicator able to take into account multiple criticality evaluations based on multiple metrics also in presence of incomplete data. The proposed method is based on the well-known Analytic Hierarchy Process (AHP) introduced by Saaty [17]. For a given set of m alternatives, relative utility ratios r_i/r_j are defined by experts. Such a setting is typical in contexts involving human decision-makers, which are usually more comfortable providing relative comparisons among the utilities of the different alternatives (e.g., "Alternative i is twice better than alternative j"), rather than directly assessing an absolute utility value of each alternative (i..e, "The value of alternative i is ..."). The AHP is a procedure able to estimate the absolute utilities r_i starting from the given utility ratios r_i/r_j. See [17] for additional notions about the AHP.

We now suppose to have m different metrics $M_1 \ldots M_m$. According to these metrics, the entries of the column vectors $\mathbf{r}^{(1)} \ldots \mathbf{r}^{(m)}$ represents the criticality rate of each node of the graph. Notice that the method is applicable also if for some metrics the criticality ratio of some node is not available [12]. Finally, let $w_1 \ldots w_m$ be positive weights defined by subject-matter experts (SMEs) representing the relevance of each metric. The larger is the weight associated to the i-th metric, the larger the influence of such metric in the final holistic indicator. Such weights can

be obtained also resolving AHP on the basis of pair-wise comparisons between the different metrics.

For each metric we define the $n \times n$ matrix $R^{(i)}$ whose entries are defined as follows:

$$R_{ab}^{(i)} = \begin{cases} r_a^{(i)}/r_b^{(i)} \text{if both} r_a^{(i)} \text{and} r_b^{(i)} \text{are defined} \\ 0 \; otherwise \end{cases} \tag{10}$$

In other words, the matrix $R^{(i)}$ collects the relative utility ratios between the a-th and b-th nodes according to the i-th metric if both the evaluation are available. Notice that some ratio $r_a^{(i)}/r_b^{(i)}$ might be undefined if $r_b^{(i)} = 0$, due to this reason, we treat zero-valued entries as not available data.

By considering the matrices $R^{(i)}$, we aim at finding the aggregated holistic indicator $\mathbf{r}^* \in \mathbb{R}^n$ that solves the following problem.

Problem 2 Find $\mathbf{r}^* \in \mathbb{R}^n$ *that solves*

$$\mathbf{r}^* = \underset{\mathbf{r} \in \mathbb{R}_+^n}{\arg\min} f(\mathbf{r}) = \sum_{i=1}^{m} w_i \sum_{a=1}^{n} \sum_{b \,|\, R_{ab}^{(i)} \neq 0} \left(\ln\left(R_{ab}^{(i)}\right) - log\,(r_a) + log\,(r_b) \right)^2 \tag{11}$$

The holistic indicator $\mathbf{r}^*$ is a new node criticality measure that represents a compromise between the m initial metrics $M_1 \ldots M_m$ by taking into account the SMEs preferences w_i. In other words, Problem 2 aims at finding the criticality indicator $\mathbf{r}_a^*$, assigned to the a-th node, such that the ratios $\mathbf{r}_a^*/\mathbf{r}_b^*$ minimize the deviation from the ratios $R^{(i)}$ for the m considered metrics.

4. Defensive strategy definition and evaluation

In this section we propose a methodology to define a defensive strategy able to improve the survivability of the network with a focus on the connectivity maintenance with respect to nodes deletion. As introduced in Section 2, an attack cost c_i is associated to each node v_i. Our aim is the definition of a new distribution of the budget in order to minimize the loss of connectivity in case of malicious attacks.

Let $B = \sum_{i=1}^{n} c_i$ the defensive budget computed on the basis of the initial removal costs. We propose a new allocation of the budget by defining the removal cost proportionally to the holistic indicator $\mathbf{r}^*$ described in Section 3. Hence, we define the new removal costs $\hat{c}_i$ as follows:

$$\hat{c}_i = \frac{1}{B} \frac{\mathbf{r}^*{}_i}{\mathbf{1_n}^T \mathbf{r}^*}. \tag{12}$$

It is now necessary evaluate the robustness of a network with a particular defensive strategy. As introduced in Section 2.1, due to its multi-objective nature, Problem 1 is characterized by the presence of multiple optimal solutions collected in the Pareto front $\mathcal{P}$. Each optimal solution $\mathbf{x}^{(j)}$ is associated to a couple of values: a particular connectivity value $f_1(\mathbf{x}^{(j)})$ and an attack cost $f_2(\mathbf{x}^{(j)})$, where f_1 and f_2 represent the two objective function of Problem 1.

In [11], the global robustness index $\prod$ is defined as the area under the polygonal chain connecting the points $(f_1(\mathbf{x}^{(j)}), f_2(\mathbf{x}^{(j)}))$ in the Pareto front using trapezoidal rule for numerical integration.

As depicted in **Figure 3**, $\prod$ is a measure of the overall robustness of the network. In fact, the larger is the 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 for large effort.

5. Case study

In this section we prove the effectiveness of the proposed three-stage methodology able to improve the network survivability via critical nodes protection. The proposed strategy is tested on the CI represented by the network depicted in **Figure 4**. Notice that the case study is based on a network that does not represents a real infrastructure. The network is composed by $n = 15$ nodes and $e = 35$ edges. As discussed in Section 2, the first step of the methodology is devoted to the identification of criticality measures able to take into account the effects about the disconnection of a node from the graph by evaluating the loss of connectivity of the entire infrastructure. Notice that, the removal costs c_i are set to 1 for each node of the infrastructure.

The first columns in **Table 1** collect the metrics defined by Eqs. 5 and 6 respectively. Concerning the distribution of the critical indices χ_i, the largest value are associated to the nodes 10 and 3. Notice that, the deletion of such nodes divides the nodes in two partitions, hence it strongly compromises the connectivity of the network in terms of nPWC.

Similar results are obtained by considering the computation of the Shapley value in order to solve the cooperative game as described in Section 2.2. We remark that this approach assigns a reward to each node of the network according to their contribution to the connectivity of the entire network by considering all the possible partitions of nodes. Notice that, the results computed via Shapley not consider the removal cost c_i while the results of Problem 1 take into account also this aspect, moreover, in this case study all the removal costs c_i are set to 1.

Finally, the fourth and fifth columns of **Table 1** collect the node degree and the betweenness centrality [18] for each node in the graph.

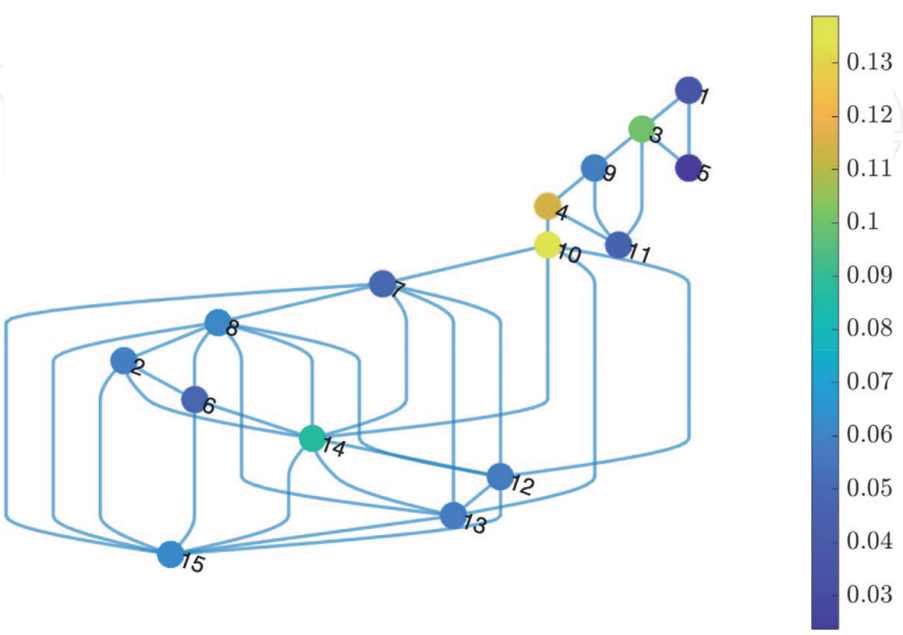

Figure 4.
Case study network. The node color depends on the holistic criticality rate computed via Eq. (7).

Node	Critical Index χ_i [a]	Shapley Value ϕ_i [b]	Degree	Betweenness	Holistic Indicator r_i^* [c]
1	0.1111	0.0354	2	0	0.0360
2	0.1852	0.0493	4	0	0.0587
3	0.2863	0.0952	4	24	0.1003
4	0.2593	0.1465	3	45	0.1143
5	0.0370	0.0354	2	0	0.0238
6	0.1111	0.0493	4	0	0.0484
7	0.1111	0.0521	6	3.5	0.0491
8	0.2593	0.0547	7	2	0.0618
9	0.1481	0.0515	3	15	0.0580
10	0.2963	0.1635	5	48	0.1389
11	0.0741	0.0515	3	15	0.0465
12	0.1852	0.0521	6	3.5	0.0577
13	0.1852	0.0521	6	3.5	0.0577
14	0.2222	0.0567	8	19.5	0.0871
15	0.2593	0.0547	7	2	0.0618

[a] *Criticality measure based on Eq. (5).*
[b] *Criticality measure based on Eq. (6).*
[c] *Holistic Indicator based on Eq. (7).*

Table 1.
Criticality evaluations based on four different metrics and computed holistic indicator.

In the last column of **Table 1**, we show the criticality rate for each node according to the new holistic indicator computed as in Eq. (7) considering m=4 metrics (i.e. the critical index, the Shapley Value, the node Degree and the Betweenness centrality). According to the procedure defined in Section 3, we have set the metric relevance as follows: $w_1 = 0.3$, $w_2 = 0.3$, $w_3 = 0.2$, and $w_4 = 0.2$ in order to emphasize the criticality metrics based on the concept of PWC.

The nodes color in **Figure 4** depends on the aggregated criticality values, according to the colormap. On the basis of this new indicator, the node 10 is the most critical node of the graph, in fact the deletion of this node strongly compromise the connectivity of the network and the creation of two disconnected partitions. Due to the same reason, a high criticality rate is also assigned to the nodes 4 and 3. Despite the node 14 is not essential for the connectivity, this node is characterized by a high node degree, in fact it is considered, according to the holistic indicator, as the fourth most critical node in the network.

Starting from the results obtained by computing the holistic indicator $\mathbf{r}^*$, we adopt a defensive strategy by defining a new attack cost $\hat{c}_i$, for each node, proportional to its holistic criticality rate as defined in Eq. (8). Notice that the defensive budget $B = \sum_{i=1}^{n} c_i = 15$.

The effectiveness of the proposed defensive strategy is proved by considering the global robustness index $\prod$, we remark that it came from the solution of Problem 1 and it is defined as the area under the Pareto front. As depicted in **Figure 5**, the new allocation of the defensive budget B is very effective to contrast an attacker especially with limited budget. In more details, in case of uniform defensive strategy (i.e. all the attack costs set to 1) the area under the Pareto front is equal to $\prod = 0.1229$, while the new budget allocation (Eq. (8)) based on the holistic indicator $\mathbf{r}^*$ improves the network robustness by increasing the area to $\prod = 0.1591$.

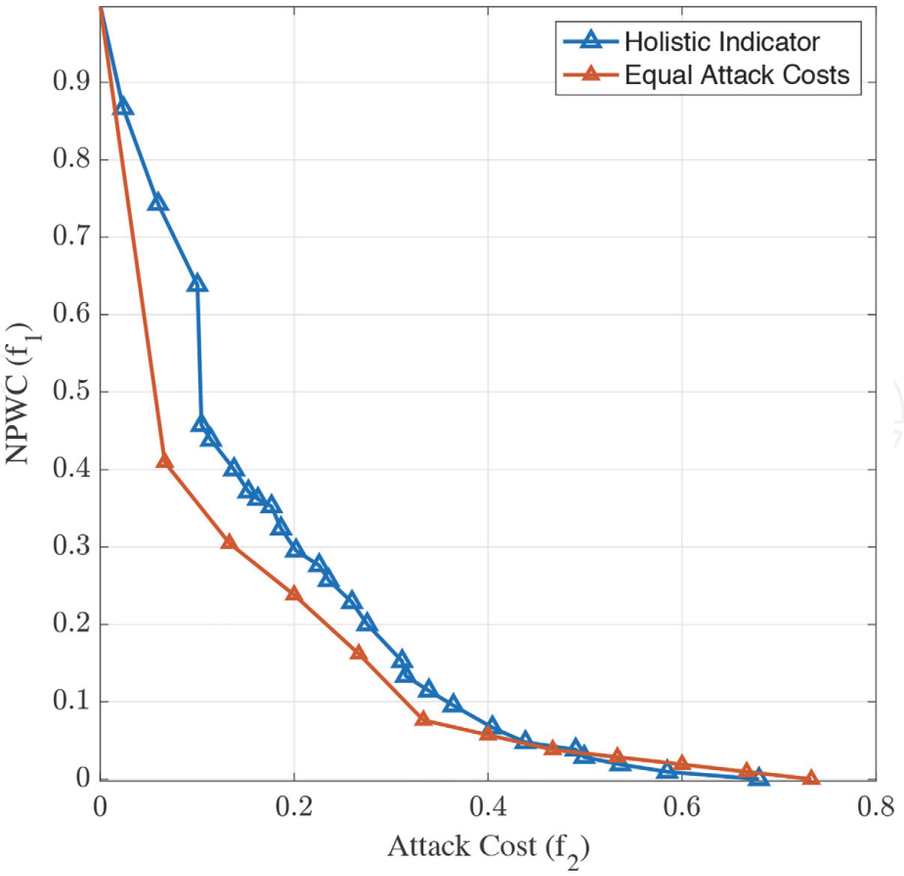

Figure 5.
Results of problem 1. Pareto fronts obtained by applying defensive strategies based on the holistic indicator (blue line), and uniform attack costs (red line).

6. Conclusions

In this chapter we provide a methodology for the definition of a defensive strategy via prioritizing the critical nodes of the network. Due to the complexity of a CI, the adoption of a unique metric for the identification of the node criticality is simplistic, to this end we propose a strategy, based on the AHP, able to merge multiple metrics which take into different aspects of the network. Moreover, the proposed aggregation procedure is applicable also in case of incomplete data. Among the multiple metrics applicable in the merging process, in this chapter we propose two metrics characterized by a focus on the network connectivity. In the one hand the critical index is computed on the basis of a multi objective optimization problem. Assuming an attacker perspective and knowing the topology of the network, the problems aims at identifying the nodes whose removal compromise the connectivity of the entire system. On the other hand, we propose the adoption of the Shapley value as a criticality evaluation by defining a cooperative game among the nodes of the network. Finally, we propose the definition of a defensive strategy that assigns to each node a removal cost proportional to the holistic indicator. Future improvement will be devoted to the inclusion of a final check able to include a final validation based on expert opinions. One of the possible validity check is based on the well-known face validity approach [19], it refers to the transparency or relevance of a test as it appears to test participants.

Acknowledgements

This work was supported by INAIL via the European Saf€ra project "Integrated Management of Safety and Security Synergies in Seveso Plants" (Saf€ra 4STER).

IntechOpen

Author details

Luca Faramondi[1*], Giacomo Assenza[1], Gabriele Oliva[1], Ernesto Del Prete[2], Fabio Pera[2] and Roberto Setola[1]

1 Unit of Automatic Control, Department of Engineering, Università Campus Bio-Medico di Roma, Rome, Italy

2 National Institute for Insurance against Accidents at Work, Italy

*Address all correspondence to: l.faramondi@unicampus.it

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Corsi, S., & Sabelli, C. (2004, June). General blackout in italy sunday september 28, 2003, h. 03: 28: 00. In IEEE Power Engineering Society General Meeting, 2004. (pp. 1691–1702). IEEE.

[2] Comfort, L. K., & Haase, T. W. (2006). Communication, coherence, and collective action: The impact of Hurricane Katrina on communications infrastructure. Public Works management & policy, 10(4), 328–343.

[3] Norio, O., Ye, T., Kajitani, Y., Shi, P., & Tatano, H. (2011). The 2011 eastern Japan great earthquake disaster: Overview and comments. International Journal of Disaster Risk Science, 2(1), 34–42.

[4] Weiss, J. (2016). Aurora generator test. Handbook of SCADA/Control Systems Security, 107.

[5] Assenza, G., Faramondi, L., Oliva, G., & Setola, R. (2020). Cyber threats for operational technologies. International Journal of System of Systems Engineering, 10(2), 128–142.

[6] Arulselvan, A., Commander, C. W., Elefteriadou, L., & Pardalos, P. M. (2009). Detecting critical nodes in sparse graphs. Computers & Operations Research, 36(7), 2193–2200.

[7] Arulselvan, A., Commander, C. W., Shylo, O., & Pardalos, P. M. (2011). Cardinality-constrained critical node detection problem. In Performance models and risk management in communications systems (pp. 79–91). Springer, New York, NY.

[8] Dinh, T. N., Xuan, Y., Thai, M. T., Park, E. K., & Znati, T. (2010, March). On approximation of new optimization methods for assessing network vulnerability. In 2010 Proceedings IEEE INFOCOM (pp. 1–9). IEEE.

[9] Faramondi, L., Oliva, G., Pascucci, F., Panzieri, S., & Setola, R. (2016, June). Critical node detection based on attacker preferences. In 2016 24th Mediterranean Conference on Control and Automation (MED) (pp. 773–778). IEEE.

[10] Faramondi, L., Setola, R., Panzieri, S., Pascucci, F., & Oliva, G. (2018). Finding critical nodes in infrastructure networks. International Journal of Critical Infrastructure Protection, 20, 3–15.

[11] Faramondi, L., Oliva, G., Panzieri, S., Pascucci, F., Schlueter, M., Munetomo, M., & Setola, R. (2018). Network structural vulnerability: a multiobjective attacker perspective. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(10), 2036–2049.

[12] Faramondi, L., Oliva, G., & Setola, R. (2020). Multi-criteria node criticality assessment framework for critical infrastructure networks. International Journal of Critical Infrastructure Protection, 28, 100338.

[13] Oliva, G., Amideo, A. E., Starita, S., Setola, R., & Scaparra, M. P. (2019, September). Aggregating Centrality Rankings: A Novel Approach to Detect Critical Infrastructure Vulnerabilities. In International Conference on Critical Information Infrastructures Security (pp. 57–68). Springer, Cham.

[14] Saaty, T. L. (2008). Decision making with the analytic hierarchy process. International journal of services sciences, 1(1), 83–98.

[15] Faramondi, L., Oliva, G., & Setola, R. (2019, October). Network Defensive Strategy Definition Based on Node Criticality. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 439–444). IEEE.

[16] Shapley, L. S., & Roth, A. E. (Eds.). (1988). "The Shapley value: essays in honor of Lloyd S. Shapley." *Cambridge University Press*.

[17] Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. Journal of mathematical psychology, 15 (3), 234–281.

[18] Biggs, N., Biggs, N. L., & Norman, B. (1993). Algebraic graph theory (Vol. 67). Cambridge university press.

[19] Nevo, B. (1985). Face validity revisited. Journal of Educational Measurement, 22(4), 287–293.

IntechOpen