Maximizing SDN resilience to node-targeted attacks through joint optimization of the primary and backup controllers placements

Michał Pióro[1] | **Mariusz Mycek**[2] | **Artur Tomaszewski**[2] | **Amaro de Sousa**[3,4]

[1]Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk, Poland

[2]Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland

[3]Instituto de Telecomunicações, Aveiro, Portugal

[4]Universidade de Aveiro – DETI, Aveiro, Portugal

Correspondence
Michał Pióro, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk, Poland
Email: michal.pioro@pw.edu.pl

Funding information
POB Research Centre Cybersecurity and Data Science of Warsaw University of Technology within the Excellence Initiative Program – Research University (ID-UB), Poland.
FCT/MCTES, Portugal, through National Funds and when applicable co-funded by EU funds under the Project UIDB/50008/2020-UIDP/50008/2020.

In Software Defined Networks (SDN) packet data switches are configured by a limited number of SDN controllers, which respond to queries for packet forwarding decisions from the switches. To enable optimal control of switches in real time the placement of controllers at network nodes must guarantee that the controller-to-controller and switch-to-controller communications delays are bounded. Apart from the primary controllers that control the switches in the nominal state, separate backup controllers can be introduced that take over when the primary controllers are unavailable, and whose delay bounds are relaxed. In this paper we present optimization models to jointly optimize the placement of primary and backup controllers in long-distance SDN networks, aimed at maximizing the network's resilience to node-targeted attacks. Applying the models to two well-known network topologies and running a broad numerical study we show that, when compared with the standard approach of using only primary controllers, the use of backup controllers provides significant resilience gains, in particular in case of strict delay bounds.

KEYWORDS
SDN, controllers placement, node-targeted attacks, resilience, optimization

1 | INTRODUCTION

The Software Defined Network (SDN) concept is a key paradigm in the evolution of communications networks, introduced to provide increased network management flexibility and enhanced services' support [10]. The concept has been investigated and applied in different networking contexts such as wide area networks [2, 28], 5G networks [5], data center networks [7], smart grids [18], or industrial Internet of Things (IoT) networks [29].

In SDN, the control and data planes of the transport network are separated. While the data plane is composed of a large number of switches and their interconnecting links, the control plane consists of a limited number of controllers, which control packet forwarding decisions at the switches, and are thus necessary for their operation. Although the SDN control plane can be equipped with a single controller, in practice it is based on multiple controllers physically distributed across the network. Still, while a data switch is placed at every network node, there are usually only a limited number of nodes where controllers are actually deployed. The problem of deciding where to place the controllers, known as Controller Placement Problem (CPP), was originally introduced in [9].

Each switch is assigned one controller to interact with and query for routing decisions. A new traffic flow arriving at the switch triggers a query from the switch to the switch's controller, making the latter respond with a routing decision on how to forward the flow. The controller must also send the information on the routing decision it makes to all other controllers, thanks to which their information about the network state is constantly updated and consistent.

The communication between switches and controllers uses the data plane network. While each controller is connected to the data plane by being connected to the switch at the same network node (a node that contains both a switch and a controller is called a controller node), each switch is typically controlled by a controller that can be connected to the switch via the least communications delay data plane path, in particular by the controller located at the same network node as the switch. Then, on one hand, the maximum switch-to-controller (SC) communications delay (i.e., signalling message transfer time between the switch and its controller) must be bounded so that switches do not wait too long for routing decisions. And, on the other hand, the maximum controller-to-controller (CC) delay must also be bounded so that it does not take too long for the controllers to become aware of the current, updated network state. In long-distance SDN networks, delays between switches and their assigned controllers as well as delays between controllers can be significant, imposing constraints on the placement of the controllers. A trade-off in controller placement can be seen: placing more controllers makes meeting SC delay bounds easier, and meeting CC delay bounds more difficult.

It is well known that SDN has the potential to enhance network security as the centralization of the control plane facilitates maintaining a complete view of the network state, thus the identifying and resolving possible threats [1]. However, apart from the known implications of data plane programmability on network security [8], also the separation of the control and data planes poses security challenges as a switch can function properly only if it can communicate with at least one controller. This makes the SDN network vulnerable to attacks that disrupt communication between switches and controllers. While the control plane-related aspects of this communication can be effectively protected [15], protecting the communication in the data plane is more troublesome. First, attacks can cause data plane link disruptions by exploiting vulnerability of the optical network infrastructure to fibre cuts or insertion of harmful optical signals [26]. Second, attacks can cause data plane node disruptions as SDN switches are usually simple switching devices susceptible to remote intrusion and shutdown. Data plane node disruptions are more damaging than link disruptions since apart from the switch being shut down also all data plane links terminated at the switch cease to exist, and the controller at this particular network node becomes disconnected from the network and unavailable as well; as a result the entire network node of the switch becomes unavailable. Therefore, in this paper we consider attacks that make network nodes completely inaccessible, regardless of reason for this situation. We assume

that the attack targets a set of network nodes and refer to the considered class of attacks as (network) node-targeted attacks.

The controller is the primary controller of a given switch if it controls the switch in the nominal state of the network, i.e., when there are no network disruptions. When such a primary controller is not available, another controller must be assigned to the switch, which becomes the switch's backup controller (note that, depending on the network state, different backup controllers can be assigned to the switch depending on the state of the network). In general, for an SDN network to be resilient to node-targeted attacks, more controllers than the minimum number required to meet the SC and CC delay bounds should be used. However, when all controllers act as primary controllers for the closest switches, the resilience gains can be limited as all pairs of primary controllers must obey the CC delay bound. To overcome this disadvantage, backup controllers separate from primary controllers can be used [4]. In the event of an attack leading to network disruptions, backup controllers take over the functions of primary controllers for the switches that can no longer communicate with their primary controllers. Backup controllers do not participate in the routing decisions in the nominal network state and are expected to serve a limited number of switches in case of the attack. Therefore, they do not require significant computational resources, and furthermore, their placement does not have to meet the bounds on the CC delays (and, for that matter, the bounds on the SC delays): although in the nominal state, the backup controllers also maintain complete view of the network state, they do not act as primary controllers for any switch and do not make any routing decisions, so the time interval in which their view of the network must be updated can be mitigated. In a non-nominal state this may lead to slower network state updates, less accurate state information and sub-optimal routing decisions at the controllers, which however is considered acceptable in non-nominal network states.

In this paper, we present models for joint optimization of the primary and backup controllers placements, aimed at maximizing the resilience of the SDN network against a list of node-targeted attacks. We consider two alternative optimization models: a compact model and a non-compact one. The compact model is useful when the SDN operator imposes no additional constraints, other than delay constraints, on the placement of primary controllers, while the non-compact model is useful when the SDN operator considers a limited list of predefined primary controllers placements and needs to select one placement from the list. To express the resilience of a network to a single attack or to a set of node-targeted attacks, we introduce two network availability measures. The measures are defined using a notion of a metric of a subset of network nodes. In the paper we consider two simple metrics: (i) a linear metric expressing the number of nodes in the set, and (ii) a quadratic metric expressing the number of node pairs. For each metric, we define optimization models that maximize either the worst-case or the average network availability measure among the considered set of node-targeted attacks.

We apply the introduced optimization models to two well-known long-distance network topologies. We compare the results between the standard approach, i.e., using only primary controllers, and the new approach of using also backup controllers, demonstrating the resilience gains obtained with the new approach. We analyze how the resilience levels achieved with backup controllers depend on SC and CC delay bounds. Finally, we examine the impact of the size of the list of the node-targeted attacks on both the computational scalability of the optimization models and on the resilience level of the optimal network solutions.

The paper is organized as follows. Section 2 summarizes related work on SDN resilience to node-targeted attacks. Section 3 describes the basic concepts behind our approach. Section 4 presents the developed optimization models for the combined primary and backup controller placement problem. Additional formulations of the problems needed to obtain numerical results are provided in Appendix A. Section 5 presents a summary of a numerical study of two selected network instances, based on the introduced models. A detailed description and discussion of the numerical results obtained for both networks is presented in Appendix B. Final remarks are given in Section 6.

Finally, we note that the material presented in this paper is a far-reaching extension of the research ideas discussed in our conference papers [13] and [17]. In the current paper we extend, improve and compare the optimization models introduced therein, and thoroughly examine both the problem and the models by means of a broad, comprehensive numerical study.

2 | RELATED WORK

Most of the works dealing with the problem of SDN network resilience against node-targeted attacks assume that the attacker has full knowledge of the topology of the data plane network, but not about the actual location of the controllers, and knowingly selects the attacked nodes (and in this way constructing a node-targeted attack) so as to achieve the most damaging effect on the network graph connectivity; such attacks are also called topological attacks or critical targeted attacks, see [4]. Recently, [23] presented an assessment of the resilience of long-distance SDN networks to node-targeted attacks. The paper compares the resilience of different controllers placement solutions to node-targeted attacks and to node attacks of non-targeted nature (in particular, random attacks), and one of the findings of this research is that node-targeted attacks are much more damaging. It is also worth noting that some work has recently been on SDN resilience to link disruption, such as [12] and [30], which deal with the problem of optimizing controllers placements that are resilient to k-link failures (the so called k-RCP problem) and, more generally, to both single-link and multiple-link failures.

A controllers placement algorithm that improves SDN resilience against node-targeted attacks is proposed in [19]. For a given data plane network, first, the most damaging attack is computed, and then, based on the required number of controllers and the type of the most damaging attack, the subset of least vulnerable network nodes is selected as the best controllers placement. Two methods of defining the most damaging attack are considered — simultaneous and sequential, each with two node centrality metrics (node degree and node betweenness). For simultaneous method, the metric values are calculated for all nodes in the network graph once and the nodes with the highest metric values are selected. For sequential method, the nodes to be attacked are selected one by one — each time the metric values are computed for all nodes in the current network graph and the node with the highest metric value is selected (and deleted from the graph). The proposed approach is applicable to small SDN networks but it cannot be used for long-distance networks as, in general, the identified set of least vulnerable network nodes might contain no subset defining the controllers placement that respects the required SC and CC delay bounds.

To maximize the resilience of the SDN network to node-targeted attacks, in [21, 22, 20] the controllers placement is required not only to meet given SC and CC delay bounds but also to guarantee a so called placement robustness property, which ensures that the shutdown of all but one controller node still enables each of the surviving switches to connect to one of the surviving controllers. The solution approach which is common to those works is based on two steps: first, all controllers placements compliant with the above constraints are enumerated; then, the resilience of each placement is evaluated for different node-targeted attacks (corresponding to different strategies of the attacker), and the best placement is selected. The resilience evaluation of controllers placements differs among the works. In [21, 22], potential placements are evaluated based on the number of surviving switches that can connect to surviving controllers, and three most damaging attacks are defined using the sequential strategy but a different node centrality metric (degree, closeness and betweenness). In [20], potential placements are evaluated by the number of surviving pairs of switches that can connect to a common surviving controller (representing the number of switch pairs still able to offer service), and apart from the three most damaging attacks described above, a fourth one is also considered, where the targeted nodes are the critical nodes of the data plane network graph.

When dealing with node-targeted attacks, all of the work mentioned above assume that the attacker is not aware of the placement of the controllers and thus their placement has no influence on the choice of nodes to attack. (As far as we know, only paper [16] considers the more general case, namely that when selecting targeted nodes, the attacker takes into account not only the network topology, but also probabilistically predicts the set of network nodes chosen by the network operator to place controllers.) Therefore, we developed the concept of defining the controllers placement and the node-targeted attack in terms of a game involving the network operator and the network attacker. We also formalized the notion of the SDN network resilience to node-targeted attacks by introducing a set of probabilistic network availability measures and associated network metrics, considering in particular linear and quadratic metrics to express, respectively, the number of switches and pairs of switches that can access the controller. We defined an optimization model that determines potentially most dangerous node-targeted attacks the attacker might launch, and an optimization model that determines the best placement of controllers that maximizes the availability of network services with respect to that set of attacks.

Then, in [27] we formulated a pair of symmetric problems of finding the most dangerous node-targeted attack and the best controller placement, defining them in terms of the min-max and max-min optimization, and proposed iterative optimization algorithms of solving the problems based on generation of, respectively, best placements and most dangerous attacks. However, focusing on the effect the attacks have on data plane network connectivity by partitioning the network into a set of connected components, we did not consider the aspect of the communications delays between switches and controllers or between controllers. And we did not introduce the distinction between primary and backup controllers either.

As far as we know, our conference paper [13] is the first work dealing with joint optimization of primary and backup controllers placements. For that purpose, an optimization model that maximizes network resilience against a given list of node-targeted attacks is proposed. The optimization model is non-compact as it considers a predefined list of allowable primary controllers placements. Then, in [17] we provided an alternative compact optimization model, which appeared much more efficient in cases when standard constraints (like delay bounds) on primary controllers placements are considered. Both models were applied to a medium size network instance showing that the SDN network resilience to node-targeted attacks can be significantly improved with only a few backup controllers.

The use of backup controllers to improve SDN resilience against node-targeted attacks was also addressed in [6, 3, 4]. However, these works assume that the placement of primary controllers is given (for example the placement actually deployed in the network or determined by the SDN network operator according to some preferences), and investigate the problem of adding a number of backup controllers in order to increase network resilience against a given predefined list of node-targeted attacks. The list is generated by means of various centrality metrics and also based on generating the above mentioned topological attacks. The resilience is measured with the number of surviving switches that can connect to a surviving controller, averaged over a set of generated attacks. In paper [4], the research from two previous papers [6, 3] is extended to provide more insight into optimization models — how they can be adapted to other resilience criteria, how different types of attacks affect SDN resilience, and how node-targeted attacks degrade communication delays when backup controllers have to be used.

3 | NETWORKS, CONTROLLERS PLACEMENTS, ATTACKS, AVAILABILITY MEASURES

The considered network is modeled by means of an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, with the set of *node locations* (called *locations* or *nodes* in short) $\mathcal{V}$, and the set of *links* $\mathcal{E} \subseteq \mathcal{V}^{|2|}$ interconnecting the locations. (The notation we use is

TABLE 1 Summary of general notation

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$	network graph
$\mathcal{V}$	set of (node) locations $(V := \lvert\mathcal{V}\rvert)$
$\mathcal{E}$	set of links interconnecting node locations $(E := \lvert\mathcal{E}\rvert)$
$\delta(v)$	set of links incident to node $v \in \mathcal{V}$ $(\delta(v) := \{\{v, w\} \in \mathcal{E} : w \in \mathcal{V} \setminus \{v\}\})$
$\mathcal{P}$	set (called also list) of primary controllers placements
$\mathcal{V}(p)$	set of primary controller locations of placement $p \in \mathcal{P}$ $(V(p) = \lvert\mathcal{V}(p)\rvert)$
BSC, BCC	upper bounds (limits) on the SC delay (SCD) and the CC delay (CCD), respectively
$d(v, w)$	the least path-delay among the paths between v and w
$d(\mathcal{G})$	diameter of the network graph with respect to $d(v, w)$ $(d(\mathcal{G}) := \max\{d(v, w) : v, w \in \mathcal{V}\})$
$\mathcal{W}(v)$	set of nodes w with $d(v, w) \leq BSC$ $(v \in \mathcal{V})$
$\mathcal{U}$	set of node-pairs $\{v, w\} \in \mathcal{V}^{\lvert 2\rvert}$ with $d(v, w) > BCC$
$\mathcal{B}$	set of backup controllers placements
$\mathcal{V}(b)$	set of backup controller locations of placement $b \in \mathcal{B}$ $(V(b) = \lvert\mathcal{V}(b)\rvert)$
$\mathcal{V}(p, b)$	joint set of controller locations for $p \in \mathcal{P}$, $b \in \mathcal{B}$, where $\mathcal{V}(p) \cap \mathcal{V}(b) = \varnothing$ $(V(p, b) = \lvert\mathcal{V}(p, b)\rvert)$
$\mathcal{A}$	set (called also list) of attacks
$w(a)$	weight of attack $a \in \mathcal{A}$
$\mathcal{V}(a)$	set of nodes affected by attack $a \in \mathcal{A}$ $(V(a) = \lvert\mathcal{V}(a)\rvert)$
$\mathcal{G}(a)$	graph surviving attack a
$\mathcal{C}(a)$	set (family) of components c resulting from attack $a \in \mathcal{A}$
$\mathcal{V}(c)$	set of nodes of component c $(V(c) := \lvert\mathcal{V}(c)\rvert)$
$Y(a, c)$	binary indicator equal to 1 if, and only if, component $c \in \mathcal{C}(a)$ contains a controller: $\mathcal{V}(c) \cap \mathcal{V}(p, b) \neq \varnothing$
$f(c)$	metric of component c $(f(c) = V(c)$ or $f(c) = \binom{V(c)}{2})$
$\mathcal{M}(a)$	network availability measure defined for attack a
$\mathcal{M}(\mathcal{A})$	network availability measure defined for set of attacks $\mathcal{A}$
$\mathcal{X}^{\lvert 2\rvert}$	set of all 2-element subsets of a given set $\mathcal{X}$
$\lvert\mathcal{X}\rvert$	number of elements in set $\mathcal{X}$
$:=$	equal by definition

summarized in Table 1 while the basic notions are illustrated in Figures 1-2). Each location $v \in \mathcal{V}$ contains a *data plane node* (*switch* in short) and optionally a *control plane node* (*controller* in short); the locations containing a controller will be called *controller locations*. The basic functionality of switches is to realize connections for data transmission, i.e., the transport-related function. In order to be able to perform this function, switches must have access to controllers — the devices necessary in the process of setting up the connections in question. For the switch in a given location $v \in \mathcal{V}$ such an access is provided by means of a path in graph $\mathcal{G}$ connecting v with one of the controller locations. (Note that the switch in a controller location has a direct access to the collocated controller.)

It is important that the set of controllers used in the nominal state of network operation (such controllers are called *primary controllers*) fulfil the requirements on the maximum *switch-to-controller delay* (SCD: for a given switch, SCD is equal to the lowest transmission delay observed among the paths connecting this switch to any of the primary controllers), and the maximum *controller-to-controller delay* (CCD: for a given pair of primary controllers, CCD is equal to the smallest transmission delay observed among the paths connecting their locations).

A particular assignment of primary controllers to node locations will be called *primary controllers placement* and denoted by p. Such a placement is *feasible* if it fulfils the SCD and CCD requirements described above. The set of feasible primary controllers placements will be denoted by $\mathcal{P}$. Note that this set may be further limited by additional requirements, such as the minimum and maximum number of controllers it consists of. The set of primary controllers locations of a given placement $p \in \mathcal{P}$ will be denoted by $\mathcal{V}(p)$ (where $\mathcal{V}(p) \subseteq \mathcal{V}$). An example of a 3-node primary controllers placement for the *cost266* network (which will be studied in the numerical section) is shown on the right side of Figure 1.

Let $d(v, w)$ denote the lowest transmission delay among the paths connecting a given pair of node locations $v, w \in \mathcal{V}$ (note that $d(v, v) := 0$), and let the assumed maximum values of SCD and CCD be denoted by BSC and BCC, respectively. Now we define the following sets

- $\mathcal{W}(v) := \{w \in \mathcal{V} : d(v, w) \leq BSC\},\ v \in \mathcal{V}$ (note that $v \in \mathcal{W}(v)$)
- $\mathcal{U} := \{\{v, w\} \in \mathcal{V}^{|2|} : d(v, w) > BCC\}$

and note that a primary controllers placement p satisfies the SCD and CCD requirements (i.e., p is feasible with respect to BSC, BCC) if, and only, if for each switch $v \in \mathcal{V}$ the set $\mathcal{W}(v)$ contains at least one controller (i.e., $\mathcal{W}(v) \cap \mathcal{V}(P) \neq \varnothing$), and for any two controllers $v, w \in \mathcal{V}(p)$, $\{v, w\} \notin \mathcal{U}$. This characterization will be used in the problem formulations presented in the following sections. In the following, quantity $d(\mathcal{G}) := \max\{d(v, w) : v, w \in \mathcal{V}\}$ will denote *diameter of the network graph* with respect to node-pair delays.

In addition to primary controllers, the network is provided with *backup controllers* that are activated in the event of an attack. Backup controllers are placed in locations disjoint with the primary controllers locations and they are not subject to the SCD and CCD restrictions. A particular assignment of backup controllers to node locations will be called *backup controllers placement* and denoted by b ($b \in \mathcal{B}$, where $\mathcal{B}$ is a given set of such placements). The set of backup controller locations of a given placement $b \in \mathcal{B}$ will be denoted by $\mathcal{V}(b)$ (where $\mathcal{V}(b) \subseteq \mathcal{V}$). Note that when primary controllers placement p and backup controllers placement b (where $p \in \mathcal{P}$ and $b \in \mathcal{B}$) are to be used, then $\mathcal{V}(p) \cap \mathcal{V}(b) = \varnothing$ and $\mathcal{V}(p, b) := \mathcal{V}(p) \cup \mathcal{V}(b)$ determines the set of all controller locations.

Node locations are subject to *node-targeted attacks* that cause both the switch and the controller (if any) in each targeted location to fail. In the following, the set of considered attacks will be denoted by $\mathcal{A}$ and the attacks in this set by a. Each attack $a \in \mathcal{A}$ is described by the set of locations $\mathcal{V}(a)$ it affects ($\mathcal{V}(a) \subseteq \mathcal{V}$). Hence, after attack a is launched, all locations v in $\mathcal{V}(a)$ and all links incident with them become unavailable. In effect, the surviving network graph, denoted by $\mathcal{G}(a) := (\mathcal{V} \setminus \mathcal{V}(a), \mathcal{E} \cap (\mathcal{V} \setminus V(a))^{|2|})$, is the maximal subgraph of $\mathcal{G}$ induced by the set of surviving

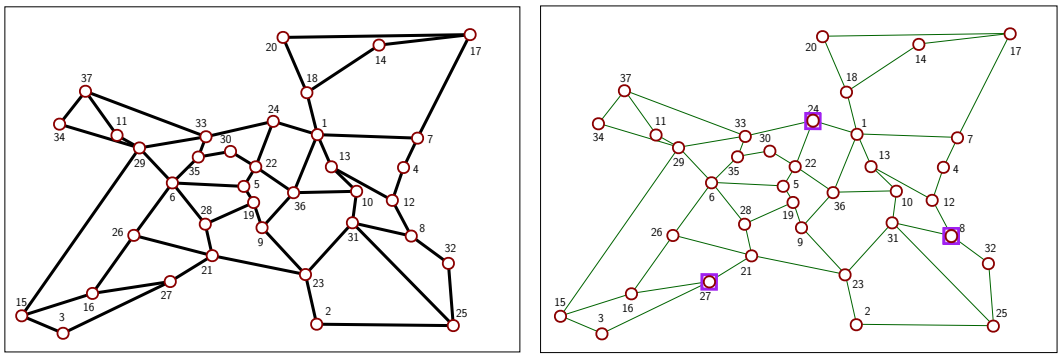

FIGURE 1 Graph of the *cost266* network (left) and a 3-node primary controllers placement (right)

nodes $\mathcal{V} \setminus \mathcal{V}(a)$. Note that after attack a, the set of surviving controllers is equal to $\mathcal{V}(p, b) \setminus \mathcal{V}(a)$, where $p \in \mathcal{P}$ and $b \in \mathcal{B}$ are the assumed primary and backup controllers placements. Two examples of 6-node attacks are shown in Figure 2.

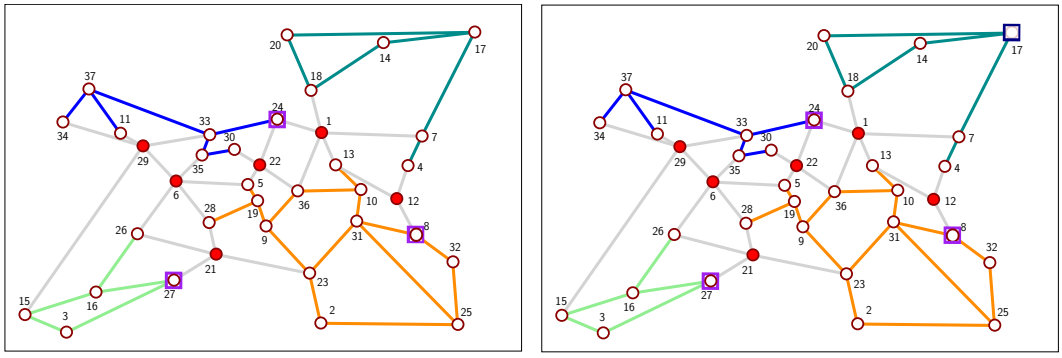

FIGURE 2 A 6-node attack and the resulting components: assuming only 3 primary controllers (left) and 3 primary and 1 backup controller (right)

As a consequence of a given attack $a \in \mathcal{A}$, the surviving graph $\mathcal{G}(a)$ is in general split into a set $C(a)$ of (disjoint) connected components, where each component $c \in C(a)$ is composed of the set of nodes denoted by $\mathcal{V}(c)$ (of size $V(c)$). Thus, the impact of attack a on the network (with given primary and backup controllers placements $p \in \mathcal{P}$ and $b \in \mathcal{B}$) can be expressed by *network availability measures* $\mathcal{M}(a)$ of the form:

$$\mathcal{M}(a) := \sum_{c \in C(a)} f(c) Y(a, c). \tag{1}$$

In this definition, $Y(a, c)$ is a binary indicator equal to 1 when a given component $c \in C(a)$ contains a controller node (i.e., when $\mathcal{V}(c) \cap \mathcal{V}(b, p) \neq \varnothing$), and to 0 otherwise (in the former case, the component is named a *surviving component*). The quantity $f(c)$, in turn, is a *component metric* defined for the components (in fact, for the subsets of $\mathcal{V}$). In the following we will consider two particular component metrics, both depending only on the size $V(c)$ of the

component c:

$$f(c) := V(c) \qquad f(c) := \binom{V(c)}{2}, \tag{2}$$

where $\binom{V(c)}{2} := 0$ for $V(c) = 1$. Using the left (*linear*) metric (L-metric in short), the quantity $\mathcal{M}(a)$ measures the overall number of nodes in the surviving components. When the right (*quadratic*) metric (Q-metric in short) is used, $\mathcal{M}(a)$ measures the total number of node-pairs in the surviving components.

The impact of a 6-node attack on node locations $\{1, 6, 12, 21, 22, 29\}$ with the primary controllers placement $\{8, 24, 27\}$ when no backup controllers are provided is illustrated on the left side of Figure 2. The considered attack splits the network into 4 components (three of them surviving). Note that the network availability measure for the L-metric is equal to 23, and for the Q-metric to 195. As illustrated on the right side of Figure 2, when the same primary controllers placement is enriched with one backup controller (placed at location 17), then for the same attack all components are surviving and the two measures are increased to 28 and 220, respectively.

Finally, for a given set of attacks $\mathcal{A}$, we define two network availability (NA) measures, namely the *worst-case network availability* (WNA in short) measure

$$\mathcal{M}(\mathcal{A}) := \min_{a\in\mathcal{A}} \mathcal{M}(a) \tag{3}$$

and the *average network availability* (ANA) measure

$$\mathcal{M}(\mathcal{A}) := \sum_{a\in\mathcal{A}} w(a)\mathcal{M}(a). \tag{4}$$

Note that in definition (4), the quantities $w(a)$, $a \in \mathcal{A}$, are given attack weights, representing for example a given probability distribution characterizing the relative frequency of the attacks under consideration.

It should be noted that for any topology of the network graph, the upper bounds (UB) of the values of measures defined in this way, which can be achieved with any controllers placement, are equal to

$$\text{WNA with the L-metric:} \quad \text{UB} = \min_{a\in\mathcal{A}}(V - V(a)) \tag{5a}$$

$$\text{ANA with the L-metric:} \quad \text{UB} = \sum_{a\in\mathcal{A}} w(a)(V - V(a)) \tag{5b}$$

$$\text{WNA/Q with the Q-metric:} \quad \text{UB} = \min_{a\in\mathcal{A}} \sum_{c\in C(a)} \binom{V(c)}{2} \tag{5c}$$

$$\text{ANA/Q with the Q-metric:} \quad \text{UB} = \sum_{a\in\mathcal{A}} w(a) \sum_{c\in C(a)} \binom{V(c)}{2}. \tag{5d}$$

A sufficient condition to meet all these bounds with primary controllers placement p and backup controllers placement b is that for each attack at least one controller is placed in all components induced by this attack, i.e., when $\mathcal{V}(p, b) \cap \mathcal{V}(c) \neq \varnothing$ for all $\in \mathcal{A}, c \in C(a)$. Note that this condition is also necessary in both cases of the ANA measure.

4 | COMBINED OPTIMIZATION OF PRIMARY AND BACKUP CONTROLLERS PLACEMENT

In this section we introduce and discuss selected variants of the basic optimization problem considered in this paper, i.e., the problem of *combined primary and backup controllers placement problem* (CPP). In short, CPP consists in finding a placement of primary controllers and a placement of backup controllers that jointly maximize the assumed network

TABLE 2 List of CPP formulations

$\mathbb{F}1$	finding joint primary and backup controllers placement maximizing the WNA measure (compact formulation) (6)
$\mathbb{F}2$	finding joint primary and backup controllers placement maximizing the ANA measure (compact formulation) (7)
$\mathbb{F}3$	finding joint primary and backup controllers placement maximizing the WNA measure (non-compact formulation) (8)
$\mathbb{F}4$	finding joint primary and backup controllers placement maximizing the ANA measure (non-compact formulation) (9)
$\mathbb{F}5$	finding allowable primary controllers placements under delay constraints (11)

TABLE 3 Notation used in CPP formulations

P', P''	minimum and maximum number of primary controllers
B', B''	minimum and maximum number of backup controllers
C	maximum overall number of controllers ($C \geq P' + B'$)
y_v	binary variable equal to 1 if, and only if, node v contains a primary controller, $y = (y_1, y_2, \ldots, y_V)$
x_v	binary variable equal to 1 if, and only if, node v contains a backup controller, $x = (x_1, x_2, \ldots, x_V)$
Y_v	binary variable equal to 1 if node v contains a controller (primary or backup)
s_{ac}	binary variable equal to 1 if, and only if, component $c \in C(a)$ contains a controller (primary or backup)
Z	continuous variable expressing the objective function
$Y(v,p)$	binary coefficient equal to 1 if, and only if, node v belongs to placement $p \in \mathcal{P}$
u_p	binary variable equal to 1 if, and only if, placement $p \in \mathcal{P}$ is selected
$\hat{\mathcal{P}}$	list of all primary controllers placements feasible with respect to the assumed BCC and BSC bounds
P', P''	minimum and maximum, respectively, number of controllers in feasible primary controllers placements
z_{vw}	binary binary variable equal to 1 if, and only if, the controller serving switch v is placed at node w
$\mathbb{B}, \mathbb{R}, \mathbb{R}_+$	sets of binary, real and non-negative real numbers
$\square$	symbol indicating the end of formulation description

availability measure $\mathcal{M}(\mathcal{A})$ (see (3) and (4)) for a given set of attacks $\mathcal{A}$. The formulations presented below are original as the so posed problem has, to the best of our knowledge, not been dealt with in the literature so far (except for our conference papers [13] and [17]).

Below we will distinguish between four kinds of optimal solutions of CPP. The term *optimal solution* will refer to a joint primary and backup controllers placement that maximizes the assumed network availability (NA) measure without imposing any limits on the number of primary and backup controllers. If such an optimal solution reaches the upper bound UB of the assumed NA measure (see definitions (5) in Section 3), it will be called *strongly optimal solution* for this measure. Finally, the (strongly) optimal solution that requires the smallest total number of controllers (primary plus backup) will be referred to as the *minimum (strongly) optimal solution*.

The problem formulations under consideration are listed in Table 2 and the notation used in those formulations is summarized in Table 3.

4.1 | Compact formulations of CPP

The two formulations considered below are *compact*, which means that in both of them the number of variables and constrains grows polynomially with the number of node locations V. Note that in fact the number of attacks in $\mathcal{A}$ may also increase exponentially with V and then our formulations would become non-compact. Yet, since in the following we consider only sets of attacks of reasonable size, we do not address this issue and assume that the number of attacks in $\mathcal{A}$ is polynomially bounded with respect to V.

The first formulation maximizes, for a given set of attacks $\mathcal{A}$, the WNA measure (3) over a set of feasible controllers placements, constrained by the lower (P', B') and upper (P'', B'') bounds on the number of primary and backup controllers, respectively.

Formulation $\mathbb{F}1[P', P'', B', B'', C, BSC, BCC, \mathcal{A}]$

$$\max \quad Z \tag{6a}$$

$$\sum_{v\in\mathcal{V}} y_v + \sum_{v\in\mathcal{V}} x_v \le C \tag{6b}$$

$$P' \le \sum_{v\in\mathcal{V}} y_v \le P'' \tag{6c}$$

$$B' \le \sum_{v\in\mathcal{V}} x_v \le B'' \tag{6d}$$

$$\sum_{w\in\mathcal{W}(v)} y_w \ge 1 \qquad v \in \mathcal{V} \tag{6e}$$

$$y_v + y_w \le 1 \qquad \{v, w\} \in \mathcal{U} \tag{6f}$$

$$Y_v = y_v + x_v \qquad v \in \mathcal{V} \tag{6g}$$

$$s_{ac} \le \sum_{v\in\mathcal{V}(c)} Y_v \qquad a \in \mathcal{A},\ c \in C(a) \tag{6h}$$

$$Y_v \le s_{ac} \qquad a \in \mathcal{A},\ c \in C(a), v \in \mathcal{V}(c) \tag{6i}$$

$$Z \le \sum_{c\in C(a)} f(c) s_{ac} \qquad a \in \mathcal{A} \tag{6j}$$

$$y_v, x_v, Y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{6k}$$

$$s_{ac} \in \mathbb{B} \qquad a \in \mathcal{A},\ c \in C(a) \tag{6l}$$

$$Z \in \mathbb{R}. \tag{6m}$$

In the formulation, the vectors of binary variables $y := (y_1, y_2, \ldots, y_V)$ and $x := (x_1, x_2, \ldots, x_V)$ determine the set of locations of primary controllers $\{v \in \mathcal{V} : y_v = 1\}$ and backup controllers $\{v \in \mathcal{V} : x_v = 1\}$, while constraints (6b)-(6g) ensure feasibility of the primary/backup controllers placements pairs determined by (y, x). In particular, constraint (6b) limits the total number of controllers to a given value C, while constraints (6c) and (6d) ensure that the numbers of primary and backup controllers are within the assumed ranges, where $P' + B' \le C$.

The next two constraints relate to delays. The first of them, constraint (6e), ensures that for each location $v \in \mathcal{V}$ there must be a primary controller placed close enough to it in terms of the SC delay (recall that $\mathcal{W}(v)$ is the set of locations w, including location v, with the SC delay between v and w not exceeding BSC). Similarly, constraint (6f) ensures that the CC delay requirements are met (recall that $\mathcal{U}$ is the set of all node-pairs whose distance, measured as the transmission delay, exceeds the upper bound BCC).

Then, constraint (6g) sets the value of binary variable Y_v to 1 if, and only if, location v contains either a primary or a backup controller. Note that binarity of Y_v does not allow to place a primary controller and a backup controller in the same location.

Next, constraints (6h) and (6i) set binary variable s_{ac} to 1 when component c induced by attack a contains a

controller, and to 0, otherwise.

Finally, constraint (6j) together with objective (6a) ensure that the optimal value of Z is properly calculated. This is because for any feasible pair (y, x), the maximum of Z (let us denote this maximum by $Z(y, x)$) is equal to $\mathcal{M}(\mathcal{A}) = \min_{a\in\mathcal{A}} \mathcal{M}(a)$ where the values $\mathcal{M}(a)$ are calculated for the primary and back controllers placement specified by (y, x). Since formulation (6) maximizes $Z(y, x)$ over all feasible pairs (x, y), the value $Z(y^*, x^*)$ for any optimal pair (y^*, x^*) of (6) maximizes the availability measure (3) over all placements in the assumed set of placements represented by constraints (6b)-(6e). □

It is worth noting that constraint (6i) is redundant since in the optimal solutions the values of s_{ac} allowed by (6h) will be set to 1 when this is advantageous for maximizing the value of Z.

Note also that for parameters $P' = B' = 0$ and $P'' = B'' = C$, constraints (6c)-(6d) can be skipped — in this case no separate bounds on the number of primary and backup controllers are imposed, only on their total number. Another observation is that we can always assume $P' \geq 1$ because in any feasible solution of $\mathbb{F}1$ at least one y_v will be equal to 1 (this is forced by constraint (6e)) — this will enforce the formulation.

For the ANA measure (4), the formulation corresponding to (6) is as follows.

Formulation $\mathbb{F}2[P', P'', B', B'', C, BSC, BCC, \mathcal{A}]$

$$\max \sum_{a\in\mathcal{A}} w(a) \sum_{c\in C(a)} f(c) s_{ac} \tag{7a}$$

$$\sum_{v\in\mathcal{V}} y_v + \sum_{v\in\mathcal{V}} x_v \leq C \tag{7b}$$

$$P' \leq \sum_{v\in\mathcal{V}} y_v \leq P'' \tag{7c}$$

$$B' \leq \sum_{v\in\mathcal{V}} x_v \leq B'' \tag{7d}$$

$$\sum_{w\in\mathcal{W}(v)} y_w \geq 1 \qquad v \in \mathcal{V} \tag{7e}$$

$$y_v + y_w \leq 1 \qquad \{v, w\} \in \mathcal{U} \tag{7f}$$

$$Y_v = y_v + x_v \qquad v \in \mathcal{V} \tag{7g}$$

$$s_{ac} \leq \sum_{v\in\mathcal{V}(c)} Y_v \qquad a \in \mathcal{A},\ c \in C(a) \tag{7h}$$

$$y_v, x_v, Y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{7i}$$

$$s_{ac} \in \mathbb{B} \qquad a \in \mathcal{A},\ c \in C(a). \tag{7j}$$

Note that constraints (7b)-(7h) are identical to constraints (6b)-(6h) in $\mathbb{F}1$, where the redundant constraint (6i) is skipped. □

In formulations $\mathbb{F}1$ and $\mathbb{F}2$, allowable primary controllers placements (forming the set of allowable placements $\mathcal{P}$) are limited by their size and the upper bounds on the CC and SC delay. Yet, additional limitations can be considered. For example, it might be natural to force locations from a given set to contain controllers, and another set of locations not to contain controllers — this can be easily achieved by fixing appropriate variables y_v to 1 or to 0, respectively. Another possibility is to require that for each pair of locations from a given set of such pairs, either both locations contain a controller or neither one does — this would be forced by additional equality constraints of the form $y_v = y_w$.

Note that other kinds of limitations on primary controllers $p \in \mathcal{P}$ can be thought of (see [16]), and also that the considered limitations can be applied to backup controllers placements $b \in \mathcal{B}$ and to joint primary and backup controllers placements (p, b). In fact, one such limitation is already imposed on (p, b) in $\mathbb{F}1$ (constraint (6g)) and $\mathbb{F}2$ (constraint (7g)): locations cannot contain a primary and a backup controller simultaneously.

4.2 | Non-compact formulations of CPP

The two formulations $\mathbb{F}3$ and $\mathbb{F}4$ of the combined optimization of primary and backup controllers placement optimization problem (CPP) presented below are *non-compact* counterparts of the corresponding compact formulations $\mathbb{F}1$ and $\mathbb{F}2$ discussed in the previous section. Now, the set of primary controllers placements considered in optimization is predefined and given by means of an explicit list of *allowable* placements $\mathcal{P}$. In the considered context, non-compactness means that the size of list $\mathcal{P}$ could potentially be exponential with the number of locations V. (Note that we still assume that the number of attacks in $\mathcal{A}$ is polynomially bounded by the number of node locations V.)

The first non-compact formulation concerns maximization of the WNA measure (3), and the second maximization of the ANA measure (4). As already mentioned, both cases assume an explicit (predefined) list $\mathcal{P}$ of primary controllers placements, and (as before) a given list of attacks $\mathcal{A}$.

The following formulation, where variables x_v, Y_v, s_{ac} have the same meaning as in $\mathbb{F}1$, maximizes the WNA measure (3).

Formulation $\mathbb{F}3[\mathcal{P}, B', B'', C, \mathcal{A}]$

$$\max \quad Z \tag{8a}$$

$$\sum_{p\in\mathcal{P}} u_p = 1 \tag{8b}$$

$$\sum_{p\in\mathcal{P}} V(p)u_p + \sum_{v\in\mathcal{V}} x_v \le C \tag{8c}$$

$$B' \le \sum_{v\in\mathcal{V}} x_v \le B'' \tag{8d}$$

$$Y_v = x_v + \sum_{p\in\mathcal{P}} Y(v,p)u_p \qquad v \in \mathcal{V} \tag{8e}$$

$$s_{ac} \le \sum_{v\in\mathcal{V}(c)} Y_v \qquad a \in \mathcal{A},\ c \in C(a) \tag{8f}$$

$$Z \le \sum_{c\in C(a)} f(c)s_{ac} \qquad a \in \mathcal{A} \tag{8g}$$

$$u_p \in \mathbb{B} \qquad p \in \mathcal{P} \tag{8h}$$

$$x_v, Y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{8i}$$

$$s_{ac} \in \mathbb{B} \qquad a \in \mathcal{A},\ c \in C(a) \tag{8j}$$

$$Z \in \mathbb{R}. \tag{8k}$$

In the formulation, binary variables u_p are used to select a primary placement p out of the set of placements $\mathcal{P}$, and constraint (8b) ensures that exactly one primary controllers placement (the placement $p \in \mathcal{P}$ for which $u_p = 1$) is actually selected. Then, constraint (8c) ensures that the total number of controllers does no exceed the assumed upper bound C (recall that $V(p)$ denotes the number of controllers in placement p), while constraint (8d) ensures that not less than B' and not more than B'' backup controllers are used.

Next, constraint (8e), where $Y(v,p)$ is a binary coefficient equal to 1 if, and only if, $v \in \mathcal{V}(p)$ (i.e., location v is used by placement p), sets the value of binary variable Y_v to 1 if, and only if, location v contains a backup controller or a primary controller from the selected placement p, i.e., the placement with $u_p = 1$ (and, additionally, ensures that at most one controller is placed in v).

Since the so defined variables Y_v have the same meaning as their counterparts in $\mathbb{F}1$, and constraints (8f)-(8g) and objective (8a) are the same as constraints (6h)-(6h) (with constraint (6i) skipped) and objective (6a) in $\mathbb{F}1$, optimal solutions of $\mathbb{F}3$ maximize the availability measure (3) over all placements (p, b) where $p \in \mathcal{P}$, and $\mathcal{V}(p) \cap \mathcal{V}(b) = \varnothing$ and $B' \le V(b) \le \min\{B'', C - V(p)\}$. □

The second formulation, a modification of (8), maximizes the ANA measure (4):

Formulation $\mathbb{F}4[\mathcal{P}, B', B'', C, \mathcal{A}]$

$$\max \ \sum_{a\in\mathcal{A}} w(a) \sum_{c\in C(a)} f(c) s_{ac} \tag{9a}$$

$$\sum_{p\in\mathcal{P}} u_p = 1 \tag{9b}$$

$$\sum_{p\in\mathcal{P}} V(p) u_p + \sum_{v\in\mathcal{V}} x_v \le C \tag{9c}$$

$$B' \le \sum_{v\in\mathcal{V}} x_v \le B'' \tag{9d}$$

$$Y_v = x_v + \sum_{p\in\mathcal{P}} Y(v,p) u_p \qquad v \in \mathcal{V} \tag{9e}$$

$$s_{ac} \le \sum_{v\in\mathcal{V}(c)} Y_v \qquad a \in \mathcal{A},\ c \in C(a) \tag{9f}$$

$$u_p \in \mathbb{B}, \qquad p \in \mathcal{P} \tag{9g}$$

$$x_v, Y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{9h}$$

$$s_{ac} \in \mathbb{B} \qquad a \in \mathcal{A},\ c \in C(a). \tag{9i}$$

We do not explain the above formulation because constraints (9b)-(9f) are identical to constraints (8b)-(8f) in $\mathbb{F}3$. □

Finally, note that when the allowable set $\mathcal{P}$ contains just one element, p, say, then the problem reduces to finding a placement of backup controllers maximally enhancing the resilience of this particular primary controllers placement to attacks in $\mathcal{A}$, and formulations $\mathbb{F}3$ and $\mathbb{F}4$ can be easily modified to their respective versions not involving variables u_p. For example, for $\mathbb{F}4$ such a modification is as follows.

Formulation $\mathbb{F}4'[\mathcal{P} = \{p\}, B', B'', C, \mathcal{A}]$

$$\max \ \sum_{a\in\mathcal{A}} w(a) \sum_{c\in C(a)} f(c) s_{ac} \tag{10a}$$

$$V(p) + \sum_{v\in\mathcal{V}} x_v \le C \tag{10b}$$

$$B' \le \sum_{v\in\mathcal{V}} x_v \le B'' \tag{10c}$$

$$Y_v = x_v + Y(v,p) \qquad v \in \mathcal{V} \tag{10d}$$

$$s_{ac} \le \sum_{v\in\mathcal{V}(c)} Y_v \qquad a \in \mathcal{A},\ c \in C(a) \tag{10e}$$

$$x_v, Y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{10f}$$

$$s_{ac} \in \mathbb{B} \qquad a \in \mathcal{A},\ c \in C(a). \tag{10g}$$

Clearly, additional constraints (discusses at the end of Section 4.1) on the locations of backup controllers can be added to the above formulations.

4.3 | Preparing lists of primary controllers placements

An important (and not obvious) question related to the non-compact formulations (8) and (9) discussed in the previous section is how to prepare lists of allowable primary controllers placements. In general, to ensure optimal solutions of CPP, the list under consideration must contain all primary controllers placements feasible with respect to the number of controllers and maximum CC and SC delays. To obtain such a list (denoted by $\hat{\mathcal{P}}$) we can proceed as follows.

First, by means of formulations $\mathbb{F}7$ and $\mathbb{F}7'$ (see formulations (14) and (15) in Section A.1), we calculate the minimum

and maximum number of controllers (P' and P'', respectively) in the (feasible) placements composing list $\hat{\mathcal{P}}$. Having done this, we execute the following procedure to generate list $\hat{\mathcal{P}}$.

Step 1. $\hat{\mathcal{P}} := \emptyset$, $P := P' - 1$.
Step 2. $P := P + 1$, $\mathcal{P} := \emptyset$; solve formulation $\mathbb{F}5[P, BSC, BCC, \mathcal{P}]$ iteratively; $\hat{\mathcal{P}} := \hat{\mathcal{P}} \cup \mathcal{P}$.
Step 3. if $P = P''$ stop; otherwise go to **Step 2**.

Formulation $\mathbb{F}5$ solved in Step 2 is used to generate all feasible primary controllers placements of a given size P and is as follows.

Formulation $\mathbb{F}5[P, BSC, BCC, \mathcal{P}]$

$$\min \ \frac{1}{V} \sum_{v \in \mathcal{V}} \sum_{w \in \mathcal{W}(v)} d(v,w) z_{vw} \tag{11a}$$

$$\sum_{v \in \mathcal{V}} y_v = P \tag{11b}$$

$$y_v + y_w \le 1 \qquad \{v,w\} \in \mathcal{U} \tag{11c}$$

$$\sum_{w \in \mathcal{W}(v)} z_{vw} = 1 \qquad v \in \mathcal{V} \tag{11d}$$

$$z_{vw} \le y_w \qquad v \in \mathcal{V},\ w \in \mathcal{W}(v) \setminus \{v\} \tag{11e}$$

$$z_{vv} = y_v \qquad v \in \mathcal{V} \tag{11f}$$

$$\sum_{v \in \mathcal{V}(p)} y_v \le P - 1 \qquad p \in \mathcal{P} \tag{11g}$$

$$y_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{11h}$$

$$z_{vw} \in \mathbb{B} \qquad v \in \mathcal{V},\ w \in \mathcal{W}(v). \tag{11i}$$

As before, binary variables y_v determine locations of primary controllers and constraint (11b) implies that exactly P controllers are located. Then, constraint (11c) (where $\mathcal{U}$ is the set of all location pairs whose distance, measured as the transmission delay, exceeds the upper bound BCC) enforces compliance with the CC delay requirements, just like constraint (6f) in formulation $\mathbb{F}1$.

The next group of constraints, (11d)-(11f), determine, using binary variables z_{vw}, the assignment of switches to controllers. Assuming that $z_{vw} = 1$ if, and only if, the switch in location v is assigned to the controller in location w, constraint (11d) ensures that the switch in location v is assigned to exactly one of the controllers located in the set $\mathcal{W}(v)$ (i.e., in the set of locations to which the transmission delay from location v is not greater than BSC), and constraint (11e) implies that if $z_{vw} = 1$ then location w must contain a controller. Constraint (11f), in turn, ensures that the switch in a location containing a controller is assigned to that controller. In effect, objective function (11a) (to be minimized) expresses the average SC delay for the assignment of switches to controllers defined by variables z_{vw}.

Finally, constraint (11g) forces the placement of controllers (located in the set $\{v : y_v = 1,\ v \in \mathcal{V}\}$) to differ from each placement in the current set $\mathcal{P}$ by at least one location.

Again, extra constraints on primary controllers locations described at the end of Section 4.1 could be added to $\mathbb{F}5$. □

Formulation $\mathbb{F}5$ is solved iteratively, starting with empty list of placements $\mathcal{P}$. After each iteration, a newly found placement is added to list $\mathcal{P}$ and the so adjusted formulation is resolved. The iterations are stopped when the formulation becomes infeasible, which means that all feasible placements have been found. Note that the placements produced in the consecutive iterations are ordered according the non-decreasing value of the average SC delay, so

the iterations can be stopped when this value becomes too large.

When the list $\mathcal{P}$ appearing in constraint (11g) is short the computation time needed to solve formulation $\mathbb{F}5$ is typically very short (less than one second for the cases considered in the numerical results). However, when the size of that list becomes large, say 10 000, the computation time can increase to hours or even more due to the excessive number of inequalities in constraint (11g) and their linear relaxation being pretty weak. Thus, to determine a large number of best controller placements (which is actually not required in our numerical studies) solving problem $\mathbb{F}5$ iteratively, every time augmenting list $\mathcal{P}$ to account for the placements that have already been found, becomes computationally inefficient. The computation time can be partly decreased by using formulation $\mathbb{F}5$ with no objective function to simply find a consecutive feasible placement outside the current list $\mathcal{P}$:

Formulation $\mathbb{F}5'[P, BSC, BCC, \mathcal{P}]$

$$\sum_{v\in\mathcal{V}} y_v = P \tag{12a}$$

$$y_v + y_w \le 1 \qquad \{v, w\} \in \mathcal{U} \tag{12b}$$

$$\sum_{w\in\mathcal{W}(v)} y_w \ge 1 \qquad v \in \mathcal{V} \tag{12c}$$

$$\sum_{v\in\mathcal{V}(p)} y_v \le P - 1 \qquad p \in \mathcal{P} \tag{12d}$$

$$y_v \in \mathbb{B} \qquad v \in \mathcal{V}. \tag{12e}$$

Clearly, in the iterative process using formulation $\mathbb{F}5'$ the order of generated placements is not controlled.

In any case, in order to determine N best problem solutions when N is large, solving the problem N times with additional constraints that exclude the solutions that have already been found is inefficient. A large number of problem instances have to be solved, gradually, the problem size increases considerably, and the linear relaxation of the previous-solution-excluding constraints is very weak too. However, one may use the following, pretty general, approach. One can implement the IP model of the problem using callable libraries of the IP solver in order to gain access to the callbacks of the branch-and-bound process. Then every time an incumbent solution is found and the respective callback is invoked, one can retrieve the incumbent solution, store it in the list of best solutions and finally make the branch-and-bound process reject the current solution and continue the search. Obviously, it is sufficient to keep only the set of N best solutions in the list. And whenever this set is being updated with the current incumbent solution, apart from rejecting the solution one should also add a user cut that sets an upper limit on the objective function value equal to the cost of the current N-th best solution to bound the search process (the effectiveness of this approach still needs to be tested).

However, in the general case, the use of more efficient approaches to the problem under consideration cannot guarantee acceptable computation times due to the number of feasible controllers placements, i.e., $|\hat{\mathcal{P}}|$, which can grow exponentially with the number of nodes V. The extreme case is when the values of both BCC and BSC are equal to or greater than the diameter of the graph (where link weights represent link delays). Then, $P' = 1, P'' = V$ and each nonempty subset of $\mathcal{V}$ would represent a feasible primary controllers placement; hence, $|\hat{\mathcal{P}}|$ would be equal to $2^V - 1$. Such an exponential growth would in general be observed even when the delay constraints (defined by BCC and BCC) and the placement size constraints (defined by P' and P'') eliminate a great deal of the subsets of $\mathcal{V}$. This issue will be illustrated in the numerical section.

Obviously, there are situations where constructing the list of allowable primary controllers placements is not a big deal. For example, when the network operator decides to install several backup controllers to increase the network resilience to attacks, the list of allowable placements $\mathcal{P}$ would be composed of just one placement p — the

FIGURE 3 Two primary controllers placements and their resilience to a 1-node attack (linear metric)

placement actually deployed in the network. Another situation of this kind is when the set $\mathcal{P}$ contains the candidate placements that are selected by the operator based on her/his experience and various practical constraints, as, for example, preference of some locations. In fact, it is precisely these kinds of situations that may require non-compact CPP formulations, since the conditions that characterize the placements under consideration may be difficult to express in terms of linear constraints.

For a given value of BCC, an important list of allowable primary controllers placements is obtained by solving formulation $\mathbb{F}5$ for $BSC = D^*$ and $P = P^*$, where D^* is the minimum SC delay achievable for all switches, and P^* is the minimum number of primary controllers required to assure $BSC = D^*$. These two values can be computed by formulations $\mathbb{F}6$ and $\mathbb{F}7$, respectively, specified in Section A.1 of Appendix A (formulations (13) and (14)). The sets of placements $\mathcal{P}$ generated in this way will be used in the numerical study; as we will see there, the so obtained lists are very short and can be quickly found in the above described way. (As a matter of fact, the value of D^* could be increased slightly if doing so resulted in a noticeable reduction in the average SC delay minimized by (11a).)

Finally, note that the list of all feasible placements generated for a given value of BCC and the corresponding values of $P = P^*$, $BSC = D^*$, might not guarantee optimal solutions in general. This is because the best (with respect to providing resilience to attacks) placement composed of only P^* primary controllers may be less advantageous than some placement composed of more primary controllers.

An example of such a case is shown in Figure 3 for a 3-node, 2-link network graph where we assume that the delay of each link is equal to 1, $BSC = 1$, $BCC = 2$, $P' = 1, P'' = 2, B' = 0, B'' = 1, C = 2$, and we consider 1-node attacks. The left placement consists of one primary controller (dark grey) placed at node v_2 and one backup controller (light gray) placed at node v_1. The right placement consists of two primary controllers (dark grey) placed at nodes v_1 and v_3 (and does not contain a backup controller). Clearly, both placements are feasible with respect to the assumed parameters and that the left placement contains the minimum number of primary controllers ($P^* = 1$). We note that the worst attack for the left placement targets node v_2 and results in only one surviving node v_1, while for the right placement all three 1-node attacks result in two surviving nodes. Hence, the primary controllers placement with $P = 2$ controllers leads to a higher resilience level in the case of the linear metric $f(c) = V(c)$ (see (2)).

A similar example, this time related to the quadratic component metric $f(c) = \binom{V(c)}{2}$ (see (2)), is shown in Figure 4. Now, using only one primary controller (in v_3) and one backup controller (in any of the remaining nodes, say in v_4 — the left placement) secures only one surviving node-pair (v_4, v_5) after attack on node v_3. Using two primary controllers (one on each side of node v_3, say in nodes v_1, v_4 — the right placement) secures at least two surviving node-pairs. More specifically, two node-pairs (v_1, v_2) and (v_4, v_5) survive when node v_3 is attacked, and 6 node-pairs survive in case any other node is attacked (this also shows that attacking a node with no controller can be advantageous).

Note that both examples can be easily modified (by increasing the number of nodes on either side of the central node) to illustrate a substantially gain achievable when more than P^* primary controllers are used.

Therefore, to be generally sure that the non-compact formulation of CPP will find an optimal solution, all feasible (with respect to BSC and BCC) primary controllers placements with $P = P', P' + 1, \ldots, P''$ (where $P' = P^*$) should be considered. Fortunately, situations where more than P^* of the primary controllers are needed to reach optimality are not common. In particular, they were not encountered in the cases considered in the numerical study presented in this work.

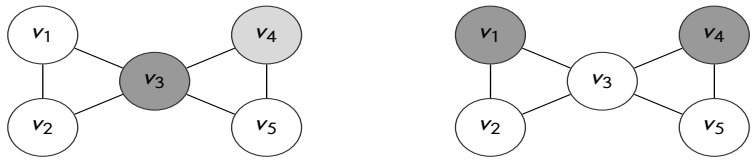

FIGURE 4 Two primary controllers placements and their resilience to a 1-node attack (quadratic metric)

5 | NUMERICAL STUDY

The main goal of the numerical study is to illustrate the benefits of using backup controllers (in addition to primary controllers) to improve network resilience. For this purpose, we present and discuss the numerical results obtained using the optimization models described in this paper for two mesh network instances: *cost266* (a pan-European network) and *coronet conus* (a continental US network).

The first network (*cost266*), consisting of $V = 37$ node locations and $E = 57$ links, is depicted in Figure 5 (and, for that matter, also in Figures 1-2); it is described in SNDlib [14] at http://sndlib.zib.de. The second network (*coronet conus*), composed of $V = 75$ node locations and $E = 99$ links, is shown in Figure 6; it is described for example in [25], [23].

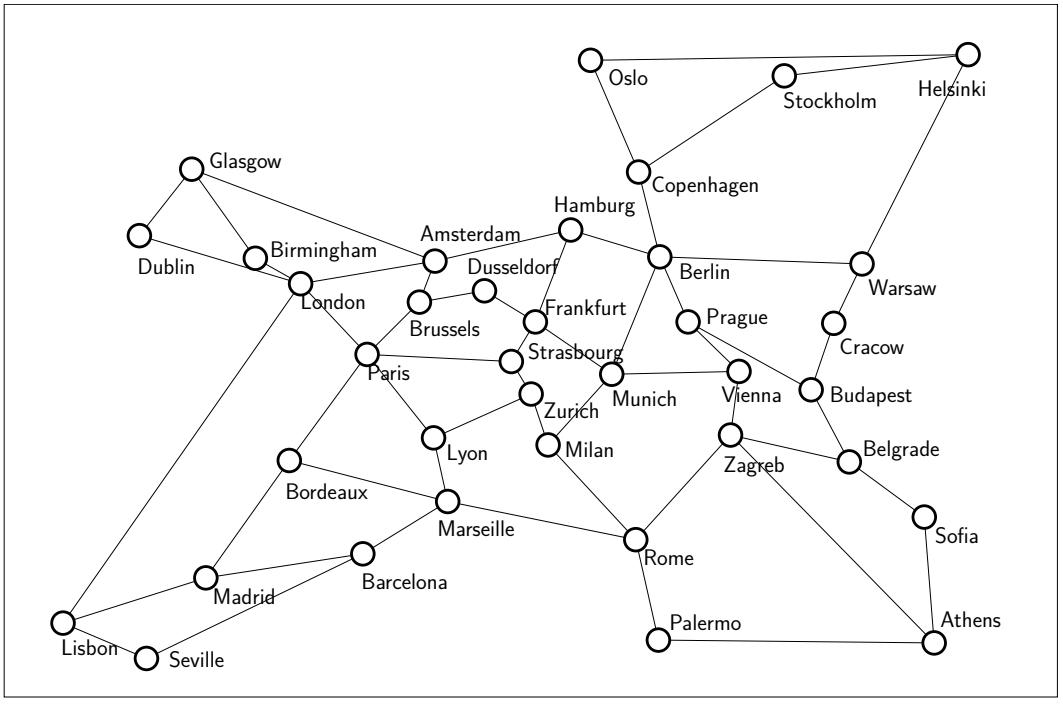

FIGURE 5 Topology of the *cost266* network

In this section, we will first describe the setup of the performed numerical experiments, the detailed description and discussion of which for both the *cost266* and *coronet conus* networks is presented in Appendix B. After that, we present important observations and conclusions from the numerical study.

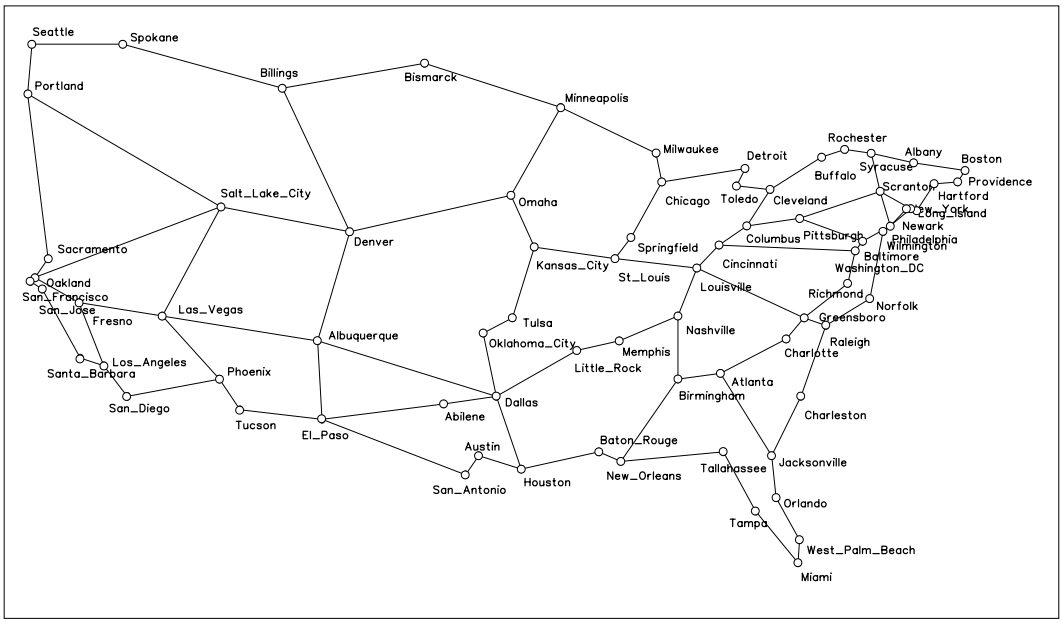

FIGURE 6 Topology of the *coronet conus* network

5.1 | Setup of experiments

The numerical results of our study were obtained by means of CPP formulations $\mathbb{F}1 - \mathbb{F}4$ (see Table 2). The parameters used in the input data were prepared by means of formulation $\mathbb{F}5$ (Table 2) and formulations $\mathbb{F}6 - \mathbb{F}8$ (see Table 11).

In the experiments, the transmission delay (SCD — switch-to-controller delay, and CCD — controller-to-controller delay) between a given pair of nodes (expressed in kilometers) was calculated as the length of the shortest path between their locations, where the lengths of the links were assumed to be equal to their geographical lengths (in kilometers). The results consider all four cases of the network availability (NA) measures implied by definitions (1)-(4). These are: the average NA (ANA) and the worst-case NA (WNA) measures, with either linear (L) or quadratic (Q) metric, where the weights $w(a)$ used in the ANA measure are uniformly set to $\frac{1}{|\mathcal{A}|}$, $a \in \mathcal{A}$.

The setup of the experiment performed for each of the two network instances is briefly as follows. We start with preparing a set of lists of most dangerous K-node attacks for $K = 4, 6, 8, 10$. Typically, each such list contains $A = 12$ attacks; additionally, for the *coronet conus* network, a long list of $A = 100$ most dangerous 6-node attacks was included. Then we select two values for the CCD delay limit (strict and loose), and for each of them we determine the minimum achievable value (denoted by D^*) of the maximum SCD (taken over all switches) and the minimum number of primary controllers (denoted by P^*) with which D^* is achieved. Next, we generate the list of all placements composed of P^* primary controllers (such placements are called *minimum primary controllers placements*) that meet the assumed CCD constraint and the corresponding SCD constraint D^* (this list is used as input to the non-compact formulations). Then, for the input parameters thus calculated, we solve all relevant instances of the combined primary and backup controllers placement problem (CPP) using both compact formulation and non-compact formulations of CPP. The considered instances cover the whole range of meaningful values of parameters P', P'', B', B''.

A list of abbreviations used in the tables showing the numerical results can be found in Table 4. Note that since in this study we assume $B' = 0$ (no lower bound on the number of backup controllers) in all cases, the upper bound

TABLE 4 Numerical results: list of abbreviations

P', P''	minimum and maximum number of primary controllers
B	maximum number of backup controllers (minimum number is always equal to 0)
C	maximum overall number of controllers ($C \geq P'$)
BSC, BCC	upper bound on the SC delay (SCD) and the CC delays (CCD), respectively
D^*	the least feasible upper bound on SCD
P^*	the smallest number of primary controllers needed to fulfil $BSC = D^*$ for a given BCC
$\mathcal{P}^*$	the set of all primary controllers placements with P^* controllers feasible for $BSC = D^*$ and a given BCC
ASCD	average SC delay (calculated)
$\mathcal{A}(K, A)$	A-element list of K-node attacks
NA	network availability
ANA/L	average network availability (with L-metric)
ANA/Q	average network availability (with Q-metric)
WNA/L	worst-case network availability (with L-metric)
WNA/Q	worst-case network availability (with Q-metric)

on the number of backup controllers is denoted by B instead of B''.

5.2 | Main findings

Below are the main observations and conclusions that can be drawn from the numerical results presented and discussed in Appendix B for *cost266* (Section B.1) and *coronet conus* (Section B.2). As for both networks most of the reported results concern the 12-attack lists of 6-node attacks (i.e., medium-size attacks) denoted by $\mathcal{A}(6, 12)$ and described in Sections B.1.1 and B.2.1, we start our discussion with this case.

- In most cases (besides *cost266* with the loose CCD limit), when backup controllers are not applied, the upper bounds (UB) on resilience levels (given by formulas (5) in Section 3) cannot be reached for any of the considered network availability (NA) measures (ANA/L, WNA/L, ANA/Q, WNA/Q), no matter how many primary controllers are used. In other words, in those cases there are no strongly optimal solutions consisting only of primary controllers (the concepts of optimality for the CPP solutions are introduced at the beginning of Section 4). Moreover, the gaps between the maximum achievable values of the NA measures under consideration and their UBs can be significant.

  - When the strict CCD limit equal to 1500 km is assumed, then for both networks there are no strongly optimal solutions consisting only of primary controllers for any of the considered NA measures. The gaps between the maximum achievable values of the NA measures and their UBs are significant, between 10% and 20% for *cost266*, and between 50% and 60% for *coronet conus*. The reason is that the strict CCD limit (which determines the diameter of the circle on the network map that all primary controllers must be in) does not allow to efficiently spread the primary controllers in the network graph. This effect is more profound for *coronet conus* because in this larger network of diameter around 6500 km it is harder to protect the components (of the sur-

viving network graphs) close to the network borders by controllers concentrated in a circle of diameter 1500 km than in the *cost266* network of diameter around 4000 km.

- For the loose CCD limit (equal to 2000 km for *cost266* and to 2500 km for *coronet conus*), strongly optimal placements composed of only primary controllers exist for all NA measures in the *cost266* case, but none of them exists in the *coronet conus* case. However, in the latter case, the considered gaps are approximately two times smaller than for the strict CCD limit.
- In the case of *cost266*, minimum optimal placements of primary controllers contain, depending on the NA measure, from 0 to 3 additional controllers so that the minimum optimal placements contain 3 to 6 primary controllers in the strict CDD limit case, and from 5 to 8 in the in the loose CCD limit case. Recall that in *cost266* minimum primary controllers placements contain $P^* = 3$ (strict CCD limit) or $P^* = 5$ (loose CCD limit) controllers to meet the delay constraints. For *coronet conus*, in minimum optimal solutions either no additional controllers are needed (strict CDD limit) or at most 1 additional controller is needed (loose CCD limit). Hence, the minimum optimal placements contain 2 controllers in the first case, and 3 or 4 controllers in the second case. Recall that in *coronet conus* minimum primary controllers placement contain $P^* = 2$ (strict CCD limit) or $P^* = 3$ (loose CCD limit) controllers.
- Thus, in the cases when the UBs are not reached (both networks with the strict CDD limit and *coronet conus* with the loose CDD limit), the number of primary controllers in minimum optimal solutions is between 2 and 6. For *cost266* and the loose CCD limit, the minimum optimal placements contain between 5 and 8 controllers, but in this case the UBs are reached for all NA measures.

- In general, the use of backup controllers is highly beneficial for increasing network resilience to attacks as it allows you to reach the upper bounds on the resilience levels with a reasonable number of backup controllers while keeping the number of primary controllers at the lower limit P^*. Clearly, with the use of backup controllers, minimal strongly optimal solutions can always be found, for example by installing backup controllers all nodes that do not contain a primary controller. So what really matters is to achieve minimum strongly optimal solutions with a small total number of controllers, which, as discussed below, is the case. What is also important, in all cases minimum strongly optimal solutions can be obtained by extending (by only a few backup controllers) an appropriately selected minimum primary controllers placement, which is an additional benefit for the network operator due to lower operational cost of backup controllers. Although, as discussed in Section 4.3 and illustrated in Figures 3 and 4, this property generally does not hold, it appears to hold for the mesh network topologies under consideration.

  - In the case of *cost266* and the strict CCD limit, no more than 4 backup controllers (plus $P^* = 3$ primary controllers) are needed to reach the upper bounds for all NA measures. This means that in this case the network can be maximally protected against the assumed 6-node attacks using at most 7 controllers in total. Moreover, for all NA measures, adding just one backup controller to an appropriate minimum primary controller placement (i.e., a placement of size P^*) makes it possible to find a CPP solution with the NA measure value very close (or even equal for WNA/Q) to its upper bound. This means that it suffices to use at most 4 controllers in total to closely approach the UB. As mentioned above, when in *cost266* the loose CCD limit is assumed, exceptionally the UBs can be reached using only primary controllers. In this case, for all NA measures the total number of controllers (equal to 8 in the worst case) in the minimum (strongly) optimal placements remains the same when backup controllers are allowed.
  - In the *coronet conus* network, the benefits form using backup controllers are even more spectacular. In the case of the strict CCD limit, the UBs are reached with 3 backup controllers (i.e., with 5 controllers in total) for

ANAL/L and WNA/L, and with 2 backup controllers (4 controllers in total) for ANA/Q and WNA/Q. For the loose limit, the respective UBs are reached with 2 backup controllers (5 controllers in total) and with 1 backup controller (4 controllers in total). Thus, *coronet conus* can be maximally protected against the considered 6-node attacks using no more than 5 controllers in total for both CCD limits.

TABLE 5 Minimum optimal solutions for primary controllers; C – placement size, V – value of $\mathcal{M}(\mathcal{A}(6,12))$

cases		*cost266*				*coronet conus*			
CCD limit	NA	C	V	UB	gap	C	V	UB	gap
strict	ANA/L	6	25.7	**31**	17.1%	2	27	**69**	60.8%
	WNA/L	6	25	**31**	19.4%	2	27	**69**	60.8%
	ANA/Q	5	123.5	**134.9**	9.1%	2	351.0	**752.7**	53.4%
	WNA/Q	3	109	**124**	12.1%	2	351	**751**	53.3%
loose	ANA/L	8	31.0	**31**	0%	4	48.5	**69**	29.7%
	WNA/L	8	31	**31**	0%	4	46	**69**	33.3%
	ANA/Q	6	134.9	**134.9**	0%	3	551.8	**752.7**	26.7%
	WNA/Q	5	124	**124**	0%	3	504	**751**	32.9%

TABLE 6 [tables 10, 25]

cases		*cost266*				*coronet conus*			
CCD limit	NA	C	V	UB	gap	C	V	UB	gap
strict	ANA/L	7	31	**31**	0%	5	69	**69**	0%
	WNA/L	7	25	**31**	0%	5	69	**69**	0%
	ANA/Q	6	134.9	**134.9**	0%	4	752.7	**752.7**	0%
	WNA/Q	4	124	**124**	0%	4	751	**751**	0%
loose	ANA/L	8	31	**31**	0%	5	69.0	**69**	0%
	WNA/L	8	31	**31**	0%	5	69	**69**	0%
	ANA/Q	6	134.9	**134.9**	0%	4	752.7	**752.7**	0%
	WNA/Q	5	124	**124**	0%	4	751	**751**	0%

Now let us extend our discussion to the remaining attack lists $\mathcal{A}(K,12)$, $K = 4, 8, 10$, each composed of 12 most dangerous K-node topological attacks for $K = 4, 8, 10$, generated for both networks. The discussion is based on the numerical results obtained for the measures with the quadratic component metric, i.e., to ANA/Q and WNA/Q. Since for both networks and all parameter settings, the behavior of optimal solutions obtained for the node sizes not previously considered, i.e., $K = 4, 8, 10$, is analogous to the behaviour of the optimal solutions for $K = 6$ discussed above, below we concentrate on discussing the features of the optimal solutions that depend on the attack sizes.

- When the backup controllers are not allowed, strong optimal solutions do or do not exist in more or less the same cases as for $K = 6$. The differences are observed for the case of $K = 4$ (weak attacks) where strong optimal solutions exist for both considered measures for *coronet conus* with the strict CCD limit, and for the case of $K = 10$ (severe attacks) where strong optimal solutions do not exist for both measures in in *cost266* with the loose CCD limit (however, the gaps are very small, 1.3% for ANA/Q and 3% for WNA/Q). The dependence of the sizes of optimal placements and of the gaps on K are as follows.
  - In *cost266*, the behaviour of the size of minimum optimal placements and the resulting gaps for both NA measures and both CCD limits is regular.
    For the strict CDD limit and ANA/Q the sizes in question for consecutive values of K are $(3, 5, 6, 6)$ and the corresponding gaps $(3.4\%, 9.1\%, 8.5\%, 32.0\%)$, and for WNA/Q $(3, 3, 3, 6)$ and $(6.4\%, 12.1\%, 60.0\%, 57.6\%)$, respectively.

For the loose CCD limit and ANA/Q, the respective values are $(5, 6, 9, 9)$ and $(0\%, 0\%, 0\%, 1.4\%)$, and for WNA/Q $(5, 5, 8, 9)$ and $(0\%, 0\%, 0\%, 3.0\%)$.

– For *coronet conus* the analogous values, not that regular, are as follows.
For the strict CCD limit: $(4, 2, 4, 3)$ and $(0\%, 53.4\%, 78.1\%, 71.2\%)$ for ANA/Q,
and $(3, 2, 2, 3)$ and $(0\%, 53.3\%, 85.1\%, 97.1\%)$ for WNA/Q.
For the loose CCD limit: $(4, 3, 5, 5)$ and $(13.8\%, 53.4\%, 78.1\%, 71.2\%)$ for ANA/Q,
and $(3, 3, 4, 5)$ and $(58.3\%, 32.8\%, 36.1\%, 46.3\$)$ for WNA/Q. Thus, although, the resilience against 4-node attacks achievable with only primary controllers is, as expected, better (and sometimes much better: *coronet conus*, strict CCD limit, ANA/Q) than for attacks of larger sizes, it is not so in the 10-node attacks case, where one would expect resilience in question to be the worst. The reason is that the upper bounds on the NA measures for $K = 10$ are much smaller than for smaller K (for example in *coronet conus* the UB on ANA/Q is equal to 1201.6 and 369.2 for $K = 4$ and $K = 10$, respectively.

- XXX

TABLE 7 [tables 11, 26]

cases		*cost266*				*coronet conus*			
CCD limit	*K*	*C*	*V*	UB	gap	*C*	*V*	UB	gap
strict	4	3	231.2	**239.3**	3.4%	4	1201.6	**1201.6**	0%
	6	5	123.5	**134.9**	9.1%	2	351.0	**752.7**	53.4%
	8	6	44.5	**66.3**	8.5%	4	114.9	**525.0**	78.1%
	10	6	24.0	**35.3**	32.0%	3	106.2	**369.2**	71.2%
loose	4	5	239.3	**239.3**	0%	4	1035.0	**1201.6**	13.8%
	6	6	234.9	**134.9**	0%	3	551.8	**752.7**	26.7%
	8	9	66.3	**66.3**	0%	5	371.7	**525.0**	50.1%
	10	9	34.8	**35.3**	1.4%	5	280.2	**369.2**	24.0%

TABLE 8 [tables 12, 27]

cases		*cost266*				*coronet conus*			
CCD limit	*K*	*C*	*V*	UB	gap	*C*	*V*	UB	gap
strict	4	4	239.3	**239.3**	0%	4	1201.6	**1201.6**	0%
	6	6	134.9	**134.9**	0%	4	752.7	**752.7**	0%
	8	9	66.3	**66.3**	0%	8	525.0	**525.0**	0%
	10	10	35.3	**35.3**	0%	11	369.2	**369.2**	0%
loose	4	5	239.3	**239.3**	0%	5	1201.6	**1201.6**	0%
	6	6	134.9	**134.9**	0%	4	752.7	**752.7**	0%
	8	8	66.3	**66.3**	0%	8	525.0	**525.0**	0%
	10	10	35.3	**35.3**	0%	10	369.2	**369.2**	0%

- The results for *cost266* obtained with the strict CCD limit, and for *coronet conus* with both the strict and loose CCD limits and for all attack sizes ($K = 4, 6, 8, 10$), reveal that the upper bounds (UB) on resilience levels (given by formulas (5) in Section 3) cannot be reached (i.e., strongly optimal solutions do not exist) for any of the considered availability measures when only primary controllers are used in the controllers placements. This difference, expressed as the gap between the maximum achievable value of the NA measure and its UB, is significant, of the order $10 - 60$ percent.
However, UBs are easily achievable for all NA measures (resulting in 0% gaps) when an appropriate minimum primary controllers placements is augmented by several backup controllers (which are not required to adhere the

TABLE 9 [tables 13, 28]

cases		*cost266*				*coronet conus*			
CCD limit	K	C	V	UB	gap	C	V	UB	gap
strict	4	3	211	**226**	6.4%	3	1191	**1191**	0%
	6	3	109	**124**	12.1%	2	351	**751**	53.3%
	8	3	25	**62**	60.0%	2	78	**524**	85.1%
	10	6	14	**33**	57.6%	3	10	**354**	97.1%
loose	4	5	226	**226**	0%	3	496	**1191**	58.3%
	6	5	124	**124**	0%	3	504	**751**	32.8%
	8	8	62	**62**	0%	4	335	**524**	36.1%
	10	9	32	**33**	3.0%	5	190	**354**	46.3%

TABLE 10 [tables 14, 29]

cases		*cost266*				*coronet conus*			
CCD limit	K	C	V	UB	gap	C	V	UB	gap
strict	4	4	226	**226**	0%	3	1191	**1191**	0%
	6	4	124	**124**	0%	4	751	**751**	0%
	8	8	62	**62**	0%	6	524	**524**	0%
	10	9	33	**33**	0%	11	354	**354**	0%
loose	4	5	226	**226**	0%	4	1191	**1191**	0%
	6	5	124	**124**	0%	4	751	**751**	0%
	8	8	62	**62**	0%	6	524	**524**	0%
	10	10	33	**33**	0%	10	354	**354**	0%

CCD limit). This means that the use of backup controllers is highly beneficial for increasing network resilience to attacks.

- In the case of *cost266* with the loose CCD limit, the results show that, for the attacks of smaller size (parameter K), the UB limits are achieved when using only additional primary controllers. The reason for this is not because more additional primary controllers can be added, but instead because the resilience levels provided by the minimum number of primary controllers are already close to the UB limits. In this case, allowing the additional controllers to be either primary or backup provides the same resilience level with the same total number of controllers. Nevertheless, the use of backup controllers allows for optimal solutions with a reduced number of primary controllers, which is still beneficial for the operator due to the lower operational costs of the former.
- The size each attack (parameter K) of the considered attack lists influences the achievable resilience level on the different NA measures (we provide results for both networks considering $K = 4, 6, 8, 10$). The larger the size is, the more additional controllers are required to achieve the UB limits (when allowing additional controllers of the two types) and the higher the gap becomes between the maximum achievable resilience and the UB limit (when allowing only primary controllers), making even more beneficial the use of backup controllers for increasing network resilience to attacks.
- When allowing the additional controllers to be of both types, the total number of controllers needed to reach the UB limits of network resilience are approximately equal to size K of the attacks and are slightly greater for the average network availability (ANA) measures than for the worst-case network availability (WNA) measures.
- Overall, results for the two considered network instances are similar and suggest that despite the fact that *coronet conus* is about twice as large as *cost66* (in terms of node count and geographic coverage), both networks behave similarly in terms of resilience to attacks.
- Compact formulations of the combined primary and backup controllers placement problem (CPP) are very powerful optimization tools, capable of solving the CPP to optimality for realistic network sizes in a very short time (see below).

- When allowing the additional controllers to be of both types, we were able to compute minimum optimal solutions and minimum strongly optimal solutions (when the solutions achieve the UB limits) for all cases, see definitions at the beginning of Section 4. This shows that, although in general optimal resilience levels might require a number of primary controllers higher than their minimum value, (see discussion in Section 4.3 and examples in Figures 3 and 4), this is very rare as in all reported results the maximum resilience is achieved with only additional backup controllers on top of the required minimum number of primary controllers.
- As a consequence of the previous observation, the use of non-compact formulations was an alternative valid approach to compute the optimal solutions in the considered problem instances, where the list of primary placement used as input to the formulations is composed by all placements with the minimum number of required primary controllers. However, to guarantee that the obtained solutions are optimal in the general case, the full list of feasible primary placements must be considered which might grow exponentially with the problem size. Nevertheless, non-compact formulations of CPP are always useful in cases where the list of primary controllers placements is predefined by the operator to accommodate special controller location constraints and preferences.
- In all previous observations, the results were obtained with attack lists composed by 12 attacks. Section B.2.5 of Appendix B extends the discussion to a much longer list consisting of $A = 100$ most dangerous 6-node attacks and compares the optimization results obtained for this list with those obtained for the list of $A = 12$ most dangerous 6-node attacks, applied to the *coronet conus* network. When allowing only additional primary controllers, the results are similar between the two lists, i.e., the maximum resilience has a large gap with the UB limits and is achieved with either the minimum number of primary controllers or this number plus one. On the other hand, when allowing additional controllers of both types, there are cases where the UB limit is achieved with the same number of controllers (in both lists) while in others an additional controller is required. Three properties are also introduced that, together with the fact that the formulations with the longer list are solved in short computational times (see below), allows the following conclusion: when aiming to compute strongly optimal placements, it is sufficient to optimize controllers placement with the longest list as a strongly optimal solution for this list is also strongly optimal for any of its sublists.
- In all previous observations, the results were obtained assuming that the primary controller placement obeys the strict upper bound BSC on the SC delay implied by a given maximum CCD delay. Section B.2.6 of Appendix B reports results where this bound is relaxed (5% and 10%) assuming that the operator may tolerate an increased maximum SC delay, allowing for considering primary controllers placements that are potentially more resilient to attacks. When allowing only additional primary controllers, the results show again that the UB limits are not achieved but there are significant improvements in the gaps between the obtained resilience values and the UB limits. On the other hand, when allowing both types of additional controllers, the tolerance of 10% allows the UB limits to be achieved with one less additional controller.

Importantly, all considered optimization problems resolve very quickly for both networks. Using the commercial AMPL/CPLEX 20.1 software package, running on a virtual machine with access to six logical processors (at Intel i7-9850H CPU) and up to 16 GB of RAM, we were able to achieve all optimal solutions in less than a few seconds, and in most cases in less that one second. Moreover, the computation times for *coronet conus* (including the case of the 100-element list of 6-node attacks considered in Section B.2.5) are only slightly longer than for *cost266*. For this reason we do not show computation times in the tables.

6 | FINAL REMARKS

In this paper, we presented an original comprehensive set of optimization models dealing with SDN controllers placements that admit backup controllers in addition to primary controllers for achieving increased network resilience to node-targeted attacks.

In our model, for a given controller-to-controller (CC) delay constraint, we first find a primary controllers placement that minimizes the maximum switch-to-controller (SC) delay, and then find the minimum number of primary controllers needed to achieve the previously obtained min-max SC bound delay. Next, we generate a list of most dangerous topological node-targeted attacks, and find a primary and backup controllers placement that maximizes network resilience (evaluated for four different variants of network availability measures) against the generated (and thus predefined) attack list. This is done by solving a joint primary and backup controllers placement problem for an assumed set of parameters including the optimized min-max SC bound for the assumed CC delay bound, and the minimum and maximum number of primary/backup controllers.

The paper includes an extensive numerical study illustrating the proposed optimization methodology for two well-known network instances. The numerical results show how the allowed number of primary and backup controllers influences the network resilience to attacks, and how the SC and CC delay constraints (imposed on the placements of primary controllers) affect this resilience.

The presented optimization model can be enriched with several important extensions. An example of such a (fairly simple) extension is the imposition of upper limits on the computing power of the primary and backup controllers. This processing power may be expressed in terms of signaling traffic volume, i.e., the number of new routing events that the controller can handle per time unit. Knowing about those volumes generated by individual switches, such an approach would lead to a better distribution of the processing load between the controllers. Another (difficult) extension is important when the list of potential attacks is large or even grows exponentially with the size of the network (for example when all attacks on K nodes, where K is relative close to $V/2$, are considered). This would require tackling the attack generation problem (embedded in an iterative procedure for controllers placement optimization) for finding the worst attack for a given controllers placement. Such extensions constitute an interesting topic for further research.

References

[1] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, *Security in software defined networks: A survey*, IEEE Commun. Surveys Tutorials **17** (2015), 2317–2346.

[2] R. Alvizu, G. Maier, N. Kukreja, A. Pattavina, R. Morro, A. Capello, and C. Cavazzoni, *Comprehensive survey on T-SDN: Software-defined networking for transport networks*, IEEE Commun. Surveys Tutorials **19** (2017), 2232–2283.

[3] E. Calle, S.G. Cosgaya, D. Martínez, and M. Pióro, *Solving the backup controller placement problem in SDN under simultaneous targeted attacks*, 11th International Workshop on Resilient Networks Design and Modeling (RNDM), 2019, pp. 1–7.

[4] E. Calle, D. Martínez, M. Mycek, and M. Pióro, *Resilient backup controller placement in distributed SDN under critical targeted attacks*, Int. J. Critical Infrastructure Protection **33** (2021), 100442.

[5] D. Camps-Mur, J. Gutierrez, E. Grass, A. Tzanakaki, P. Flegkas, K. Choumas, D. Giatsios, A.F. Beldachi, T. Diallo, J. Zou, P. Legg, J. Bartelt, J.K. Chaudhary, A. Betzler, J.J. Aleixendri, R. Gonzalez, and D. Simeonidou, *5G-XHaul: A novel wireless-optical sdn transport network to support joint 5G backhaul and fronthaul services*, IEEE Commun. Magazine **57** (2019), 99–105.

[6] S.G. Cosgaya, E. Calle, and J.L. Marzo, *Resilient controller location under target attacks*, 2018 20th International Conference on Transparent Optical Networks (ICTON), 2018, pp. 1–5.

[7] B. Dai, G. Xu, B. Huang, P. Qin, and Y. Xu, *Enabling network innovation in data center networks with software defined networking: A survey*, J. Network Comput. Appl. **94** (2017), 33–49.

[8] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, *A survey on the security of stateful SDN data planes*, IEEE Commun. Surveys Tutorials **19** (2017), 1701–1725.

[9] B. Heller, R. Sherwood, and N. McKeown, *The controller placement problem*, 1st workshop on Hot Topics in Software Defined Networks (HotSDN), 2012, pp. 7–12.

[10] M. Karakus and A. Durresi, *Quality of service (QoS) in software defined networking (SDN): A survey*, J. Network Comput. Appl. **80** (2017), 200–218.

[11] M. Lalou, T. Mohammed Amin, and H. Kheddouci, *The Critical Node Detection Problem in networks: A survey*, Comput. Sci. Review **28** (2018), 92–117.

[12] L. Li, N. Du, H. Liu, R. Zhang, and C. Yan, *Towards robust controller placement in software-defined networks against links failure*, 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2019, pp. 216–223.

[13] M. Mycek, M. Pióro, A. Tomaszewski, and A. de Sousa, *Optimizing primary and backup SDN controllers' placement resilient to node-targeted attacks*, 17th International Conference on Network and Service Management (CNSM 2021), 2021, pp. 397–401.

[14] S. Orlowski, M. Pióro, A. Tomaszewski, and R. Wessäly, *SNDlib 1.0 – Survivable network design library*, Networks: An Int. J. **55** (2010), 276–286.

[15] B. Pandya, S. Parmar, Z. Saquib, and A. Saxena, *Framework for securing SDN southbound communication*, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1–5.

[16] M. Pióro, M. Mycek, and A. Tomaszewski, *Network protection against node attacks based on probabilistic availability measures*, IEEE Trans. Network Service Manage. **18** (2021), 2742–2763.

[17] M. Pióro, M. Mycek, A. Tomaszewski, and A. de Sousa, *On joint primary and backup controllers placement optimization against node-targeted attacks*, 12th International Workshop on Resilient Networks Design and Modelling (RNDM 2022), 2022, pp. 1–7.

[18] M.H. Rehmani, A. Davy, B. Jennings, and C. Assi, *Software defined networks-based smart grid communication: A comprehensive survey*, IEEE Commun. Surveys Tutorials **21** (2019), 2637–2670.

[19] D.F. Rueda, E. Calle, and J.L. Marzo, *Improving the robustness to targeted attacks in software defined networks (SDN)*, 13th International Conference on Design of Reliable Communication Networks (DRCN 2017), 2017, pp. 1–8.

[20] D. Santos, A. de Sousa, and C.M. Machuca, *Combined control and data plane robustness of SDN networks against malicious node attacks*, 2018 14th International Conference on Network and Service Management (CNSM), 2018, pp. 54–62.

[21] D. Santos, A. de Sousa, and C.M. Machuca, *Robust SDN controller placement to malicious node attacks*, 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018, pp. 1–8.

[22] D. Santos, A. de Sousa, and C.M. Machuca, *The controller placement problem for robust SDNs against malicious node attacks considering the control plane with and without split-brain*, Ann. Telecommunications **74** (2019), 575–591.

[23] D. Santos, A. de Sousa, C. Mas-Machuca, and J. Rak, *Assessment of connectivity-based resilience to attacks against multiple nodes in SDNs*, IEEE Access **9** (2021), 58266–58286.

[24] D. Santos, A. de Sousa, and P. Monteiro, *Compact models for critical node detection in telecommunication networks*, Electron. Notes Discr. Math. **64** (2018), 325–334.

[25] J. Simmons, *Optical Network Design and Planning (2nd edition)*, Springer, Switzerland, 2014.

[26] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, *Physical-layer security in evolving optical networks*, IEEE Commun. Magazine **54** (2016), 110–117.

[27] A. Tomaszewski, M. Pióro, and M. Mycek, *Max-min optimization of controller placements vs. min-max optimization opf attacks on nodes in service networks*, 10th International Network Optimization Conference (INOC 2022), 2022, pp. 69–74.

[28] Y. Uematsu, S. Kamamura, H. Date, H. Yamamoto, A. Fukuda, R. Hayashi, and K. Koda, *Future nationwide optical network architecture for higher availability and operability using transport sdn technologies*, IEICE Trans. Commun. **E101.B** (2018), 462–475.

[29] C. Urrea and D. Benítez, *Software-defined networking solutions, architecture and controllers for the industrial internet of things: A review*, Sensors **21** (2021), 6585.

[30] S. Yang, L. Cui, Z. Chen, and W. Xiao, *An efficient approach to robust SDN controller placement for security*, IEEE Trans. Network Service Manage. **17** (2020), 1669–1682.

TABLE 11 Formulations' description (continued)

$\mathbb{F}6$	finding primary controllers placement minimizing the maximum SC delay under a given CC delay upper bound (13)
$\mathbb{F}7$	finding primary controllers placement minimizing the number of controllers under given SC delay and CC delay upper bounds (14) (and its maximization version $\mathbb{F}7'$)
$\mathbb{F}8$	finding the most dangerous topological attack (17)

A | FORMULATIONS OF AUXILIARY PROBLEMS

The three optimization problem formulations in this appendix are listed in Table 11.

A.1 | Optimization of Primary Controllers Placements

This section introduces two IP (integer programming) formulations that solve two aspects of the *primary controllers placement problem*. The first of them ($\mathbb{F}6$) minimizes the maximum SC delay (under the assumed CC delay upper bound BCC), while the second ($\mathbb{F}7$) minimizes the number of primary controllers required to meet the assumed upper bounds on the SC delays BSC and on the CC delays BCC.

A.1.1 | Minimizing the maximum SC delay

The following IP formulation deals with the problem of finding a primary controllers placement with the number of controllers between P' and P'' that minimizes the maximum SC delay while keeping the CC delay below the assumed upper bound BCC.

Formulation $\mathbb{F}6[P', P'', BSC, BCC]$

$$\min \; D \tag{13a}$$
$$P' \le \sum_{v\in\mathcal{V}} y_v \le P'' \tag{13b}$$
$$y_v + y_w \le 1, \quad \{v,w\} \in \mathcal{U} \tag{13c}$$
$$\sum_{w\in\mathcal{W}(v)} z_{vw} = 1, \quad v \in \mathcal{V} \tag{13d}$$
$$z_{vw} \le y_w, \quad v \in \mathcal{V}, w \in \mathcal{W}(v) \setminus \{v\} \tag{13e}$$
$$z_{vv} = y_v, \quad v \in \mathcal{V} \tag{13f}$$
$$D \ge \sum_{w\in\mathcal{W}(v)} d(v,w) z_{vw}, \quad v \in \mathcal{V} \tag{13g}$$
$$y_v \in \mathbb{B},\ v \in \mathcal{V};\ z_{vw} \in \mathbb{B},\ v \in \mathcal{V}, w \in \mathcal{W}(v) \tag{13h}$$
$$D \in \mathbb{R}. \tag{13i}$$

Above, as in formulation $\mathbb{F}1$ (and, for that matter, in $\mathbb{F}2$), binary variables y_v determine locations of primary controllers. Thus, constraint (13b) assures that the number of located controllers is between the assumed values P' and P''. Then, constraint (13c) (a counterpart of constraints (6f) and (7f)) keeps the CC delays under the upper bound BCC.

The next group of constraints determine, using binary variables z_{vw}, the assignment of switches to controllers.

Assuming that $z_{vw} = 1$ if, and only if, the switch in location v is assigned to the controller in location w, constraint (13d) assures that switch v is assigned to exactly one controller and this controller is located in the set $\mathcal{W}(v)$ (the latter assures that the SC delay of the considered switch does not exceed the assumed upper bound BSC).

Next, constraint (13e) implies that if $z_{vw} = 1$ then location w must contain a controller. Constraint (13f) in turn ensures that the switch in the location containing a controller is assigned to that controller.

Finally, constraint (13g) ensures that the value of variable D is greater than or equal to the SC delay for all switches. As this variable is minimized by objective (13a), its final value will minimize the maximum SC delay among the SC delays calculated for all switches. As a result, the optimal value of the objective function is the lowest feasible value of the upper bound BSC. □

In the above formulation, parameter BSC (the upper bound on the SC delay) is used merely to limit the cardinality of the sets $\mathcal{W}(v)$, $v \in \mathcal{V}$, and thus to limit the number of variables z_{vw}. Clearly, with no upper bound, i.e., with $BSC = d(\mathcal{G})$, $\mathcal{W}(v)$ would be equal to $\mathcal{V}$ for all node locations.

Finally, we note that the computation times required to solve 𝔽6 for both *cost266* and *coronet conus* are very short, equal to fractions of a second.

A.1.2 | Minimizing (maximizing) the number of primary controllers

The second formulation dealing with primary controllers finds a primary controllers placement with the minimum size (but not less than $P \geq 0$) required to fulfill the assumed upper bounds BSC and BCC.

Formulation $\mathbb{F}7[P, BSC, BCC]$

$$\min \ \sum_{v\in\mathcal{V}} y_v \tag{14a}$$

$$\sum_{v\in\mathcal{V}} y_v \geq P \tag{14b}$$

$$y_v + y_w \leq 1 \qquad \{v, w\} \in \mathcal{U} \tag{14c}$$

$$\sum_{w\in\mathcal{W}(v)} y_w \geq 1 \qquad v \in \mathcal{V} \tag{14d}$$

$$y_v \in \mathbb{B} \qquad v \in \mathcal{V}. \tag{14e}$$

Note that if BSC is equal to the value D^* minimized by means of formulation 𝔽6 (see (13a)), then $\mathbb{F}7[1, D^*, BCC]$ finds a minimum (in terms of size) placement of primary controllers that meets the most stringent requirement for the individual SC delays.

Finally, the following formulation finds a placement of primary controllers with the maximum size (but not greater than $P \leq V$) that meets the requirements imposed by parameters BSC and BCC.

Formulation $\mathbb{F}7'[P, BSC, BCC]$

$$\max \sum_{v\in\mathcal{V}} y_v \tag{15a}$$
$$\sum_{v\in\mathcal{V}} y_v \le P \tag{15b}$$
$$y_v + y_w \le 1 \qquad \{v,w\}\in\mathcal{U} \tag{15c}$$
$$\sum_{w\in\mathcal{W}(v)} y_w \ge 1 \qquad v\in\mathcal{V} \tag{15d}$$
$$y_v \in \mathbb{B} \qquad v\in\mathcal{V}. \tag{15e}$$

As for $\mathbb{F}6$, the computation times required to solve $\mathbb{F}7$ and $\mathbb{F}7'$ for both *cost266* and *coronet conus* are very short, equal to fractions of a second.

A.2 | Generating most dangerous topological attacks

Below we present an IP formulation $\mathbb{F}8$ that finds a K-node *topological* attack a which minimizes the total number of undirected node-pairs in the components induced by a, i.e.,

$$\sum_{c\in C(a)} \binom{V(c)}{2}, \tag{16}$$

where $\binom{V(c)}{2} := 0$ for $V(c) = 1$. Such attacks are called *topological* because their construction does not use any information about actual or potential controllers placements, only the information about the structure of the network. Note that the considered optimization problem is one of the versions of so called *critical node detection* (CND) problem considered in the graph theory [11] for undirected graphs $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.

Attacks minimizing the above quantity turn out to be the most dangerous from the point of the resilience measures considered in this paper, surpassing the effectiveness of attacks constructed on the basis of other criteria independent of the distribution of controllers, such as node degree. The intuitive reason is that the component families $C(a)$ minimizing (16) tend to have a maximum number of minimum size components, and therefore require more controllers than others to achieve a given resilience level. (For a discussion of this issue the reader is referred to [4].)

Formulation $\mathbb{F}8$ is a modified version of the formulation described in [24] (and called MILP1* there). For the purpose of $\mathbb{F}8$ we number the nodes from 1 to V (i.e., we assume that $\mathcal{V} = \{1, 2, \ldots, V\}$) and consider the set of directed node-pairs $\mathcal{H} = \{(v,w) : v, w \in \mathcal{V}, v < w\}$ that represents the set of all undirected node-pairs of graph $\mathcal{G}$, i.e., the set $\mathcal{V}^{|2|}$. We split this set into two subsets:

- $\mathcal{H}(\mathcal{E}) = \{(v,w) \in \mathcal{H} : \{v,w\} \in \mathcal{E}\}$: the set of directed node-pairs representing the set $\mathcal{E}$ of (undirect) links of graph $\mathcal{G}$
- $\mathcal{H}'(\mathcal{E}) = \{(v,w) \in \mathcal{H} : \{v,w\} \notin \mathcal{E}\}$: the set complementary to $\mathcal{H}(\mathcal{E})$ representing those node-pairs that are not connected by a link in $\mathcal{E}$.

Next, let $\mathcal{V}(v)$ be the set of nodes adjacent to node v in graph $\mathcal{G}$ (note that $|\mathcal{V}(v)|$ is equal to the node degree). For each node-pair $(v,w) \in \mathcal{H}'(\mathcal{E})$, the set $\mathcal{V}(v,w)$ is defined as $\mathcal{V}(v)$ if $|\mathcal{V}(v)| \le |\mathcal{V}(w)|$, and as $\mathcal{V}(w)$ if $|\mathcal{V}(v)| > |\mathcal{V}(w)|$.

In the introduced formulation we will use the following two sets of variables:

- binary variables a_v ($v \in \mathcal{V}$), where $a_v = 1$ if, and only if, node v is selected to be attacked
- binary variables u_{vw} ($(v,w) \in \mathcal{H}$), where $u_{vw} = 1$ if, and only if, nodes v and w belong to the same component after attack a.

The formulation of the CND problem is as follows (for its detailed explanation the reader is referred to [24]):

Formulation $\mathbb{F}8[K]$

$$\min \ \sum_{(v,w)\in\mathcal{H}} u_{vw} \tag{17a}$$

$$\sum_{v\in\mathcal{V}} a_v = K \tag{17b}$$

$$u_{vw} + a_v + a_w \geq 1 \qquad (v,w) \in \mathcal{H}(\mathcal{E}) \tag{17c}$$

$$u_{vw} \geq u_{[vt]} + u_{[tw]} + a_t - 1 \qquad (v,w) \in \mathcal{H}'(\mathcal{E}),\ t \in \mathcal{V}(v,w) \tag{17d}$$

$$a_v \in \mathbb{B} \qquad v \in \mathcal{V} \tag{17e}$$

$$u_{vw} \in \mathbb{B} \qquad (v,w) \in \mathcal{H}. \tag{17f}$$

In constraint (17d), symbol $u_{[vt]}$ denotes variable u_{vt} if $v < t$, and u_{tv} if $v > t$; the same convention concerns $u_{[tw]}$.

Note that although by definition variables u_{vw} are binary, they could be declared as non-negative continuous ($u_{vw} \in \mathbb{R}_+,\ (v,w) \in \mathcal{H}$) because in any optimal solution their values will be binary anyway. □

Let $a(1)$ be an optimal attack obtained by means of the above formulation. If we call this attack the first most dangerous attack, then the second most dangerous attack, $a(2)$, is computed by solving formulation $\mathbb{F}8[K]$ with the following additional constraint (which excludes $a(1)$ from the set of feasible solutions):

$$\sum_{v\in\mathcal{V}(a(1))} a_v \leq K - 1. \tag{18}$$

Having found $a(2)$, we add constraint

$$\sum_{v\in\mathcal{V}(a(2))} a_v \leq K - 1 \tag{19}$$

to $\mathbb{F}8[K]$. In effect, we augment formulation (17) with constraints (18) and (19) and resolve it in order to find $a(3)$. This process is continued (by adding consecutive constraints to $\mathbb{F}8[K]$ and resolving the augmented formulation) until the required set $\mathcal{A} = \{a(1), a(2), \ldots, a(A)\}$ of A most dangerous (topological) attacks is obtained. Note that in this set the attacks are ordered by non-decreasing values of the objective function (17a), i.e.,

$$\sum_{c\in C(a(1))} \binom{V(c)}{2} \leq \sum_{c\in C(a(2))} \binom{V(c)}{2} \leq \cdots \leq \sum_{c\in C(a(A))} \binom{V(c)}{2}. \tag{20}$$

Let us finally note that the above procedure is time efficient. For example, generating a 10-node attack for the *coronet conus* network on our computational platform takes 2.16 seconds on the average when the list of 12 such attacks is created, and 2.82 seconds for the corresponding list of 100 attacks.

B | NUMERICAL RESULTS

B.1 | Results for the *cost266* network

Below we present and discuss numerical results for *cost266*. The numbers assigned to node locations depicted in Figure 5 are listed in Table 12; these numbers will be used to identify the node locations when presenting the results.

TABLE 12 *cost266*: node numbers

1	Berlin	9	Milan	17	Helsinki	25	Athens	33	Amsterdam
2	Palermo	10	Vienna	18	Copenhagen	26	Bordeaux	34	Dublin
3	Seville	11	Birmingham	19	Zurich	27	Barcelona	35	Brussels
4	Cracow	12	Budapest	20	Oslo	28	Lyon	36	Munich
5	Strasbourg	13	Prague	21	Marseille	29	London	37	Glasgow
6	Paris	14	Stockholm	22	Frankfurt	30	Dusseldorf		
7	Warsaw	15	Lisbon	23	Rome	31	Zagreb		
8	Belgrade	16	Madrid	24	Hamburg	32	Sofia		

B.1.1 | Lists of attacks

For studying the *cost266* resilience to attacks we used four lists of attacks generated by the iterative procedure described in Section A.2 of Appendix A. Hence, each of them contains $A = 12$ most dangerous K-node topological attacks for $K = 4, 6, 8, 10$. For each K, the so obtained list of attacks is denoted by $\mathcal{A}(K, 12)$.

One of these lists, $\mathcal{A}(6, 12) = \{a(1), a(2), \ldots, a(12)\}$, is specified in Table 13. The sets of nodes directly affected by the attacks (i.e., $\mathcal{V}(a(i))$) are listed in the third column of the table, while for each attack $a(i)$ the overall number of node-pairs in the components of family $C(a(i))$, i.e., $\sum_{c \in C(a(i))} \binom{V(c)}{2}$, is given in the appropriate row of column 2. Note that the minimum of these numbers (124) is attained by $a(1)$, and their average (134.9) is given in the last row of column 2. Since for each attack $a(i)$ in the considered list the number of attacked nodes ($V(a(i))$) is equal to 6 and, by assumption, the weight ($w(a(i))$) is equal to $\frac{1}{A} = \frac{1}{12}$, the values of the upper bounds (UB) on the NA measures for $\mathcal{A}(6, 12)$ (calculated according to formulas (5) given in Section 3) are equal to $V - 6 = 31$ for WNA/L and ANA/L, and to 124 for WNA/Q and to 134.9 for ANA/Q. Clearly, all these bounds are valid for any primary/backup controllers placement.

B.1.2 | Input parameters

Table 14 presents the basic parameters characterizing the primary controllers placements, which are the input for the CPP formulations $\mathbb{F}1 - \mathbb{F}4$ used in the study. Two sets of parameters are considered, each calculated for one of the two selected values of the CC delay upper bound (CCD), denoted by BCC and given in the first column of the table. The first value, $BCC = 1500$, is a strict CCD bound, and the other, $BCC = 2000$, a loose one. Each set of parameters, specified in the appropriate row, was calculated as follows:

Step 1. D^* (column 2): the min-max SCD calculated by formulation $\mathbb{F}6[1, P = V, d(\mathcal{G}), BCC]$ (see Section A.1.1)

TABLE 13 *cost266*: list of topological attacks $\mathcal{A}(6,12)$

$\mathcal{A}(6,12)$	$\sum_{c\in C(a)} \binom{V(c)}{2}$	$\mathcal{V}(a)$					
$a(1)$	**124**	1	6	12	21	22	29
$a(2)$	127	1	6	12	15	21	22
$a(3)$	130	1	6	12	21	22	33
$a(4)$	132	1	6	9	12	21	22
$a(5)$	132	1	4	6	21	22	29
$a(6)$	135	1	4	6	15	21	22
$a(7)$	136	1	4	6	9	21	22
$a(8)$	138	1	4	6	21	22	33
$a(9)$	138	1	6	12	19	21	22
$a(10)$	142	1	6	7	9	21	22
$a(11)$	142	1	6	7	21	22	29
$a(12)$	143	1	4	6	19	21	22
average	**134.9**						

with no upper bound on the number of primary controllers ($P' = 1, P'' = V$, recall that there must be at least one primary controller used) and no upper bound on SCD ($BSC = d(\mathcal{G})$, where $d(\mathcal{G}) := \max\{d(v,w) : v,w \in \mathcal{V}\}$ denotes the diameter of the network graph in terms of path delays).

Step 2. P^* (column 3): the minimum number of primary controllers needed to meet the upper bound BCC on the CC delay and the upper bound $BSC = D^*$ on the SC delay specified in columns 1-2. The value of P^* is calculated by formulation $\mathbb{F}7[1, D^*, BCC]$ (see Section A.1.2).

Step 3. $|\mathcal{P}^*|$ (column 4): the number of elements $|\mathcal{P}^*|$ in the list $\mathcal{P}^*$ of all primary controllers placements with the minimum number of controllers P^* (specified in column 3) meeting the delay constraints $BSC = D^*$ (specified in column 2) and BCC (specified in column 1). This parameter and the entire list $\mathcal{P}^*$ are calculated in the way described in Section 4.3 by formulation $\mathbb{F}5[P^*, D^*, BCC, \mathcal{P}]$. The resulting two lists of primary controllers placements $\mathcal{P}^*$ are shown in Tables 21 and 23 in Section B.1.4.

Step 4. range of ASCD over $\mathcal{P}^*$ (column 5): minimum and maximum average SD delays of the placements in lists $\mathcal{P}^*$ calculated in Step 3.

In the following, a feasible primary controllers placement composed of P^* controllers, where P^* is the minimum number of primary controllers needed to meet the minimum SCD upper bound $BSC = D^*$ ($D^* = 1529$ or $D^* = 1168$, depending on the assumed BCC) will be called *minimum primary controllers placement*. Thus, the list $\mathcal{P}^*$ contains all minimum primary controllers placements ($V(p) = P^*$, $p \in \mathcal{P}^*$). As shown in column 4, for $BCC = 1500$ there are (only) 5 such (3-node) placements, while for $BCC = 2000$ there are 8 such (5-node) placements. Note that increasing the upper bound on the CC delay (from 1500 to 2000) allows for a wider dispersion of the primary controllers, thus reducing the SC delays, both in terms of their maximum (column 2) and average (column 5).

TABLE 14 *cost266*: input parameters

1	2	3	4	5
BCC	D^* ($\mathbb{F}6[1, V, d(\mathcal{G}), BCC]$)	P^* ($\mathbb{F}7[0, D^*, BCC]$)	$\lvert\mathcal{P}^*\rvert$ ($\mathbb{F}5[P^*, D^*, BCC, \mathcal{P}]$)	range of ASCD over $\mathcal{P}^*$
1500	1529	3	5	656.4 – 727.5
2000	1168	5	8	517.9 – 559.9

B.1.3 | Results for CPP — compact formulations

We start by discussing CPP solutions obtained with the compact formulations, i.e., with $\mathbb{F}1$ and $\mathbb{F}2$, when only primary controllers are used ($B = 0$) for the attacks in $\mathcal{A}(6, 12)$ described in Table 13. Such placements must obey the upper bounds on the CC and SC delays (given in columns 1 and 2 of Table 14). In the computations we used formulations $\mathbb{F}1$ and $\mathbb{F}2$ with the following parameters (implied by Table 14):

- $BCC = 1500$: $P' = P^* = 3$, $P'' = 3, 4, 5, 6$, $C = P''$, $B = 0$, $BSC = D^* = 1529$
- $BCC = 2000$: $P' = P^* = 5$, $P'' = 5, 6, 7, 8$, $C = P''$, $B = 0$, $BSC = D^* = 1168$.

Table 15 presents the optimal values of $\mathcal{M}(\mathcal{A}(6, 12))$ for all NA measures considered and both values of BCC. For each value of C (in this case, C represents the maximum number of primary controllers), the corresponding column shows the maximized value of each NA measure ("value") and the minimum number of controllers required to reach this value ("$[P]$"). Note that in each row, the last nonempty element shows the maximum value of the NA measure considered in that row, which is the value reached by a minimum optimal solution of CPP, meaning that increasing C will not improve the resilience level. (To make sure this is the case, we solved formulations $\mathbb{F}1$ and $\mathbb{F}2$ with no upper limit on the number of controllers, i.e., for $C = V$.) Next, column "UB" shows the upper bound (calculated in Section B.1.1) for the NA measure in question. Finally, column "gap" shows the gap (in percent) between the value of UB and the value of the NA measure obtained with the optimal solution. Note that the when the number in column "value" is bold, the corresponding CPP solution is minimum strongly optimal and therefore its gap is equal to 0. (The concepts of optimal, strongly optimal, and minimum (strongly) optimal CPP solutions are defined at the beginning of Section 4.)

TABLE 15 *cost266*: primary controllers placements maximizing resilience to 12 most dangerous 6-node attacks (compact formulations)

			$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$		
BCC	BSC	NA	value $[P]$	value $[P]$	value $[P]$	value $[P]$	value $[P]$	value $[P]$	UB	gap
1500	1529	ANA/L	24.3 [3]	25.2 [4]	25.6 [5]	25.7 [6]			**31**	17.1%
1500	1529	WNA/L	22 [3]	23 [4]	24 [5]	25 [6]			**31**	19.4%
1500	1529	ANA/Q	122.6 [3]	123.3 [4]	123.5 [5]				**134.9**	9.1%
1500	1529	WNA/Q	109 [3]						**124**	12.1%
2000	1168	ANA/L	–	–	29.7 [5]	30.7 [6]	30.8 [7]	**31.0 [8]**	**31**	0%
2000	1168	WNA/L	–	–	28 [5]	30 [6]	30 [6]	**31 [8]**	**31**	0%
2000	1168	ANA/Q	–	–	134.2 [5]	**134.9 [6]**			**134.9**	0%
2000	1168	WNA/Q	–	–	**124 [5]**				**124**	0%

Table 15 reveals that for $BCC = 1500$ the upper bounds on for the NA measures cannot be reached and the resulting gaps, ranging from 9.1% to 19.4% (see column "gap"), are non-negligible. The reason is that the strict CCD upper bound does not allow to efficiently spread the primary controllers in the network graph (see the remark at the end of Section 3). Another observation is that in all cases the number of primary controllers in minimum optimal solutions is not too large compared to $P^* = 3$ (the number of additional primary controllers is 3, 3, 2 and 0 for ANA/L, WNA/L,

ANA/Q and WNA/Q, respectively). Finally, the resilience levels provided by the best minimum primary controllers placements (see column $C = P^*$) are close (or even equal for WNA/Q) to the optimal ones.

Table 15, in turn, shows that for the less strict delay bound $BCC = 2000$ minimum strongly optimal solutions exist in all cases, when, respectively, 3, 3, 1 and 0 (i.e., almost the same numbers as for $BCC = 1500$) additional primary controllers are added to a minimum primary controllers placement. Apparently, now the primary controllers can be spread more efficiently, as can be seen by the small gaps between the best solutions achieved by the minimum primary controllers placements and the corresponding UB values.

TABLE 16 *cost266*: primary and backup controllers placements maximizing resilience to 12 most dangerous 6-node attacks (compact formulations)

		$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$
BCC	NA	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	ANA/L	24.3 [3/0]	29.6 [3/1]	30.5 [3/2]	30.8 [3/3]	**31.0 [3/4]**	
1500	WNA/L	22 [3/0]	28 [3/1]	29 [3/2]	30 [3/3]	**31 [3/4]**	
1500	ANA/Q	122.6 [3/0]	134.0 [3/1]	134.7 [3/2]	**134.9 [3/3]**		
1500	WNA/Q	109 [3/0]	**124 [3/1]**				
2000	ANA/L	–	–	29.7 [5/0]	30.7 [5/1]	30.8 [5/2]	**31.0 [5/3]**
2000	WNA/L	–	–	28 [5/0]	30 [5/1]	30 [5/1]	**31 [5/3]**
2000	ANA/Q	–	–	134.2 [5/0]	**134.9 [5/1]**		
2000	WNA/Q	–	–	**124 [5/0]**			

We now move on to discuss the CPP solutions obtained for the same list of attacks as before, but this time considering the use of back up controllers on top of the primary ones. As we will see, this ability makes a big difference because while the CC and SC delay upper bounds (given in columns 1 and 2 of Table 14) must still be respected by the primary controllers placements, they do not apply to the locations of backup controllers.

In the computations we used formulations $\mathbb{F}1$ and $\mathbb{F}2$ with the following parameters:

- $BCC = 1500$: $P' = P^* = 3$, $P'' = 3, 4, \ldots, 7$, $C = P''$, $B = C - P'$, $BSC = D^* = 1529$
- $BCC = 2000$: $P' = P^* = 5$, $P'' = 5, 6, 7, 8$, $C = P''$, $B = C - P'$, $BSC = D^* = 1168$.

Note that since C is the upper bound on the total number of controllers and P' is the minimum number of primary controllers, the number of backup controllers is between 0 and $B = C - P'$.

The results are shown in Table 16, which illustrates to what extent network resilience is increased using backup controllers. In the table, columns "BSC", "UB" (the same as in Table 15) and "gap" (all gaps are now equal to 0) are skipped, and in columns "C", the description "value $[P]$" is replaced by "value $[P/B]$", which refers to the maximized NA measure (as before) and to the number of primary (P) and backup (B) controllers in the optimal solution.

Comparing the cases with the same total number of controllers C in Tables 15 and 16, we see that for $BCC = 1500$, the use of backup controllers leads to strongly optimal solutions, i.e., allows the upper bounds UB to be reached for all resilience measures. The most spectacular case is WNA/Q, where adding just one backup controller on top of three primary controllers improves the resilience level from 109 to 124, i.e., to the upper bound (cf. columns "$C = 3$" in Table 15 and "$C = 4$" in Table 16). Note that adding one more primary controller (cf. columns "$C = 3$" and "$C = 4$" in Table 15) does not improve WNA/Q, and this shows that the CC delay constraints can impose strong limitation on the primary controllers placements, as far as the resilience to attacks is concerned.

In the case of $BCC = 2000$ for all NA measures and all C, the same values are obtained with C primary controllers (Table 15) as with a combination of C primary and backup controllers (Table 16). For example, for WNA/L, eight primary controllers (and no backup controllers) reach the resilience value of 31 (see column "$C = 8$" in Table 15), while

with backup controllers this value is reached using the smallest feasible number of primary controllers ($P^* = 5$) and three backup controllers (see column "$C = 8$" in Table 16). So, in this particular case backup controllers are not needed to improve resilience.

In all cases included in Table 16, the use of backup controllers allows to obtain minimum strongly optimal CPP solutions with the smallest feasible number of primary controllers, which can be beneficial for the operator due to lower operational costs of backup controllers. It should noted here that there are also cases where such minimum solutions with more than the minimum number of primary controllers exist. For example, for $BCC = 1500$ and $C = 7$ minimum strongly optimal placements (with the value of WNA/L equal to 31) exist for all combinations $[P/B] = [3/4], [4/3], [5/2], [6, 1]$.

Recall that, in general, optimal resilience levels might require a number of primary controllers higher than their minimum value P^*, as discussed in Section 4.3 (see Figures 3 and 4). However, the minimum strongly optimal solutions presented in Table 16 are in all cases composed of the minimum number of primary controllers ($P^* = 3$ for $BCC = 1500$ and $P^* = 5$ for $BCC = 2000$) with all additional controllers being of the backup type. This observation is valid in all reported results for both *cost266* and *coronet conus*, showing that the need for more primary controllers than the minimum required ones to reach optimal resilience levels is very rare.

Finally, note that in both cases (using only primary controllers in Table 15 or using primary and backup controllers in Table 16), minimum optimal solutions are achieved with less (sometimes the same) number of controllers for the Q-metric than for the L-metric . Also this observation is valid in all reported results for both the *cost266* and *coronet conus* networks.

Let us now move on to compare the CPP solutions obtained for all four attack lists $\mathcal{A}(K, 12)$, with $K = 4, 6, 8, 10$. We will discuss here the results for the ANA/Q and WNA/Q measures only, taking advantage of the fact that the results for ANA/L and WNA/L are of similar character. Of course, the results for $K = 6$ have already been shown in the previous tables.

The results for the ANA/Q are shown in Table 17 (when only primary controllers are used) and Table 18 (when primary and backup controllers are used). Table 17 shows that for the strict CCD constraint ($BCC = 1500$), the upper bounds on the resilience level cannot be reached for any value of K, no matter how many primary controllers are deployed, and the gap between the maximum achievable values of ANA/Q and its UB dramatically increases with the increase of K (from 3.4% for $K = 4$ to 32.0% for $K = 10$, see column "gap"). When the CCD bound is less strict ($BCC = 2000$), UBs are reached for $K = 4, 6, 8$ but not for $K = 10$. Not surprisingly, for both BCC cases, the number of additional controllers required to achieve the minimum optimal solution increases with the increase of the number of attacked nodes.

Table 18, in turn, shows that the use of backup controllers substantially increases the level of resilience in the case of the strict CCD upper bound $BCC = 1500$, while this effect is negligible when this bound is loosen to $BCC = 2000$ (this effect is observed for all NA measures and $K = 6$ in Tables 15 and 16). As expected, in all cases when UB on ANA/Q is not reached with primary controllers only, adding backup controllers will enable this. For $BCC = 1500$ and $K = 8$, a minimum strongly optimal solution is achieved with $P^* = 3$ primary and 6 backup controllers ($C = 9$ controllers in total), while for $K = 10$, a minimum strongly optimal solution is achieved with 3 primary and 7 backup controllers ($C = 10$ controllers in total). For $BCC = 2000$ and $K = 10$, one more controller is required (5 primary and 5 backup controllers in total) to achieve the ANA/Q upper bound (35.3).

Now let us discuss the analogous results for WNA/Q, shown in Tables 19 and 20. Roughly speaking, the observations for ANA/Q are basically valid also for WNA/Q, and the main difference is that this time when UB for WNA/Q is not reached, then the gap is larger than for ANA/Q.

In the case of the primary controllers placement (Table 19), for $BCC = 1500$ and $K = 4, 6, 8$, the maximum value

TABLE 17 *cost266*: primary controllers placements maximizing ANA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

			$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$	$C = 9$		
BCC	*BSC*	*K*	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	UB	gap
1500	1529	4	231.2 [3]							**239.3**	3.4%
1500	1529	6	122.6 [3]	123.3 [4]	123.5 [5]					**134.9**	9.1%
1500	1529	8	40.3 [3]	43.4 [4]	44.3 [5]	44.5 [6]				**66.3**	8.5%
1500	1529	10	18.6 [3]	21.6 [4]	23.1 [5]	24.0 [6]				**35.3**	32.0%
2000	1168	4	–	–	**239.3 [5]**					**239.3**	0%
2000	1168	6	–	–	134.2 [5]	**134.9 [6]**				**134.9**	0%
2000	1168	8	–	–	60.7 [5]	63.8 [6]	65.2 [7]	66.1 [8]	**66.3 [9]**	**66.3**	0%
2000	1168	10	–	–	23.1 [5]	27.3 [6]	30.3 [7]	33.3 [8]	34.8 [9]	**35.3**	1.4%

TABLE 18 *cost266*: primary and backup controllers placements maximizing ANA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

		$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$	$C = 9$	$C = 10$
BCC	*K*	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]	value [*P*/*B*]
1500	4	231.2 [3/0]	**239.2 [3/1]**						
1500	6	122.6 [3/0]	134.0 [3/1]	134.7 [3/2]	**134.9 [3/3]**				
1500	8	40.3 [3/0]	55.3 [3/1]	60.4 [3/2]	63.5 [3/3]	65.2 [3/4]	66.1 [3/5]	**66.3 [3/6]**	
1500	10	18.6 [3/0]	23.6 [3/1]	27.8 [3/2]	30.8 [3/3]	33.8 [3/4]	34.8 [3/5]	35.2 [3/6]	**35.3 [3/7]**
2000	4	–	–	**239.3 [5/0]**					
2000	6	–	–	134.2 [5/0]	**134.9 [5/1]**				
2000	8	–	–	60.7 [5/0]	63.8 [5/1]	65.5 [5/2]	**66.3 [5/3]**		
2000	10	–	–	23.1 [5/0]	27.3 [5/1]	30.3 [5/2]	33.3 [5/3]	34.8 [5/4]	**35.3 [5/5]**

of WNA/Q (much lower than UB) is already reached for the minimum number of controllers ($P^* = 3$), and only for $K = 10$ the number of controllers ($P = 6$) that provides the maximum achievable value of the WNA/Q measure (equal to 14) is greater; however, this value is still much lower than UB (equal to 33). For $BCC = 2000$ it is possible to achieve UB for $K = 4, 6, 8$ with 5, 5, 8 primary controllers, respectively; for $K = 10$ the optimal solution achievable with primary controllers (equal to 32, achieved with $P = 9$ controllers) is (slightly) less than UB. Note that for $BCC = 2000$ and $K = 4, 6$, UB is achieved with the minimum number of controllers $P^* = 5$.

When backup controllers are allowed (Table 20), for $K = 4, 6$ and $BCC = 1500$ the UB limit is reached with just one backup controller on top of $P^* = 3$ primary controllers, while for $BCC = 2000$ and $K = 4, 6$ it is achieved with the minimum number ($P^* = 5$) of primary controllers (no backup controllers are required). For $BCC = 1500$ and attacks of larger size, 5 backup controllers (on top of $P^* = 3$ primary controllers) are required for this purpose for $K = 8$, and 6 for $K = 10$. For $BCC = 2000$, the required number of backup controllers is equal to 3 ($K = 8$) and to 5 ($K = 10$).

TABLE 19 *cost266*: primary controllers placements maximizing WNA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

			$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$	$C = 9$		
BCC	*BSC*	*K*	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	value [*P*]	UB	gap
1500	1529	4	211 [3]							**226**	6.4%
1500	1529	6	109 [3]							**124**	12.1%
1500	1529	8	25 [3]							**62**	60.0%
1500	1529	10	7 [3]	10 [4]	13 [5]	14 [6]				**33**	57.6%
2000	1168	4	–	–	**226 [5]**					**226**	0%
2000	1168	6	–	–	**124 [5]**					**124**	0%
2000	1168	8	–	–	56 [5]	59 [6]	61 [7]	**62 [8]**		**62**	0%
2000	1168	10	–	–	13 [5]	23 [6]	26 [7]	29 [8]	32 [9]	**33**	3.0%

TABLE 20 *cost266*: primary and backup controllers placements maximizing WNA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

		$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 7$	$C = 8$	$C = 9$	$C = 10$
BCC	K	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	4	211 [3/0]	**226 [3/1]**						
1500	6	109 [3/0]	**124 [3/1]**						
1500	8	25 [3/0]	41 [3/1]	56 [3/2]	59 [3/3]	60 [3/4]	**62 [3/5]**		
1500	10	7 [3/0]	19 [3/1]	25 [3/2]	28 [3/3]	31 [3/4]	32 [3/5]	**33 [3/6]**	
2000	4	–	–	**226 [5/0]**					
2000	6	–	–	**124 [5/0]**					
2000	8	–	–	56 [5/0]	59 [5/1]	61 [5/2]	**62 [5/3]**		
2000	10	–	–	13 [5/0]	23 [5/1]	26 [5/2]	29 [5/3]	32 [5/4]	**33 [5/5]**

B.1.4 | Results for CPP — non-compact formulations

Now we move on to the results obtained with the non-compact formulations $\mathbb{F}3$ and $\mathbb{F}4$ (see Section 4.2) of the combined primary and backup controllers placement problem considered for the input parameters described in Table 14 and attack list $\mathcal{A}(6, 12)$ described in Table 13.

As stated in Table 14, the minimum number of primary controllers needed to fulfil the delay constraints $BCC = 1500$ and $BSC = D^* = 1529$ is equal to $P^* = 3$ (see column 3 in Table 14) and the set (list) $\mathcal{P}^*$ of all feasible placements containing $P = 3$ primary controllers has 5 elements (see column 4). This list is shown in Table 21 (where the values of the average SCD for all 5 placements are listed in column "ASCD") and illustrated in Figure 7.

TABLE 21 *cost266*: list of minimum primary controllers placements for $BCC = 1500$ and $DSC = 1529$ and their NA measures for $\mathcal{A}(6, 12)$

$\mathcal{P}^*$	ASCD	$\mathcal{V}(p)$			ANA/L	WNA/L	ANA/Q	WNA/Q
$p(1)$	656.4	8	21	24	20.9	14	113.1	78
$p(2)$	675.4	21	24	31	20.9	14	113.1	78
$p(3)$	684.3	10	21	24	20.9	14	113.1	78
$p(4)$	712.8	21	23	24	20.9	14	113.1	78
$p(5)$	727.5	23	24	26	24.3	22	122.6	109

It turns out that for $BCC = 1500$ and $BSC = 1529$ feasible placements exist for the size up to $P = 13$ — this was checked by means of formulation $\mathbb{F}7'$ (15) described in Section A.1.2. The sets of all feasible placements with a given number of controllers placements $P = 3, 4, \ldots, 13$ are denoted by $\mathcal{P}(P)$ and their sizes are given in Table 22. Note that in this table, $\mathcal{P}(3)$ denotes the list $\mathcal{P}^*$ specified in Table 21, and the last column gives the total number of feasible placements, i.e., $\sum_{P=3}^{13} |\mathcal{P}(P)| = 4864$. Recall that for each fixed placement's size P, the corresponding list $\mathcal{P}(P)$ was generated by means of the procedure (based on formulation $\mathbb{F}5$) described in Section 4.3.

TABLE 22 *cost266*: feasible primary controllers placements for $BCC = 1500$ and $BSC = 1529$

$\lvert\mathcal{P}(3)\rvert$	$\lvert\mathcal{P}(4)\rvert$	$\lvert\mathcal{P}(5)\rvert$	$\lvert\mathcal{P}(6)\rvert$	$\lvert\mathcal{P}(7)\rvert$	$\lvert\mathcal{P}(8)\rvert$	$\lvert\mathcal{P}(9)\rvert$	$\lvert\mathcal{P}(10)\rvert$	$\lvert\mathcal{P}(11)\rvert$	$\lvert\mathcal{P}(12)\rvert$	$\lvert\mathcal{P}(13)\rvert$	$\Sigma\lvert\mathcal{P}(P)\rvert$
5	49	217	572	994	1190	994	572	217	49	5	**4864**

Analogous results for $BCC = 2000$ and $BSC = 1168$ are as follows. The minimum and maximum number of controllers in a feasible primary controllers placement is equal to $P = P^* = 5$ and $P = 21$, respectively. The list

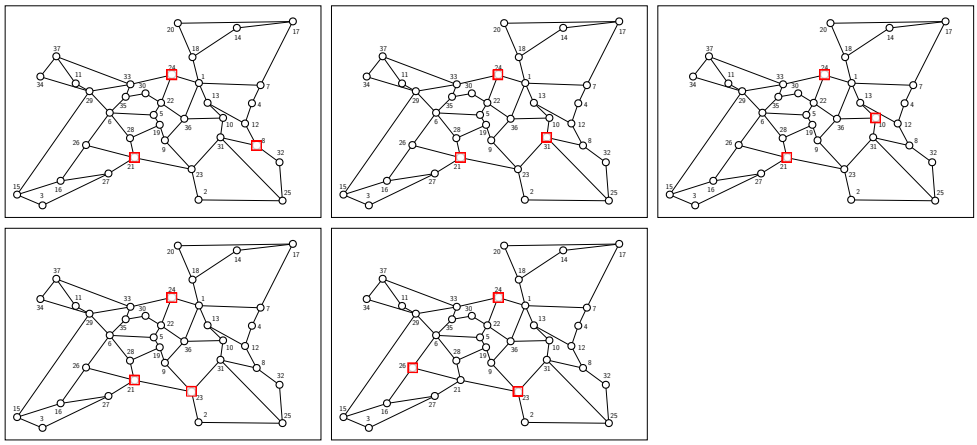

FIGURE 7 *cost266*: list of primary controllers placements $\mathcal{P}^*$ for $DCC = 1500$ and $DSC = 1529$

$\mathcal{P}(5) = \mathcal{P}^*$ of all feasible placements with $P = P^* = 5$ controllers includes 8 elements and is shown in Table 23 and illustrated in Figure 8.

TABLE 23 *cost266*: list of minimum primary controllers placements for $BCC = 2000$ and $BSC = 1168$ and their NA measures for $\mathcal{A}(6, 12)$

$\mathcal{P}^*$	ASCD	$\mathcal{V}(p)$					ANA/L	WNA/L	ANA/Q	WNA/Q
$p(1)$	517.9	8	18	21	26	35	29.7	28	134.2	124
$p(2)$	517.9	8	18	21	26	33	29.4	28	134.0	124
$p(3)$	523.3	6	8	18	21	26	26.3	23	124.1	99
$p(4)$	530.7	18	21	26	31	33	29.4	28	134.0	124
$p(5)$	535.3	6	18	21	26	31	26.3	23	124.1	99
$p(6)$	535.4	18	21	26	31	35	29.7	28	134.2	124
$p(7)$	541.4	18	21	26	29	31	27.7	24	128.8	103
$p(8)$	559.9	11	18	21	26	31	29.4	28	134.0	124

Table 24, a counterpart of Table 22, shows the sizes of the lists of feasible placements with a fixed number of elements. Note that for $P = 10, 11, \ldots, 15$, the actual number of placements is not shown because the upper bound (10 000) on the number of generated placements assumed in the calculations was reached. In fact, in these cases the computation times needed to reach the upper bound were excessive, of the order od tens of hours. This shows that in the case when only primary controllers are installed, non-compact formulations may be ineffective if all feasible primary controllers placements have to be considered to ensure optimal CPP solutions.

However, as we already know, the use of the full list of feasible controllers placements is in general not necessary since it can be possible to achieve the exact optima of CPP (in terms of maximizing the resilience levels) using only the list $\mathcal{P}^*$ of (minimum) feasible primary controllers placements. Moreover, the overall number of controllers ($C = P^* + B$) required to reach the optimal solutions can also be minimized in this way. This phenomenon, detected using compact CPP formulations, is observed in all cases considered in Section B.1.3, and illustrated in Tables 15-20.

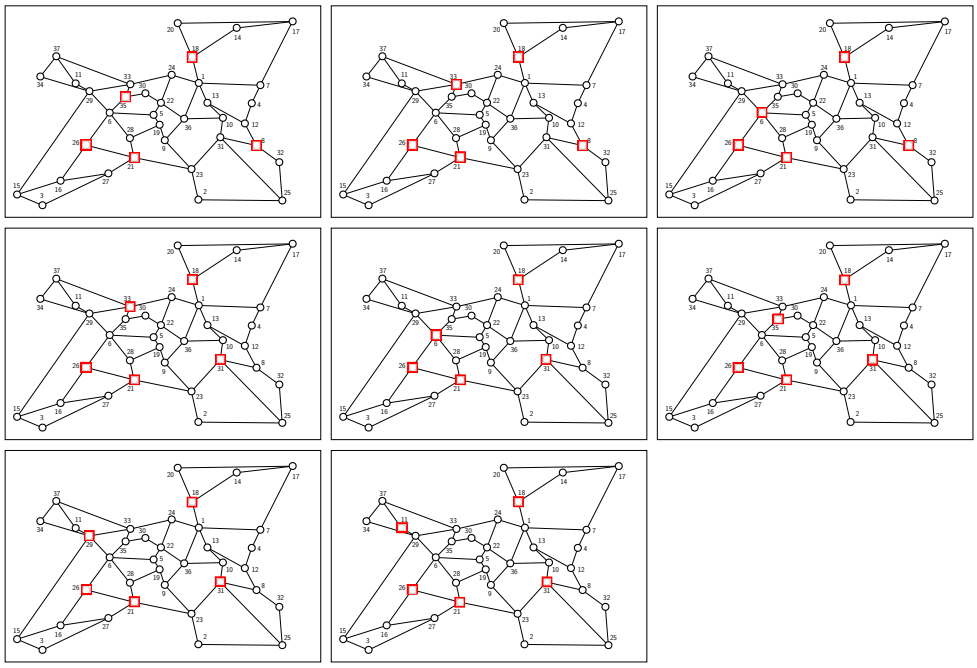

FIGURE 8 *cost266*: list of primary controllers placements $\mathcal{P}^*$ for $DCC = 2000$ and $BSC = 1168$

TABLE 24 *cost266*: feasible primary controllers placements for $BCC = 2000$ and $BSC = 1168$

$\lvert\mathcal{P}(5)\rvert$	$\lvert\mathcal{P}(6)\rvert$	$\lvert\mathcal{P}(7)\rvert$	$\lvert\mathcal{P}(8)$	$\lvert\mathcal{P}(9)\rvert$	$\lvert\mathcal{P}(10)\rvert$	$\lvert\mathcal{P}(11)\rvert$	$\lvert\mathcal{P}(12)\rvert$	$\lvert\mathcal{P}(13)\rvert$
8	112	734	2990	8477	> 10 000	> 10 000	> 10 000	> 10 000
$\lvert\mathcal{P}(14)\rvert$	$\lvert\mathcal{P}(15)\rvert$	$\lvert\mathcal{P}(16)\rvert$	$\lvert\mathcal{P}(17)\rvert$	$\lvert\mathcal{P}(18)\rvert$	$\lvert\mathcal{P}(19)\rvert$	$\lvert\mathcal{P}(20)\rvert$	$\lvert\mathcal{P}(21)\rvert$	$\Sigma\lvert\mathcal{P}(P)\rvert$
> 10 000	> 10 000	7994	2939	800	152	18	1	**> 84 225**

Note that both lists $\mathcal{P}^*$ are quite short: list $\mathcal{P}(3)$ in Table 22 consists of 5 placements, and list $\mathcal{P}(5)$ in Table 24 consists of 8 placements. Thanks to this, they can be generated in just a few seconds and then used for different values of parameters C, B', B'' in formulations $\mathbb{F}3$ and $\mathbb{F}4$. Moreover, the number of binary variables u_p, $p \in \mathcal{P}^*$, becomes very small and this leads to very short computation times of the resulting CPP instances. The results of CPP optimization assuming the two lists under consideration are discussed below.

Table 25 shows the solutions of CPP for the maximum CC delay $BCC = 1500$ and the corresponding min-max SC delay $BSC = 1529$, and the two settings indicated in column 1:

- "S" (single): list $\mathcal{P}$ contains only one element, namely the first placement in $\mathcal{P}(3)$, i.e., placement $p(1)$ in Table 21
- "F" (full): the full (5-element) list $\mathcal{P}(3)$ of allowable placements is assumed.

In Table 25, the columns starting with the third show the values of the NA measures optimized for increasing values of B (recall that B is the maximum allowable number of backup controllers). Note that the results are presented up to the value of B for which the upper bound on the value of the NA measure is achieved. (Recall that for ANA/L, WNA/L, ANA/Q, and WNA/Q these bounds are equal to 31, 31, 134.9 and 124, respectively.)

TABLE 25 *cost266*: primary and backup controllers placements optimization for $BCC = 1500$ parameters: $B = 0, 1, \ldots, 5$, $\mathcal{P} = \mathcal{P}(3)$, $\mathcal{A} = \mathcal{A}(6, 12)$ (non-compact formulations)

		B=0	B=1	B=2	B=3	B=4	B=5	UB
S	ANA/L	20.9	26.2	29.6	30.5	30.8	**31.0**	**31**
S	WNA/L	14	22	28	29	30	**31**	**31**
S	ANA/Q	113.1	124.5	134.0	134.7	**134.9**		**134.9**
S	WNA/Q	78	109	**124**				**124**
F	ANA/L	24.3	29.6	30.5	30.8	**31.0**		**31**
F	WNA/L	22	28	29	30	**31**		**31**
F	ANA/Q	122.6	134.0	134.7	**134.9**			**134.9**
F	WNA/Q	109	**124**					**124**

Looking at the third column ("$B = 0$") and the four rows marked with "S" in Table 25, we notice that the levels of resilience to the attacks under consideration provided by the assumed primary controllers placement $p(1) \in \mathcal{P}^*(3)$ (recall that $p(1)$ has the minimum average SC delay equal to 656.4 among the placement in $\mathcal{P}^*(3)$, see row $p(1)$ in Table 21) without backup controllers are substantially lower than the respective upper bounds $31, 31, 134.9, 124$. However, when the full list $\mathcal{P}(3)$ is considered, then the resilience levels are improved, as illustrated by the four rows marked with "F". It turns out that for all four NA measures the best result in terms of maximum resilience is attained for the last placement on the list, i.e., for $p(5)$ with $\mathcal{V}(p(5)) = \{23, 24, 26\}$ and ASCD equal to 727.5. The gain in resilience (as compared to the "S" results) can be significant, for example equal to 57.1% for WNA/L and 28.4% for WNA/Q, but is achieved on the expense of the increase in ASCD by 10.8%.

However, as shown in the subsequent columns, adding backup controllers gradually improves the resilience levels to finally reach the upper bounds on the NA measures. In the "S" case, the consecutive resilience bounds are achieved when 5, 5, 4 and 2, respectively, backup controllers are added. In the "F" case, these bounds are achieved with a smaller number of backup controllers, 4, 4, 3 and 1, respectively.

TABLE 26 *cost266*: primary and backup controllers placements optimization for $BCC = 2000$ parameters: $B = 0, 1, \ldots, 5$, $\mathcal{P} = \mathcal{P}(5)$, $\mathcal{A} = \mathcal{A}(6, 12)$ (non-compact formulations)

	NA	B=0	B=1	B=2	B=3	B=4	UB
S	ANA/L	29.4	30.3	30.7	30.8	**31.0**	**31**
S	WNA/L	28	28	30	30	**31**	**31**
S	ANA/Q	134.0	134.7	**134.9**			**134.9**
S	WNA/Q	**124**					**124**
F	ANA/L	29.7	30.7	30.8	**31.0**		**31**
F	WNA/L	28	30	30	**31**		**31**
F	ANA/Q	134.2	**134.9**				**134.9**
F	WNA/Q	**124**					**124**

The results for the second value of the maximum CC delay $BCC = 2000$ are shown in Table 26, which has the same layout as the previous table. It turns out that for the case "$B = 0$" and "F", the first primary controllers placement

($p(1)$) in the assumed list $\mathcal{P}(5)$ (see Table 23) is optimal for WNA/L and WNA/Q, and the last placement $p(8)$ is optimal for ANA/L and ANA/Q (but with negligible improvement with respect to $p(1)$). An additional observation is that for WNA/Q the upper bound on the level of resilience is achieved already with the primary controllers placement, so no backup controllers are required.

Note also that now the number of backup controllers needed to reach the upper bounds on different NA measures is smaller than in the case of $BCC = 1500$ considered in Table 25. These differences are due to the increased number of primary controllers which is equal to 5 with respect to the previous case, which requires 3 primary controllers.

Let us finally note that the results presented in Tables 25 and 26 in the "F" case are the same as the corresponding presented in Table 16. This was, of course, expected, since all primary controllers placements used in the optimal solutions shown in Table 16 contain the minimum number of controllers P^*, and all feasible primary controllers placements composed of P^* controllers are included in the respective lists $\mathcal{P}^*(3)$ and $\mathcal{P}^*(5)$. More specifically, the entries in column "$B = 0$" and rows "F" of Table 25 are the same as the ones given in column "$C = 3$" for $BCC = 1500$ in Table 16, and the numbers in column "$B = 0$" and rows "F" of Table 26 are the same as the ones given in column "$C = 5$" for $BCC = 2000$ in Table 16. Considering rows "F" for the cases with $B > 0$ it can be seen that the entries in both Table 25 and Table 26 are the same as the corresponding entries in the columns C in Table 16, were $C = 3 + B$ for $BCC = 1500$ and $C = 5 + B$ for $BCC = 2000$.

Since the above observation is also valid for other attack sizes ($K = 4, 8, 10$), we omit the presentation of the results of non-compact formulations $\mathbb{F}3$ and $\mathbb{F}4$ for the cases considered in Tables 18 and 20.

B.2 | Results for the *coronet conus* network

Below we present and discuss numerical results for *coronet conus*, a network instance two times larger than *cost266*. The numbers assigned to node locations depicted in Figure 6 are listed in Table 27. As before, these numbers will be used to identify the node locations when presenting the results.

TABLE 27 *coronet conus*: node numbers

1	Abilene	16	Cincinnati	31	Long Island	46	Orlando	61	Santa Barbara
2	Albany	17	Cleveland	32	Los Angeles	47	Philadelphia	62	Scranton
3	Albuquerque	18	Columbus	33	Louisville	48	Phoenix	63	Seattle
4	Atlanta	19	Dallas	34	Memphis	49	Pittsburgh	64	Spokane
5	Austin	20	Denver	35	Miami	50	Portland	65	Springfield
6	Baltimore	21	Detroit	36	Milwaukee	51	Providence	66	St Louis
7	Baton Rouge	22	El Paso	37	Minneapolis	52	Raleigh	67	Syracuse
8	Billings	23	Fresno	38	Nashville	53	Richmond	68	Tallahassee
9	Birmingham	24	Greensboro	39	New Orleans	54	Rochester	69	Tampa
10	Bismarck	25	Hartford	40	New York	55	Sacramento	70	Toledo
11	Boston	26	Houston	41	Newark	56	Salt Lake City	71	Tucson
12	Buffalo	27	Jacksonville	42	Norfolk	57	San Antonio	72	Tulsa
13	Charleston	28	Kansas City	43	Oakland	58	San Diego	73	Washington DC
14	Charlotte	29	Las Vegas	44	Oklahoma City	59	San Francisco	74	West Palm Beach
15	Chicago	30	Little Rock	45	Omaha	60	San Jose	75	Wilmington

B.2.1 | Lists of attacks

As in the case of *cost266*, to test the resilience of *coronet conus* to attacks we generated four lists of 12 most dangerous topological attacks $\mathcal{A}(6,K)$ ($K = 4, 6, 8, 10$). One of them, $\mathcal{A}(6,12)$, is specified in Table 28 (which is analogous to Table 13).

TABLE 28 *coronet conus*: 12 most dangerous 6-node topological attacks

$\mathcal{A}(6,12)$	$\sum_{c\in C(a)} \binom{V(c)}{2}$	$\mathcal{V}(a)$					
$a(1)$	**751**	15	19	22	24	33	40
$a(2)$	751	15	19	22	24	33	75
$a(3)$	751	15	19	22	33	53	75
$a(4)$	751	15	19	22	33	42	53
$a(5)$	751	15	19	22	33	42	73
$a(6)$	751	15	19	22	33	52	73
$a(7)$	753	15	19	22	33	40	53
$a(8)$	753	15	19	22	33	52	53
$a(9)$	753	15	19	22	24	33	42
$a(10)$	753	15	19	22	33	73	75
$a(11)$	757	15	19	22	24	33	52
$a(12)$	757	15	19	22	33	40	73
average	**752.7**						

Now, the average of the values in column 2, and hence the upper bound on the maximum value of the ANA/Q measure, is equal to 752.7 (for any primary/backup controllers placement). Moreover, the upper bound on WNA/Q imposed by attack $a(1)$ (and, for that matter, attacks $p(2), p(3), \ldots, p(6)$) is equal 751, and $V - 6 = 69$ is the upper bound for both ANA/L and WNA/L.

B.2.2 | Input parameters

TABLE 29 *coronet conus*: input parameters

1	2	3	4	5
BCC	D^* ($\mathbb{F}6[1, V, d(\mathcal{G}), BCC]$)	P^* ($\mathbb{F}7[0, D^*, BCC]$)	$\lvert\mathcal{P}^*\rvert$ ($\mathbb{F}5[P, BSC, BCC, \mathcal{P}]$)	range of ASCD over $\mathcal{P}^*$
1500	3094	2	1	1833
2500	2174	3	2	1241-1272

Table 29 contains the results analogous to those shown in Table 14 for *cost266*. This time we consider the CCD upper bounds (BCC) equal to 1500 and 2500 while the rest of the parameters used in formulation $\mathbb{F}6$ remain the same. Note that, relative to the corresponding values for *cost266* shown in Table 14, the number of controllers required to achieve the minimum of the maximum SCD (given in column 2) has decreased (see column 3) from $P = 5$ to $P = 2$ ($BCC = 1500$), and from $P = 8$ to $P = 3$ ($BCC = 2500$). Also, the lists of all feasible primary controllers placements

composed of P^* controllers with the SCD delay not exceeding D^* are extremely short. As shown in column 4, there is only one such placement for $BCC = 1500$, and two placements for $BCC = 2500$. Like in the *cost266* case, with the increased allowable CC delay (now equal to 2500), the primary controllers can be spread more efficiently and thus reduce the SC delays, both in terms of D^* (column 2) and the average SCD (column 5).

B.2.3 | Results for CPP — compact formulations

Table 30 (analogous to Table 15 for *cost266*) shows the results of solving CPP for the case when backup controllers are not used ($B = 0$), so only primary controllers are deployed. The resulting primary controllers placements must obey the upper bounds on the CC and SC delays (given in columns 1 and 2 of Table 29), and maximize the assumed NA measure for the attacks in $\mathcal{A}(6, 12)$ (listed in Table 28). In the computations the following parameters (implied by Table 29) were used in formulations $\mathbb{F}1$ and $\mathbb{F}2$:

- $BCC = 1500$: $P' = P^* = 2$, $P'' = 2$, $C = P''$, $B = 0$, $BSC = D^* = 3094$
- $BCC = 2500$: $P' = P^* = 3$, $P'' = 3, 4$, $C = P''$, $B = 0$, $BSC = D^* = 2174$.

As in the case of Table 15, in each row the last nonempty element shows the value of the NA measure achieved by the minimum optimal solution. (As for *cost266*, to be sure about that we first solved $\mathbb{F}1$ and $\mathbb{F}2$ with no upper bound on the number of controllers.) The results shown in the table reveal that for $BCC = 1500$, the use of primary controllers only results in poor, as compared to the upper bounds given in column "UB", resilience levels. Moreover, the maximum achievable resilience levels for all four measures (27 for ANA/L and WNA/L and 351 for ANA/Q and WNA/Q are obtained already with the minimum number of controllers $P = P^* = 2$, which shows that the CC delay bound equal to 1500 is really strict and does not allow primary controllers to be properly spread for better resilience to the considered attacks. (Recall that the same effect, but to a lesser extent, is observed for *cost266* in Table 15.)

With the less strict CCD bound, i.e., $BCC = 2500$, the resilience levels are visibly increased for all measures, yet, contrary to the *cost266* case, they are still quite far from the upper bounds. Also now the maximum resilience levels for ANA?Q and WNA/Q are achieved with the minimum feasible number of controllers $P = P^* = 3$, but for ANA/L and WNA/L this requires $P = 4$ controllers (yet, the additional controller results in a marginal improvement). Note that in the case of *cost266*, the increased BCC allows for reaching the upper bounds on resilience levels in all cases (see Table 15).

TABLE 30 *coronet conus*: primary controllers placements maximizing resilience to 12 most dangerous 6-node attacks (compact formulations)

			$C = 2$	$C = 3$	$C = 4$		
BCC	BSC	NA	value [P]	value [P]	value [P]	UB	gap
1500	3094	ANA/L	27.0 [2]			**69**	60.8%
1500	3094	WNA/L	27 [2]			**69**	60.8%
1500	3094	ANA/Q	351.0 [2]			**752.7**	53.4%
1500	3094	WNA/Q	351 [2]			**751**	53.3%
2500	2174	ANA/L	–	47.5 [3]	48.5 [4]	**69**	29.7%
2500	2174	WNA/L	–	45 [3]	46 [4]	**69**	33.3%
2500	2174	ANA/Q	–	551.8 [3]		**752.7**	26.7%
2500	2174	WNA/Q	–	504 [3]		**751**	32.9%

Next, let us consider Table 31, which (as its *cost266* counterpart Table 16) illustrates the gain achieved from using backup controllers for the considered list of twelve 6-node attacks. Now, the following parameters were used in

TABLE 31 *coronet conus*: primary and backup controllers placements maximizing resilience to 12 most dangerous 6-node attacks (compact formulations)

		$C = 2$	$C = 3$	$C = 4$	$C = 5$
BCC	NA	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	ANA/L	27.0 [2/0]	47.5 [2/1]	68.0 [2/2]	**69.0 [2/3]**
1500	WNA/L	27 [2/0]	45 [2/1]	68 [2/2]	**69 [2/3]**
1500	ANA/Q	351.0 [2/0]	551.8 [2/1]	**752.7 [2/2]**	
1500	WNA/Q	351 [2/0]	504 [2/1]	**751 [2/2]**	
2500	ANA/L	–	47.5 [3/0]	68.0 [3/1]	**69.0 [3/2]**
2500	WNA/L	–	45 [3/0]	68 [3/1]	**69 [3/2]**
2500	ANA/Q	–	551.8 [3/0]	**752.7 [3/1]**	
2500	WNA/Q	–	504 [3/0]	**751 [3/1]**	

formulations $\mathbb{F}1$ and $\mathbb{F}2$:

- $BCC = 1500$: $P' = P^* = 2$, $P'' = 2, 3, \ldots, 6, 8$, $C = P''$, $B = C - P'$, $BSC = D^* = 3094$
- $BCC = 2500$: $P' = P^* = 3$, $P'' = 3, 4, \ldots, 6, 8$, $C = P''$, $B = C - P'$, $BSC = D^* = 2174$.

Comparing the cases with the same total number of controllers C in Tables 31 and 30, we notice that now the use of backup controllers significantly improves the resilience levels not only for the strict CCD, as for *cost266*, but also for the loose CCD. In fact, even with a relatively small number of backup controllers, the upper bounds on resilience measures are achieved in all cases.

TABLE 32 *coronet conus*: primary controllers placements maximizing ANA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

			$C = 2$	$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 8$		
BCC	BSC	K	value $[P]$	value $[P]$	value $[P]$	value $[P]$	value $[P]$	value $[P]$	UB	gap
1500	3094	4	465.0 [2]	1201.3 [3]	**1201.6 [4]**				**1201.6**	0%
1500	3094	6	351.0 [2]						**752.7**	53.4%
1500	3094	8	100.6 [2]	114.8 [3]	114.9 [4]				**525.0**	78.1%
1500	3094	10	105.3 [2]	106.2 [3]					**369.2**	71.2%
2500	2174	4	–	1034.8 [3]	1035.0 [4]				**1201.6**	13.8%
2500	2174	6	–	551.8 [3]					**752.7**	26.7%
2500	2174	8	–	259.9 [3]	358.9 [4]	371.7 [5]			**525.0**	50.1%
2500	2174	10	–	169.8 [3]	275.9 [4]	280.2 [5]			**369.2**	24.0%

TABLE 33 *coronet conus*: primary and backup controllers placements maximizing ANA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

		$C = 2$	$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 8$	$C = 9$	$C = 10$	$C = 11$
BCC	K	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	4	465.0 [2/0]	1201.3 [2/1]	**1201.6 [2/2]**						
1500	6	351.0 [2/0]	551.8 [2/1]	**752.7 [2/2]**						
1500	8	100.6 [2/0]	274.9 [2/1]	441.5 [2/2]	524.0 [2/3]	524.8 [2/4]	**525.0 [2/6]**			
1500	10	105.3 [2/0]	212.1 [2/1]	284.4 [2/2]	347.4 [2/3]	354.1 [2/4]	363.6 [2/6]	367.8 [2/7]	368.7 [2/8]	**369.2 [2/9]**
2500	4	–	1034.8 [3/0]	1201.3 [3/1]	**1201.6 [3/2]**					
2500	6	–	551.8 [3/0]	**752.7 [3/1]**						
2500	8	–	259.9 [3/0]	426.5 [3/1]	512.1 [3/2]	524.8 [3/3]	**525.0 [3/5]**			
2500	10	–	165.8 [3/0]	282.7 [3/1]	348.3 [3/2]	354.9 [3/3]	364.4 [3/5]	368.7 [3/6]	**369.2 [3/7]**	

Tables 32 and 33 (analogous to Tables 17 and 18 for *cost266*) extend the results for the ANA/Q measure given

TABLE 34 *coronet conus*: primary controllers placements maximizing WNA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

			$C = 2$	$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 8$		
BCC	BSC	K	value [P]	value [P]	value [P]	value [P]	value [P]	value [P]	UB	gap
1500	3094	4	351 [2]	**1191 [3]**					**1191**	0%
1500	3094	6	351 [2]						**751**	53.3%
1500	3094	8	78 [2]						**524**	85.1%
1500	3094	10	0 [2]	10 [3]					**354**	97.1%
2500	2174	4	–	496 [3]					**1191**	58.3%
2500	2174	6	–	504 [3]					**751**	32.8%
2500	2174	8	–	190 [3]	335 [4]				**524**	36.1%
2500	2174	10	–	93 [3]	184 [4]	190 [5]			**354**	46.3%

TABLE 35 *coronet conus*: primary and backup controllers placements maximizing WNA/Q for 12-attack lists for $K = 4, 6, 8, 10$ (compact formulations)

		$C = 2$	$C = 3$	$C = 4$	$C = 5$	$C = 6$	$C = 8$	$C = 9$	$C = 10$	$C = 11$
BCC	K	value [P/B]	value [P/B]	value [P/B]	value [P/B]	value [P/B]	value [P/B]	value [P/B]	value [P/B]	value [P/B]
1500	4	351 [2/0]	**1191 [2/1]**							
1500	6	351 [2/0]	504 [2/1]	**751 [2/2]**						
1500	8	78 [2/0]	244 [2/1]	420 [2/2]	514 [2/3]	**524 [2/4]**				
1500	10	0 [2/0]	169 [2/1]	218 [2/2]	316 [2/3]	326 [2/4]	343 [2/6]	348 [2/7]	353 [2/8]	**354 [2/9]**
2500	4	–	496 [3/0]	**1191 [3/1]**						
2500	6	–	504 [3/0]	**751 [3/1]**						
2500	8	–	190 [3/0]	361 [3/1]	420 [3/2]	**524 [3/3]**				
2500	10	–	93 [3/0]	222 [3/1]	326 [3/2]	336 [3/3]	348 [3/5]	353 [3/6]	**354 [3/7]**	

in Tables 30 and 31 to the lists of 12 attacks generated for $K = 4, 8, 10$.

Analyzing Table 32 we first of all notice that for the 4-node (i.e., the least severe) attacks, the upper bound on ANA/Q is reached already with $C = 4$ primary controllers for $BCC = 1500$, while for $BCC = 2500$ it cannot be reached even with $C = 8$ primary controllers. This, somewhat untypical, behavior is caused by the SC delay upper bound, which is apparently too strict. The network resilience to more severe attacks ($K = 8, 10$) achieved without backup controllers behaves more or less as in the $K = 6$ case. The provided resilience levels are low, especially for $K = 8, 10$. Note that for these attacks and $BCC = 2500$, increasing the number of primary controllers from 3 (the minimum) to 4 (and then to 5) substantially improves the resilience levels for ANA/Q and WNA/Q.

Table 33, in turn, shows that in all cases adding backup controllers makes it possible to find strongly optimal solution, i.e, to reach the upper bounds on ANA/Q for all attack lists. (Actually, as mentioned above, for $BCC = 1500$ and $K = 4$ backup controllers are not necessary.)

Finally, Tables 34 and 35, analogous to Tables 19 and 20 for *cost266*, present the results for the WNA/Q measure. The two main observations are: (i) admitting backup controllers significantly helps to achieve the upper bound on the network resilience; (ii) for more severe attacks and $BCC = 1500$, the resilience levels achieved with only primary controllers are very poor. For example, the value of WNA/Q for $K = 8$ is equal to 78 (while its upper bound equals 524) and for $K = 10$ it is equal to 10 (while its upper bound equals 354). Also for $BCC = 2500$ these values are substantially smaller than in the ANA/Q case.

B.2.4 | Results for CPP — non-compact formulations

Below we briefly discuss the results related to application of non-compact formulations $\mathbb{F}3$ and $\mathbb{F}4$ of the combined primary and backup controllers placement problem considered for the input parameters soecified in Table 29 and the

attack list $\mathcal{A}(6,12)$ described in Table 28.

As stated in Table 29, the minimum number of primary controllers needed to fulfil the delay constraints $BCC = 1500$ and $BSC = D^* = 3094$ is equal to $P^* = 2$ (see column 3 in Table 29) and the list $\mathcal{P}^*$ of feasible placements containing $P = 2$ primary controllers has just 1 element (see column 4 in Table 29). This (one-element) list is shown in Table 36 and illustrated in Figure 9.

TABLE 36 *coronet conus*: list of minimum primary controllers placements for $BCC = 1500$ and $BSC = 3094$ and their NA measures for $\mathcal{A}(6,12)$

$\mathcal{P}(2)$	ASCD	$\mathcal{V}(p)$	ANA/L	WNA/L	ANA/Q	WNA/Q
$p(1)$	1833	19 45	27	27	351.0	351

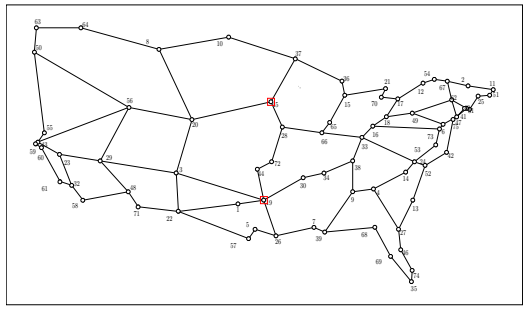

FIGURE 9 *coronet conus*: the single primary controllers placement forming list $\mathcal{P}^*$ for $BCC = 1500$ and $BSC = 3094$

Note that this unique minimum placement with $\mathcal{V}(p) = \{19, 45\}$ provides the same resilience level (equal to 27 for the linear metric and to 351 for the quadratic metric) for all attacks in $\mathcal{A}(6,12)$. This is because the controller at node 19 is always attacked and for all attacks the controller at node 45 always belongs to a surviving 27-node component with $\binom{27}{2} = 351$ node-pairs.

It turns out that for $BCC = 1500$ and $BSC = 3094$ feasible placements exist for the size of up to $P = 6$ controllers. The lists of all feasible placements $\mathcal{P}(P)$, $P = 2, 3, \ldots, 6$, with a given number of controllers and their sizes are given in Table 37. Note that in the table, $\mathcal{P}(2)$ denotes the list $\mathcal{P}^*$ specified in Table 36, and the last column gives the total number of feasible placements, i.e., $\sum_{P=2}^{6} |\mathcal{P}(P)| = 24$.

TABLE 37 *coronet conus*: feasible primary controllers placements for $BCC = 1500$ and $BSC = 3094$

$\lvert\mathcal{P}(2)\rvert$	$\lvert\mathcal{P}(3)\rvert$	$\lvert\mathcal{P}(4)\rvert$	$\lvert\mathcal{P}(5)\rvert$	$\lvert\mathcal{P}(6)\rvert$	$\Sigma\lvert\mathcal{P}(P)\rvert$
1	5	9	7	2	**24**

Analogous results for $BCC = 2500$ and $BSC = 2174$ are as follows. The minimum and maximum number of controllers in a feasible primary controllers placement is equal to $P = P^* = 3$ and $P = 15$, respectively. The list $\mathcal{P}(3) = \mathcal{P}^*$ of all feasible placements with $P = 3$ controllers includes only 2 elements and is shown in Table 23 and illustrated in Figure 10. Note that both placements of the minimum size $P = 3$ provide the same values for all NA measures under consideration.

The sizes of the lists of all feasible placements $\mathcal{P}(P)$, $P = 2, 3, \ldots, 15$, are given in Table 39. In the table, $\mathcal{P}(3)$

denotes the list $\mathcal{P}^*$ specified in Table 36; as before, the last column gives the total number of feasible placements, i.e., $\sum_{P=3}^{15} |\mathcal{P}(P)| = 7566$.

TABLE 38 *coronet conus*: list of minimum primary controllers placements for $BCC = 2500$ and $BSC = 2174$ and their NA measures for $\mathcal{A}(6, 12)$

$\mathcal{P}(3)$	ASCD	$\mathcal{V}(p)$			ANA/L	WNA/L	ANA/Q	WNA/Q
$p(1)$	1241	20	22	38	47.5	45	551.8	504
$p(2)$	1272	3	20	38	47.5	45	551.8	504

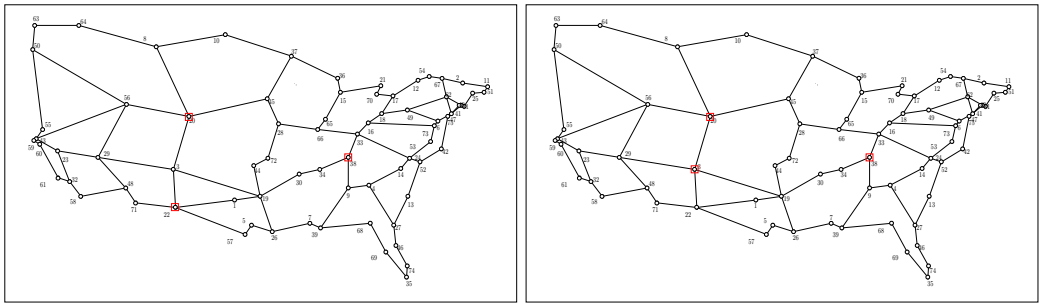

FIGURE 10 *coronet conus*: the two primary controllers placements forming list $\mathcal{P}^*$ for $BCC = 2500$ and $BSC = 2174$

TABLE 39 *coronet conus*: feasible primary controllers placements for $BCC = 2500$ and $BSC = 2174$

$\lvert\mathcal{P}(3)\rvert$	$\lvert\mathcal{P}(4)\rvert$	$\lvert\mathcal{P}(5)\rvert$	$\lvert\mathcal{P}(6)\rvert$	$\lvert\mathcal{P}(7)\rvert$	$\lvert\mathcal{P}(8)\rvert$	$\lvert\mathcal{P}(9)\rvert$
2	24	131	430	945	1464	1638
$\lvert\mathcal{P}(10)\rvert$	$\lvert\mathcal{P}(11)\rvert$	$\lvert\mathcal{P}(12)\rvert$	$\lvert\mathcal{P}(13)\rvert$	$\lvert\mathcal{P}(14)\rvert$	$\lvert\mathcal{P}(15)\rvert$	$\Sigma\lvert\mathcal{P}(P)\rvert$
1332	1178	320	87	14	1	**7566**

As in the case of *cost266* discussed in Section B.1.4, also for *coronet conus* the use of the full lists of feasible controllers placements is not necessary since the exact optima of CPP can be achieved using only the lists $\mathcal{P}^*$ of (minimum) feasible primary controllers placements. This is shown in Tables 30-35 presented in Section 4.1.

Finally, note that in order to solve CPP for the two lists of minimum primary controllers placements given in Tables 36 and 38, we could use (as for *cost266*), non-compact CPP formulations $\mathbb{F}3$ (8) and $\mathbb{F}4$ (9). However, since these two lists are extremely short, we might as well solve the simplified versions of $\mathbb{F}3$ and $\mathbb{F}4$ (described at the end of Section 4.2, where such a simplified version of $\mathbb{F}4$ is given in formulation (10)), separately for each of the primary controllers placement under consideration, and, in the case of $BCC = 2500$, simply choose the better (out of two) primary controllers placement in each of the examined cases of C.

We omit the presentation of the tables analogous to Tables 25 and 26 presented in Section B.1.4 for *cost266*. Such tables (in the "F" case) can be obtained from Table 31 in the same way as Tables 25 and 26 are obtained from Table 16.

B.2.5 | Additional results for a list of one hundred 6-node attacks

Until now, the network resilience assessment was based on attack lists consisting of $A = 12$ most dangerous K-node topological attacks for $K = 4, 6, 8, 10$. In this section, we will extend our discussion to a much longer list consisting of $A = 100$ most dangerous 6-node topological attacks and compare the optimization results obtained for this list with those obtained for the list of $A = 12$ most dangerous 6-node attacks described in Table 28. However, before presenting the numerical results, let us formulate some general properties of attack lists related to CPP.

Consider an arbitrary attack list $\mathcal{A}$ and an attack $a \in \mathcal{A}$, and define the quantities

$$S(a) := \sum_{c \in C(a)} V(c) = V - V(a) \qquad S^2(a) := \sum_{c \in C(a)} \binom{V(c)}{2} \tag{21a}$$

$$S(\mathcal{A}) := \min_{a \in \mathcal{A}} S(a) \qquad S^2(\mathcal{A}) := \min_{a \in \mathcal{A}} S^2(a). \tag{21b}$$

Using the above definitions, the upper bounds (UB) on the achievable network availability measures $\mathcal{M}(\mathcal{A})$ (see formulas (5) in Section 3) can be expressed as follows:

$$\text{WNA/L:} \quad \text{UB} = \min_{a \in \mathcal{A}} S(a) = V - \max_{a \in \mathcal{A}} V(a) \tag{22a}$$

$$\text{ANA/L:} \quad \text{UB} = \tfrac{1}{A} \sum_{a \in \mathcal{A}} S(a) = \tfrac{1}{A} \sum_{a \in \mathcal{A}} (V - V(a)) \tag{22b}$$

$$\text{WNA/Q:} \quad \text{UB} = \min_{a \in \mathcal{A}} S^2(a) \tag{22c}$$

$$\text{ANA/Q:} \quad \text{UB} = \tfrac{1}{A} \sum_{a \in \mathcal{A}} S^2(a). \tag{22d}$$

Note that the assumed attack weights ($w(a) = \frac{1}{A}$, $a \in \mathcal{A}$) do not affect the generality of our considerations.

The following properties apply to strongly optimal controllers placements (i.e., placements achieving the upper bound of a given NA measure) and minimum strongly optimal placements (i.e., strongly optimal placements with the minimum number of controllers).

Property 1 *Any strongly optimal placement for an attack list $\mathcal{A}$ and a given NA measure (one of ANA/L, WNA/L, ANA/Q, WNA/Q) is also strongly optimal for*

- *all sublists of $\mathcal{A}$, if NA = ANA/L or NA=ANA/Q*
- *all those sublists of $\mathcal{A}$ that contain at least one attack a with $S(a) = S(\mathcal{A})$, if NA=WNA/L*
- *all those sublists of $\mathcal{A}$ that contain at least one attack a with $S^2(a) = S^2(\mathcal{A})$, if NA=WNA/Q.*

Note that for all NA measures, the minimum strongly optimal placement for $\mathcal{A}$ is not necessarily the minimum strongly optimal placement for proper sublists of $\mathcal{A}$.

Property 2 *When all attacks in $\mathcal{A}$ are of the same size K, i.e., when $V(a) = K$, $a \in \mathcal{A}$, then also in the case of NA=WAN/L any strongly optimal placement for $\mathcal{A}$ is strongly optimal for all its sublists. This is implied by the second item in Property 1.*

Property 3 *Any strongly optimal placement for $\mathcal{A}$ and ANA/L is also strongly optimal for $\mathcal{A}$ and all its sublists for WNA/L; the same holds for ANA/Q and WNA/Q. In both cases, the minimality of the placement for ANA does not necessarily imply its minimality for WNA.*

Now consider the list $a(1), a(2), \ldots, a(100)$ of $A = 100$ most dangerous 6-node attacks generated using the attack generation procedure described in Section A.2. This list will be denoted by $\mathcal{A}(6, 100)$ and called *long list* in the following. Note that the first twelve attacks in $\mathcal{A}(6, 100)$, i.e., $a(1), a(2), \ldots, a(12)$, form the list $\mathcal{A}(6, 12)$ described in Table 28. In the following, this list will be called *short list*. By construction, the attacks in both lists are ordered by a non-decreasing total number of node-pairs in component families induced by successive attacks.

Thus, by Property 1, for each of the considered measures ANA/L, WNA/L, ANA/Q, WNA/Q, each strongly optimal placement for $\mathcal{A}(6, 100)$ is strongly optimal also for $\mathcal{A}(6, 12)$. The upper bounds on ANA/L, WNA/L, ANA/Q and WNA/Q for $\mathcal{A}(6, 100)$ are equal to 69, 69, 774.9 and 751, respectively. Thus, for the long list $\mathcal{A}(6, 100)$ the upper bounds for ANA/L, WNA/L and WNA/Q are the same as for $\mathcal{A}(6, 12)$. However, in the case of ANA/Q, the upper bound for $\mathcal{A}(6, 100)$ (equal to 774.9) is greater than the upper bound for $\mathcal{A}(6, 12)$, which is 752.7 (see Table 28); this difference is due to the increasing values of $S(a(i))$ in the considered lists of attacks: from $S(a(1)) = 751$ to $S(a(12)) = 757$ in both lists, and further from $S(a(13)) = 758$ to $S(a(100)) = 796$ in the long list.

In Tables 40 and 41 we compare the achieved resilience levels for the two considered lists of 6-node attacks for ANA/Q and WNA/Q, both values of BCC (1500 and 2500), and the corresponding values of BSC (3094 and 2174). The results for the short list $\mathcal{A}(6, 12)$ are taken from the appropriate rows in Tables 30 and 31, while their equivalents for the long list $\mathcal{A}(6, 100)$ were calculated (by means formulations $\mathbb{F}1$ and $\mathbb{F}2$) for the same range of the number of controllers used in the placements. Tables 40 and 41 are constructed analogously to Tables 30 and 31, with one additional column "A" whose elements identify the number of attacks in the list ($A = 12$ for $\mathcal{A}(6, 12)$, and $A = 100$ for $\mathcal{A}(6, 100)$) considered in a given row.

TABLE 40 *coronet conus*: primary controllers placements maximizing resilience to $\mathcal{A}(6, 12)$ and $\mathcal{A}(6, 100)$

				$C = 2$	$C = 3$	$C = 4$		
BCC	BSC	NA	A	value [P]	value [P]	value [P]	UB	gap
1500	3094	ANA/Q	12	351.0 [2]			**752.7**	53.4%
1500	3094	ANA/Q	100	394.7 [2]			**774.9**	49.1%
1500	3094	WNA/Q	12	351 [2]			**751**	53.3%
1500	3094	WNA/Q	100	351 [2]			**751**	53.3%
2500	2174	ANA/Q	12	–	551.8 [3]		**752.7**	26.7%
2500	2174	ANA/Q	100	–	555.9 [3]		**774.9**	28.3%
2500	2174	WNA/Q	12	–	504 [3]		**751**	32.9%
2500	2174	WNA/Q	100	–	354 [3]	390 [4]	**751**	48.1%

Table 40 shows that in all cases except one, the maximum level of resilience achievable with only primary controllers has already been reached with the minimum feasible number of controllers ($P = 2$ for $BCC = 1500$ and $P = 3$ for $BCC = 2500$). The only exception is the case considered in the last row, when one additional primary controller is required to achieve the maximum of WNA/Q. The table reveals also that for ANA/Q the quality of the maximum resilience levels (measured by the gap between the achieved value and its upper bound) are very close for both lists (note that for ANA/Q the maxima for the long list are slightly larger than those for the short list because the respective upper bounds, 774.9 and 752.7, are not equal). The same concerns the WNA/Q measure for $BCC = 1500$ (strict CCD limit) for which the maximum (351) is the same for both lists. An exception here are the maxima of WNA/Q in the $BCC = 2500$ case (loose CCD limit), where the maximum achievable for the long list (390) is noticeably smaller than for the short list (504). Clearly, in all cases the (minimum) optimal solutions are not strongly optimal since it is not possible to reach the NA upper bounds using placements with only primary controllers.

Nevertheless, it can be said that the number of primary controllers needed to defend the network (against the attacks) in the most effective way possible without the use of backup controllers is very small, and practically does not increase with the length of the list of attacks.

TABLE 41 *coronet conus*: primary and backup controllers placements maximizing resilience to $\mathcal{A}(6, 12)$ and $\mathcal{A}(6, 100)$

			$C = 2$	$C = 3$	$C = 4$	$C = 5$
BCC	NA	A	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	ANA/Q	12	351.0 [2/0]	551.8 [2/1]	**752.7 [2/2]**	
1500	ANA/Q	100	394.7 [2/0]	611.1 [2/1]	774.7 [2/2]	**774.9 [2/3]**
1500	WNA/Q	12	351 [2/0]	504 [2/1]	**751 [2/2]**	
1500	WNA/Q	100	351 [2/0]	504 [2/1]	**751 [2/2]**	
2500	ANA/Q	12	–	551.8 [3/0]	**752.7 [3/1]**	
2500	ANA/Q	100	–	555.9 [3/0]	772.3 [3/1]	**774.9 [3/2]**
2500	WNA/Q	12	–	504 [3/0]	**751 [3/1]**	
2500	WNA/Q	100	–	354 [3/0]	732 [3/1]	**751 [3/2]**

Table 41 shows the results for combined primary and backup controllers optimization, i.e., when backup controllers are used to support primary controllers in increasing network resilience to attacks. As we already know from Table 31, for the short list the upper bounds on the resilience levels are in all cases achieved when a minimum primary controllers placement (with $P = 2$ for $BCC = 1500$ and $P = 3$ for $BCC = 2500$) is supported by $B = 2$ ($BCC = 1500$) or $B = 1$ ($BCC = 2500$) backup controllers, so in total only 4 controllers are needed in both BCC cases. The same holds for the long list of attacks, and only for WNA/Q and $BCC = 2500$ one extra backup controller is needed to obtain the minimum strongly optimal placement for the long list. (To be precise, one more backup controller is needed also for ANA/Q and both cases of BCC, but the gain from adding such an extra controller is negligible.) Note that introducing backup controllers leads to strongly optimal controllers placements.

Taking into account the above observation, Properties 1-3, and the fact that in all cases included in Tables 40 and 41 computation times are not greater than 0.1 sec. (and are virtually the same for both attack lists), we can formulate the following conclusion: It is sufficient to optimize controllers placement just once, only for the ANA measure (ANA/L or ANA/Q, depending on the assumed component metric) using the long list of attacks. The so obtained minimum strongly optimal placement for ANA will be strongly optimal for all sublists of the long attack list both ANA and WNA, and almost (in terms of the number of controllers used) minimum strongly optimal in all cases. This conclusion is further supported by the negligible difference in the computation time needed to generate the short and the long attack lists (see the last paragraph in Section A.2).

It should be noted, however, that the above conclusion needs to be verified for other attack sizes, other sizes of the attack lists and their sublists, and other mesh networks (including *cost266*).

B.2.6 | Impact of the relaxation of the SC delay bound

Let us now discuss another issue. So far, the placements of primary controllers have been optimized assuming that the strict upper bound BSC on the SC delay implied by a given maximum CCD delay is obeyed. Yet, in practice, the operator may tolerate an increased maximum SC delay, allowing for considering primary controllers placements that are potentially more resilient to attacks. Tables 42 and 43 show the effect of loosening the SC delay constraint (i.e.,

increasing the value of BSC) on the maximized values of ANA/Q and WNA/Q for $BCC = 1500$. In the tables, the increase (in percent) of BSC (recall that for $BCC = 1500$ the minimized value of BSC is equal to 3094) is indicated in column "↗", where three values, 0%, 5% and 10%, are considered.

The presented results reveal that when only primary controllers are used, increasing the value of BSC leads to a noticeable improvement in the resilience levels both with the 5% and 10% increase, but again, using only primary controllers, neither for ANA/Q nor WNA/Q the upper bounds in question can be reached. When backup controllers are allowed, a 5% increase does not lead to any improvement, but a 10% increase allows to reach the upper bounds on both ANA/Q and WNA/Q with one less backup controller.

It turns out that in the case of $BCC = 2500$, increasing the upper bound on SCD does not improve resilience neither for ANA/Q nor for WNA/Q. (When both primary and backup controllers are used, this is because the upper bounds on both ANA/Q and WNA/Q are practically achieved with a single backup controller.) In conclusion, in the case under consideration, loosening the SC delay constraint is only worthwhile if the CC delay constraint is strict.

TABLE 42 *coronet conus*: primary controllers placements maximizing resilience to $\mathcal{A}(6, 100)$ for relaxed BSC

				$C = 2$	$C = 3$	$C = 4$		
BCC	BSC	↗	NA	value $[P]$	value $[P]$	value $[P]$	UB	gap
1500	3094	0%	ANA/Q	394.7 [2]			**774.9**	49.1%
1500	3249	5%	ANA/Q	394.7 [2]	529.1 [3]		**774.9**	31.7%
1500	3403	10%	ANA/Q	611.1 [2]			**774.9**	21.1%
1500	3094	0%	WNA/Q	351 [2]			**751**	53.3%
1500	3249	5%	WNA/Q	351 [2]	387 [3]		**751**	48.5%
1500	3403	10%	WNA/Q	504 [2]			**751**	32.9%

TABLE 43 *coronet conus*: primary and backup controllers placements maximizing resilience to $\mathcal{A}(6, 100)$ for relaxed BSC

				$C = 2$	$C = 3$	$C = 4$	$C = 5$
BCC	BSC	↗	NA	value $[P/B]$	value $[P/B]$	value $[P/B]$	value $[P/B]$
1500	3094	0%	ANA/Q	394.7 [2/0]	611.1 [2/1]	774.7 [2/2]	**774.9 [2/3]**
1500	3249	5%	ANA/Q	394.7 [2/0]	611.1 [2/1]	774.7 [2/2]	**774.9 [2/3]**
1500	3403	10%	ANA/Q	611.1 [2/0]	774.7 [2/1]	**774.9 [2/2]**	
1500	3094	0%	WNA/Q	351 [2/0]	504 [2/1]	**751 [2/2]**	
1500	3249	5%	WNA/Q	351 [2/0]	504 [2/1]	**751 [2/2]**	
1500	3403	10%	WNA/Q	504 [2/0]	**751 [2/1]**		