Optimizing the Resilience of Interdependent Infrastructure Systems against Intentional Attacks

Yiping Fang[1]
[1]Chaire Systems Science and the Energy Challenge
Laboratoire Génie Industriel, CentraleSupélec Université Paris-Saclay
3 rue Joliot-Curie, Gif-sur-Yvette, France
e-mail: yiping.fang@centralesupelec.fr

Enrico Zio[1,2]
[2]Energy Department
Politecnico di Milano
Via La Masa 34, Milano, Italy
e-mail: enrico.zio@polimi.it,
enrico.zio@centralesupelec.fr

***Abstract*—This paper develops a defender-attacker-defender (DAD) model for the resilience optimization of interdependent critical infrastructures (CIs) against intentional at-tacks. In the outer level, the system defender identifies the components to be hardened in order to reduce the damage associated with the worst case attack. In the middle level, the attacker disrupts the system to inflict maximum damage. In the inner level, the defender responds to the attack to minimize the consequence of the attack by optimal operation of the system. A recently developed decomposition-based two-layer cutting plane algorithm is adopted to solve the proposed model. A case of interdependent power and water systems is presented to show the proposed model**

Keywords-resilience; intentional attacks; interdependent critical infrastructures; defender-attacker-defender model; optimization

I. INTRODUCTION

Modern society relies on the effective functioning of critical infrastructures (CIs) such as the power grid, transportation network, Internet, water distribution network, etc. to provide public services, improve quality of life, sustain private profits and spur economic growth. These CIs do not exist in isolation of one another – the Internet requires electricity, transportation networks often use sophisticated control and information systems, the generation of electricity requires fuels, and so forth. CIs are physically, geographically, cyber and logically dependent and interdependent, thus called interdependent CIs [1-5]. The interdependencies can improve the operational efficiencies of these systems, but they can also create new vulnerabilities by providing new hazards and extra channels for failure propagation among different CIs, resulting in so-called cascading failures [6-8]. By recognizing the significance of these issues, many governments and organizations have initiated interdependent CIs protection plans aiming at improving the resilience of national/regional interdependent CIs [9, 10]. Also, in the research field, the number of the resilience-related papers has increased exponentially during the past decades [11].

Albeit no consensus exists for the concept of resilience, it is essentially related to the capability of a system to withstand, adapt to and quickly recover from the effects of a disruptive event [2, 12]. System resilience under a disruptive event is mainly affected by its robustness and recovery rapidity under this event, where system robustness is quantified by the system functionality level immediately after the event, and the recovery rapidity describes how quickly the system recovers after the event [13]. In this paper, we regard improving robustness as the primary strategy for system resilience enhancement, and the system recovery phase is not considered.

This paper mainly focuses on the resilience of interdependent CIs under intentional attacks. In the literature, scholars have studies interdependent CIs system resilience under malicious attacks, where the attacks are usually modeled as the failure of important components which are selected by the local [14-16] or global [3, 17, 18] importance metrics of the components. In these approaches, the attack strategies and the system protection strategies are not affected by each other, i.e. there are no interactions between the attackers and the system defenders. The results from these models are not necessarily the worst-case disruptions at the system level, differing from the principle of worst-case analysis highly advocated for the terrorist risk study for CI systems [19, 20].

Despite the reduced number of studies for interdependent CIs under intentional attacks, similar problems have been extensively studied for single CIs in the literature. These problems usually introduce a virtual attacker who seeks to find the most harmful attack strategy to disrupt the system and a defender who pursues minimum damage from the attack through pre-attack defense and post-attack response. The interactions between the attacker and the defender can be modeled by a tri-level defender-attacker-defender (DAD) framework. The outer level of this model describes how the defender optimally protect the system, the middle level describes how the attacker disrupts the system to have a maximum damage, and the inner level describes how the defender responds to the attack to minimize the consequence of the attack, e.g., via re-dispatching network flow in an electric power grid. This modeling framework has been applied to identify the optimum protection strategies for electric power grids [21-23], rail systems [24], commodity distribution networks [20, 25] and some other CIs [26]. Ouyang [27] recently applied the DAD framework for the resilience optimization of interdependent CIs under spatially localized attacks.

978-1-5386-3322-9/17/$31.00 ©2017 IEEE

In this paper, we adapt the DAD framework for the resilience optimization of interdependent CIs against intentional attacks, addressing the challenges of modeling interdependencies among different CIs and analyzing the importance of such interdependencies for system defense. To the best of the authors' knowledge, this has not been studied previously. For illustrative purposes, this paper considers hardening weak components as the defense strategy to enhance system resilience. Yet, other defense strategies that can be used to improve interdependent CIs resilience, e.g., system expansion by constructing new components, can be easily incorporated into the model.

The remainder of this paper is organized as follows. Section 2 proposes a detailed formulation of the trilevel DAD model for the resilience optimization of interdependent CIs under intentional attacks. The methodology adopted for the solution of the proposed model is briefly introduced in Section 3. Section 4 presents the analysis of the computational results obtained from the application to interdependent power and water systems. Concluding remarks are given in Section 5.

II. Model Formulation

This paper uses a network flow-based approach for the modeling of interdependent CIs, where each CI is modeled as a network and their interdependencies are represented via inter-links. Specifically, the set of CIs of concern is denoted by $\boldsymbol{\kappa}$. Each CI k in $\boldsymbol{\kappa}$ is modeled by a network $G^k(N^k, L^k)$ described by a collection of nodes N^k and edges L^k. Each link $l \in L^k$ in CI network k has an associated capacity $\bar{f}_l^k$ representing the maximal amount of flow that can pass through it, while each node $n \in N^k$ has a supply capacity $\bar{s}_n^k$ and a required demand $\hat{d}_n^k$ of flow for its nominal operation. Flow distributes through the CI networks according to the flow capacities of the links and supply capacities of the nodes, following flow conservation.

For each CI network, resilience to a disruptive event is regarded as the system performance level immediately after the event, quantified by the normalized total satisfied demand level. Then, the resilience of the interdependent CIs under this event is represented by the weighted sum of the resilience of each CI network, expressed by

$$R = \sum_{k \in \boldsymbol{\kappa}} \left(w^k \frac{\sum_{n \in N^k} d_{nk}}{\sum_{n \in N^k} \hat{d}_{nk}} \right) \quad (1)$$

where w^k is the weighting factor for the resilience of CI network k.

For optimizing interdependent CIs resilience against intelligent attacks, a virtual attacker and a defender are introduced. The attacker tries to disrupt the system with the most destructive attack strategy and the defender seeks the ex-ante actions, e.g., protecting weak components, and ex-post actions, e.g., dispatching system flow, that maximize resilience. The interactions between the defender and the attacker lead to a three stage DAD model, which includes: the first stage, in which the defender makes protection decisions pursuing maximum system performance subject to a limited protection budget; the second stage, in which the attacker minimizes system performance subject to an attack budget, and the third stage, in which the defender's response aims at maximum system resilience after the attack.

The problem is framed within a three-level max-min-max formulation that implements the DAD model. The mathematical formulation uses the following notation:

Index, Sets and Parameters

$k \in \boldsymbol{\kappa}$	Set of all CI networks
$n \in N^k$	Set of nodes in network k
$l \in L^k$	Set of edges in network k
$o(l)$	Origin or sending node of link l
$d(l)$	Destination or receiving node of link l
$L_n^{k,nbr}$	Set of neighbor links connecting with node n in network k, i.e., $L_n^{k,nbr} = \{l \mid l \in L^k : o(l) = n \text{ or } d(l) = n\}$
$\bar{s}_n^k$	Generation capacity at node n in network k
$\bar{f}_l^k$	Capacity of link l in CI network k
$\hat{d}_n^k$	Required demand at node n in CI network k
C^k	Set of all nodes in network k that depend on the nodes of other networks to operate
D^k	Set of all nodes in network k that any other network nodes depend on
$C^{k \leftarrow m}$	Set of all nodes in network k that depend on the nodes in network m $(m \neq k)$ to operate
$D^{k \rightarrow m}$	Set of nodes in network k that the operation of the nodes in network $m(m \neq k)$ depend on
$F_{i,j}^{k \rightarrow m}$	Set of ordered pairs (i, j) associated with node $i \in D^{k \rightarrow m}$ and node $j \in C^{m \leftarrow k}$, and node j is operational only when the demand of flow of node i in network k can be fully satisfied
B_P	Protection budget
B_A	Attack budget
$c_l^{k,P}$	Cost of protecting link l in network k
$c_l^{k,A}$	Cost of attacking link l in network k
w^k	Weight factor for the resilience of network k

Decision variables

y_l^k	Binary variable that is equal to 1 if link l in network k is protected, 0 otherwise
x_l^k	Binary variable that is equal to 0 if link l is attacked, 1 otherwise
f_l^k	Flow on link l in network k
s_n^k	Flow generation at node $n \in N^k$ in network k
d_n^k	Flow satisfied at node $n \in N^k$ in network k
$\delta_{ij}^{k \rightarrow m}$	Interdependency variable that is equal to 1 if the interdependency from node i in network k to node j in network m works normally, 0 otherwise

The mathematical formulation of the DAD model for optimizing interdependent CIs resilience against intelligent attacks is:

$$\max_{\boldsymbol{v}} \min_{\boldsymbol{x}} \max_{\boldsymbol{o} \in \mathbb{O}(\boldsymbol{v})} \sum_{k \in \boldsymbol{\kappa}} \left(w^k \frac{\sum_{n \in N^k} d_{nk}}{\sum_{n \in N^k} \hat{d}_{nk}} \right) \quad (2)$$

Subject to:

First level (protection) constraints:

$$\sum_{k\in\boldsymbol{\kappa}}\sum_{l\in L^k} c_l^{k,P} y_l^k \le B_P \tag{3}$$

$$y_l^k \in \{0,1\}, \forall l \in L^k, n \in N^k, k \in \boldsymbol{\kappa} \tag{4}$$

Second level (attack) constraints:

$$\sum_{k\in\boldsymbol{\kappa}}\sum_{l\in L^k} c_l^{k,A}\left(1 - x_l^k\right) \le B_A \tag{5}$$

$$x_l^k \in \{0,1\}, \forall l \in L^k, k \in \boldsymbol{\kappa} \tag{6}$$

Third level (response) constraints:

$$s_n^k - \sum_{(l\in L^k | o(l)=n)} f_l^k + \sum_{(l\in L^k | d(l)=n)} f_l^k - d_n^k = 0\ , \forall n \in N^k, k \in \boldsymbol{\kappa} \tag{7}$$

$$-\bar{f}_l^k\left[x_l^k\left(1-y_l^k\right)+y_l^k\right] \le f_l^k \le \bar{f}_l^k\left[x_l^k\left(1-y_l^k\right)+y_l^k\right], \forall l \in L^k, k \in \boldsymbol{\kappa} \tag{8}$$

$$0 \le s_n^k \le \bar{s}_n^k, \forall n \in N^k, k \in \boldsymbol{\kappa} \tag{9}$$

$$0 \le d_n^k \le \hat{d}_n^k, \forall n \in N^k, k \in \boldsymbol{\kappa} \tag{10}$$

$$d_i^k = \delta_{ij}^{k\to m}\hat{d}_i^k, \forall (i,j) \in F_{i,j}^{k\to m}, k \in \boldsymbol{\kappa} \tag{11}$$

$$s_j^m \le \delta_{ij}^{k\to m}\bar{s}_j^m, \forall (i,j) \in F_{i,j}^{k\to m}, k \in \boldsymbol{\kappa} \tag{12}$$

$$d_j^m \le \delta_{ij}^{k\to m}\hat{d}_j^m, \forall (i,j) \in F_{i,j}^{k\to m}, k \in \boldsymbol{\kappa} \tag{13}$$

$$-\delta_{ij}^{k\to m}\bar{f}_l^m \le f_l^m \le \delta_{ij}^{k\to m}\bar{f}_l^m, \forall (i,j) \in F_{i,j}^{k\to m}, l \in L_j^{m,nbr}, k \in \boldsymbol{\kappa} \tag{14}$$

A. First Level − Defender's Protection Problem

In the defender's protection planning phase, the system defender makes investment decisions for hardening weak components in the interdependent CIs with the objective of maximizing the system performance under the worst case attack, as expressed by Eq. 2). A protected component is assumed to become invulnerable to damage, meaning that it remains operating even under attack. For simplicity, this paper focuses only on the protections (and attacks) of network links, but the approach can be easily extended to account for the protections (and attacks) of other components. The cost of protecting a link l in network k is denoted as $c_l^{k,P}$, and the protection budget is denoted as B_P, as described by Constraint 3). Constraint 4) enforces the binary nature of the protection variables: $y_l^k = 1$ if link l in network k is protected, 0 otherwise.

B. Second Level – Attacker's Problem

The attacker's choice of the components (links) to target is described by the second-level attack problem, which is parameterized in terms of the first-level variables y_l^k. The attack decision is modeled by binary variable x_l^k, which is equal to 0 if link l in network k is attacked, and $x_l^k = 1$ otherwise. The attacker aims to minimize the best-response system resilience, which is determined in the third level defender's response problem, presented in Section 2.3. The attack budget is denoted as B_A and enforced by Constraint 5), where $c_l^{k,A}$ represents the cost of attacking link l in network k. Constraint 6) ensures the integrality of the attack variables.

C. Third Level − Defender's Response Problem

The defender's response to the attack is modeled in the third-level problem, where the defender aims to mitigate the system resilience loss caused by the attack, i.e. to maximize system resilience via re-dispatching the network flows. The flow re-dispatch depends on the protection decisions in the first phase and the attacker's decisions in the second phase. The operation of each CI system modeled by network flows is described by Constraints 7)- 10). Constraint 7) guarantees flow conservation at each node. Constraint 8) limits the flow across link l in network k to its capacity. The term $x_l^k\left(1-y_l^k\right)+y_l^k$ in 8) models the operation status of link l in network k, ensuring that link l is always operating, i.e., it is equal to 1 if i) it is protected $y_l^k = 1$ or ii) it is neither protected $y_l^k = 0$ nor attacked $x_l^k = 1$, and link l is offline if it is attacked $x_l^k = 1$ while not being protected $y_l^k = 0$, i.e., it is equal to 0. Constraint 9) bounds the output of flow generation at node n in network k to its capacity, and 10) ensures that the real satisfied demand cannot exceed the required demand for each node.

Physical interdependencies among different CIs are also considered. The physical interdependency is modeled by defining a set of ordered node pairs (i,j) associated with node i in one CI network and node j in another CI network, where node j is operational if the flow demand of node i is fully satisfied [27, 28]. Then, we use a binary variable $\delta_{ij}^{k\to m}$ to represent the physical interdependency from node i in network k to node j in network m, and $\delta_{ij}^{k\to m} = 1$ if the interdependency works normally and $\delta_{ij}^{k\to m} = 0$ otherwise. For each ordered node pair $(i,j) \in F_{i,j}^{k\to m}$, the demand level at node i in network k is either zero or fully satisfied, depending on whether their interdependency relation can work normally, as described by Constraint 11). For each node j in the ordered pair $(i,j) \in F_{i,j}^{k\to m}$, the flow generation is bounded by zero or its generation capacity, as stated by Constraint 12), and its demand level is bounded by zero or the required demand, as stated by Constraint 13). Furthermore, if node j is damaged, the flow on the attached links is zero, as described by Constraint 14)

III. SOLUTION ALGORITHM

The max-min-max formulation 2)- 14) of Section 2 configures a mixed-integer nonlinear tri-level programming problem. Due to the presence of binary variables $\delta_{ij}^{k\to m}$ in the third level, the second and third level min-max problems cannot be merged into a single min problem using the KKT conditions (or the strong duality) of the third level max problem [29]. Therefore, solution methods that depend on

the gradual reconstruction of the upper stage problem using dual information from the lower stage are inapplicable [23, 25].

We adopt a recently developed algorithm, called the "Nested Column-and-Constraint Generation" (NC&CG) method [30], which is proven to be effective in dealing with mixed integer programming recourse problems [23, 25]. A general overview of this algorithm is presented in Figure 1. The problem is decomposed into an outer-level master problem and an outer-level subproblem, which iteratively exchange primal decision variables until convergence to an optimal solution. The outer-level subproblem provides the attacker's optimum plan and can be expanded into a min-max-max formulation by separating the binary variables $\delta_{ij}^{k\to m}$ and other continuous variables f_l^k, s_n^k and d_n^k in the third level problem. Thus, the outer-level subproblem can be solved by decomposing it into an inner-level master problem and an inner-level subproblem and by applying a cutting plane method.

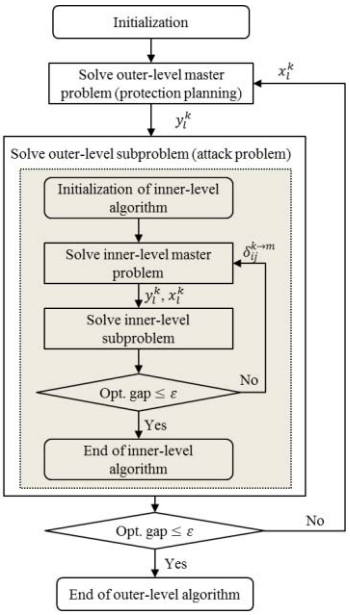

Figure 1. Flow diagram of the NC&CG algorithm

The detailed formulations of the outer-level and inner-level problems are omitted for simplicity and because of the limitation of space. The interested readers are referred to [23, 25] for similar formulations and to [30] for the detailed mathematical derivations, proofs and analysis.

IV. CASE STUDY

This section presents a case study involving interdependent power and water systems, adapted from [27]; the network layouts of the two systems are shown in Figure 2. The interdependency relations are described as follows: the water node w8 depends on the power demand node p11; w7 depends on node p10; node w1 depends on node p4; node w3 depends on node p9; the power generation node p1 depends on the water demand node w9 [27].

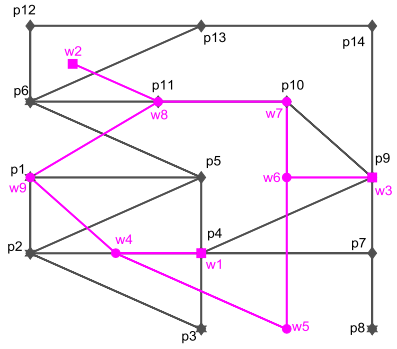

Figure 2. Layout of the interdependent power and water systems [27]

The proposed algorithm is implemented by the IBM ILOG CPLEX [31] and the calculations are performed on a laptop with Intel (R) Core (TM) 2.6 GHz and 8GB memory. This study assumes that protecting one link in the interdependent CIs needs one unit of protection resources and attacking one link takes one unit of attack budget. The weighting factor is set as 0.5 for the resilience of each interdependent system.

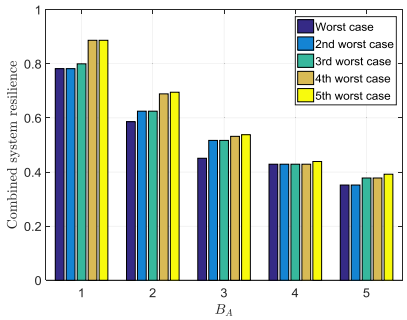

Figure 3. The combined system resilience associated with the worst-case, the second-worst through the fifth-worst attacks for each attack budget

First, when there is no defense investment, namely, $B_P = 0$. Figure 3 shows the combined power and water systems resilience associated with the worst attack scenarios, and the second worst (i.e., rank order 2) through fifth-worst (i.e., rank order 5) combination of system resilience for each attack budget. These second-worst through fifth-worst results were obtained by adding a new constraint that eliminates the previous solution. From the Figure, it is possible to see that the combined system resilience generally decreases as the attack budget increases for the worst case attack, which is expected. Furthermore, the second-worst attacks do not necessarily have strictly larger resilience than the worst cases, e.g., for the cases $B_A = 1, 4$ and 5. In other words, the identified worst-case scenarios are not unique but are accompanied by some equally bad ones, implying that defending against only one of the worst cases is not likely to improve the system resilience.

Second, when the defense investment is considered, we solve the DAD model for different combinations of protection budget B_P and attack budget B_A. Figure 4 shows the combined power and water resilience as a function of the attack budget B_A under different B_P. From the Figure, it can

be seen that in the case of no defense, the resilience decreases almost linearly with the increase of B_A, which can be mitigated by increasing the protection budget B_P, i.e., $B_P = 2, 4, 6$ and 8. However, due to the non-uniqueness of the worst case attack for some attack budgets, the improvement of system resilience is not always promising. For example, the combined system resilience is increased by only 2.3% when B_P is increased from 0 to 2 for $B_A = 1$, compared to the average improvement of 28.4% for other attack scenarios under the same increase of B_P.

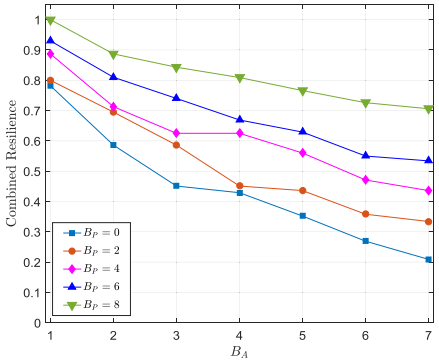

Figure 4. Interdependent power and water systems

Then, we investigate the importance of considering interdependency in system defense. In practice, a coordinated defense agency for different CIs may not exist. Thus, each system makes its own protection decisions without considering the interdependencies. To investigate this case, we assume there is a governor who distributes the defense budget evenly to the power and water systems, and each of them protects itself separately without considering the interdependencies among them, while the attacker disrupts the two systems by recognizing the interdependencies. We call this strategy as "separate protection" to differentiate it from the "coordinated protection" where the interdependent systems are protected as a whole. Figure 5(a) shows the combined power and water system resilience as a function of the attack budget B_A for the separate protection and the coordinated protection when the protection budget $B_P = 4$. It is clearly shown that the combined resilience values in the case of separate protection are always smaller than that in the case of coordinated protection. The difference of the combined system resilience between the two cases can reflect the importance of considering interdependencies in interdependent CIs protection. Figure 5(b) presents the difference of the combined system resilience between the two cases for different protection budget B_P. From this Figure, it can be seen that when B_P is relatively small, the difference of the combined system resilience is relatively insignificant, e.g., under or around 0.1 when $B_P = 2$; when B_P increases, the difference becomes increasingly significant. These results highlight the significance of protecting interdependent CIs as a whole against intentional attacks, especially when the protection budget is relatively high.

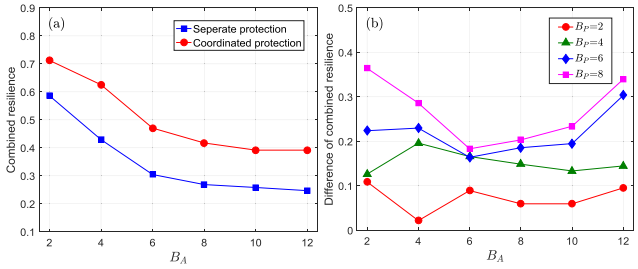

Figure 5. (a) The combined system resilience curves as a function of the attack budget B_A for the separate protection and the coordinated protection when $B_P = 4$; (b) The combined resilience difference between the separate protection and the coordinated protection as a function of the attack budget B_A when $B_P = 2, 4, 6$ and 8.

Finally, Figure 6 reports the computation times of the adopted NC&CG algorithm for solving the proposed model. It can be observed that the computation burden is relatively light for small attacks, e.g., $B_A = 1, 2, 3$, and it becomes heavy when the attack budget B_A increases. Besides, the computation time is relatively increased for certain values of the protection budget B_P, e.g., $B_p = 3, 4, 5$. However, the computation time is overall acceptable (< 300 seconds) for the proposed system planning problem, which can be solved offline.

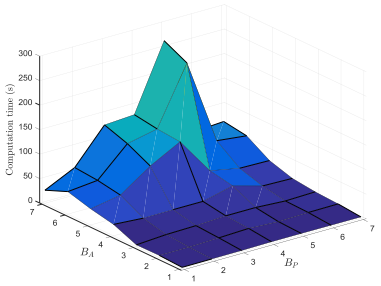

Figure 6. Computation times of the solution algorithm

V. CONCLUSION

This paper has presented an adapted DAD model for the optimal allocation of defensive resources in interdependent CIs for resilience against intentional attacks. To the best of our knowledge, it is the first tri-level DAD model presented for interdependent CIs resilience under intentional attacks. To address the computational challenge of the proposed mixed-integer nonlinear tri-level programming, a recently developed decomposition-based two-layer cutting plane algorithm, called NC&CG, has been adopted. A case study has been performed to demonstrate the effectiveness of the proposed approach. This has allowed to also highlight the significance of considering interdependencies among different CIs when considering interdependent CIs defense.

REFERENCES

[1] Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies.* IEEE Control Systems, 2001. 21(6): p. 11-25.

[2] Zio, E., *Reliability engineering: Old problems and new challenges.* Reliability Engineering & System Safety, 2009. 94(2): p. 125-141.

[3] Zio, E. and G. Sansavini, *Modeling interdependent network systems for identifying cascade-safe operating margins.* IEEE Transactions on Reliability, 2011. 60(1): p. 94-101.

[4] Ouyang, M., *Review on modeling and simulation of interdependent critical infrastructure systems.* Reliability engineering & System safety, 2014. 121: p. 43-60.

[5] Liu, X., E. Ferrario, and E. Zio, *Resilience analysis framework for interconnected critical infrastructures.* ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, 2017. 3(2): p. 021001.

[6] Helbing, D., *Globally networked risks and how to respond.* Nature, 2013. 497(7447): p. 51-59.

[7] Fang, Y., N. Pedroni, and E. Zio, *Optimization of Cascade‐Resilient Electrical Infrastructures and its Validation by Power Flow Modeling.* Risk Analysis, 2015. 35(4): p. 594-607.

[8] Buldyrev, S.V., et al., *Catastrophic cascade of failures in interdependent networks.* Nature, 2010. 464(7291): p. 1025-1028.

[9] Moteff, J.D., *Critical infrastructure resilience: the evolution of policy and programs and issues for congress*. 2012: Congressional Research Service US.

[10] Giannopoulos, G., R. Filippini, and M. Schimmer, *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.* JRC Technical Notes, 2012.

[11] Bergström, J., R. van Winsen, and E. Henriqson, *On the rationale of resilience in the domain of safety: A literature review.* Reliability Engineering & System Safety, 2015. 141: p. 131-141.

[12] Fang, Y.-P., N. Pedroni, and E. Zio, *Resilience-based component importance measures for critical infrastructure network systems.* IEEE Transactions on Reliability, 2016. 65(2): p. 502-512.

[13] Bruneau, M., et al., *A framework to quantitatively assess and enhance the seismic resilience of communities.* Earthquake spectra, 2003. 19(4): p. 733-752.

[14] Wang, S., et al., *Vulnerability analysis of interdependent infrastructure systems under edge attack strategies.* Safety science, 2013. 51(1): p. 328-337.

[15] Buldyrev, S.V., N.W. Shere, and G.A. Cwilich, *Interdependent networks with identical degrees of mutually dependent nodes.* Physical Review E, 2011. 83(1): p. 016112.

[16] Huang, X., et al., *Robustness of interdependent networks under targeted attack.* Physical Review E, 2011. 83(6): p. 065101.

[17] Nan, C., I. Eusgeld, and W. Kröger, *Analyzing vulnerabilities between SCADA system and SUC due to interdependencies.* Reliability Engineering & System Safety, 2013. 113: p. 76-93.

[18] Zio, E., L.R. Golea, and G. Sansavini, *Optimizing protections against cascades in network systems: A modified binary differential evolution algorithm.* Reliability Engineering & System Safety, 2012. 103: p. 72-83.

[19] Brown, G.G. and A. Cox, *Making terrorism risk analysis less harmful and more useful: Another try.* Risk Analysis, 2011. 31(2): p. 193.

[20] Alderson, D.L., G.G. Brown, and W.M. Carlyle, *Operational models of infrastructure resilience.* Risk Analysis, 2015. 35(4): p. 562-586.

[21] Brown, G., et al., *Defending critical infrastructure.* Interfaces, 2006. 36(6): p. 530-544.

[22] Yuan, W., L. Zhao, and B. Zeng, *Optimal power grid protection through a defender–attacker–defender model.* Reliability Engineering & System Safety, 2014. 121: p. 83-89.

[23] Fang, Y. and G. Sansavini, *Optimizing power system investments and resilience against attacks.* Reliability Engineering & System Safety, 2017. 159: p. 161-173.

[24] Alderson, D.L., G.G. Brown, and W.M. Carlyle, *Assessing and improving operational resilience of critical infrastructures and other systems*, in *Bridging Data and Decisions*. 2014, INFORMS. p. 180-215.

[25] Ouyang, M. and Y. Fang, *A mathematical framework to optimize critical infrastructure resilience against intentional attacks.* Computer‐Aided Civil and Infrastructure Engineering, 2017.

[26] Alderson, D.L., et al., *Solving defender-attacker-defender models for infrastructure defense*. 2011, NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF OPERATIONS RESEARCH.

[27] Ouyang, M., *A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks.* European Journal of Operational Research, 2017.

[28] Lee II, E.E., J.E. Mitchell, and W.A. Wallace, *Restoration of services in interdependent infrastructure systems: A network flows approach.* IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007. 37(6): p. 1303-1317.

[29] Thiele, A., T. Terry, and M. Epelman, *Robust linear optimization with recourse.* Rapport technique, 2009: p. 4-37.

[30] Zhao, L. and B. Zeng, *An exact algorithm for two-stage robust optimization with mixed integer recourse problems.* submitted, available on Optimization-Online. org, 2012.

[31] CPLEX, I.I., *V12. 1: User's Manual for CPLEX.* International Business Machines Corporation, 2009. 46(53): p. 157.