Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions

Yiping Fang, Enrico Zio

Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions

Yiping Fang

Chaire on Systems Science and the Energy Challenge, Fondation Electricité de France (EDF), Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, 3 rue Joliot-Curie, 91192 Gif-Sur-Yvette Cedex, France.

Email : yiping.fang@centralesupelec.fr

Enrico Zio*

Chaire on Systems Science and the Energy Challenge, Fondation Electricité de France (EDF), Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, 3 rue Joliot-Curie, 91192 Gif-Sur-Yvette Cedex, France;

Energy Department, Politecnico di Milano, Via La Masa 34, Milano, 20156, Italy.

Email: enrico.zio@centralesupelec.fr; enrico.zio@polimi.it

Abstract This chapter addresses the challenges associated with assessing and improving the resilience of interdependent critical infrastructure systems under potential disruptive events. A specific set of analytical tools are introduced based on quantitative models of infrastructure systems operation and their functional interdependencies. Specifically, the game-theoretic attacker-defender and defender-attacker-defender modeling techniques are applied to assessing the resilience of interdependent CI systems under worst-case disruptions, and advising policymakers on making pre-disruption decisions for improving the resilience of interdependent infrastructures. A case of interdependent power and gas systems is presented to show the proposed model and highlight the significance of protecting interdependent CIs.

1 Introduction

The phrase, "critical infrastructure protection (CIP)," did not appear in print until in 1997, when the "Marsh report" [1] provided the first definition of infrastructure as "a network of independent, mostly privately-owned, man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services". Then, critical infrastructures (CIs) are defined as network systems that provide life-essential services [2] and whose incapacity or destruction can have a debilitating impact on the health, safety, security, economics, and social well-being, including the effective functioning of governments [3, 4].

CI systems, usually distributed on large geographical extensions, are complex collections of many interacting elements (or subsystems) having an internal dynamic structure and comprising a unified whole. More importantly, different CIs do not operate 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 [5, 6].

On one side, the interdependencies can improve the operational efficiencies of CI systems, but on the other side they can also create new vulnerabilities by providing new hazards and introducing additional channels for failure propagation within and across different CIs, i.e., the disruption of one part of a CI may trigger a domino effect causing the loss of functionality of other key services, as seen in various recent disasters ranging from hurricanes to large-scale power outages and terrorist attacks [7, 8].

By recognizing the significance of these issues, many governments and organizations have initiated interdependent CIs protection plans aiming at strengthening the security and resilience of national/regional interdependent CIs, such as issuing "Critical infrastructure resilience: final report and recommendations" in 2009 in USA [9]; publishing "Australian Government's Critical Infrastructure Resilience Strategy" in 2010 in Australia [10]; issuing "Climate Resilient Infrastructure: Preparing for a Changing Climate" in 2011 in UK [11]; initiating the European Programme for Critical Infrastructure Protection and lanuching a Thematic Area to address it systematically since 2006 in European Union [3]. In these plans, the concept of infrastructure "resilience" has been highlighted.

"Resilience" has many definitions, without a broadly accepted one, even only focusing on CIs [12-15]. A complicating aspect in previous attempts to define resilience is the recognition that "resilience is a family of related ideas, not a single thing" [16]. Zolli and Healy [17] provide perhaps the most comprehensive discussion of the concepts of resilience. Recently, other authors have also provided fairly comprehensive surveys and summaries of the growing literature on resilience and its relationship to the study of risk, specifically for engineered infrastructure systems [12, 18, 19]. Although there are no unique resilience definition and no common

resilience metric, there still exist some consensuses. Basically, resilience is recognized as the capability of a system to withstand internal/external stresses and to recover from them. The main difference for various resilience definitions and metrics is that such capability to face adverse events can be considered (and computed) with reference to the time needed to recover, to the time slot in which urban services do not work, to the number of citizens reallocated, to the urban efficiency loss, and so forth [12, 13, 20, 21]. Nevertheless, these are all factors directly related to the system functionality and to its ability to guarantee continuity, even when the global equilibrium is compromised. Thus, a distinguishing feature of resilience is the adaptation in the way that components work together to achieve persistence in the ability of a system to function over time, and in the presence of disruptions.

In this chapter, we consider the challenges associated with assessing and improving the resilience of interdependent CI systems under potential disruptive events. We describe a specific set of analytical tools based on quantitative models of infrastructure systems operation and their functional interdependencies. Specifically, we are interested in (1) assessing the resilience of multiple interdependent CIs, (2) identifying critical vulnerabilities that threaten their continued function, and (3) advising policymakers on making pre-disruption decisions for CI resilience improvement. We apply the game-theoretic attacker-defender (AD) and defender-attacker-defender (DAD) modeling techniques [22] to assess the worst-case disruptions to system function and to identify the most effective defensive measures against them.

The remainder of this chapter is organized as follows. Section 2 begins with the quantitative CI operation and interdependency models. Section 3 discusses the detailed formulation of the optimization framework for assessing and improving the resilience of interdependent CIs. Section 4 illustrates how to apply this framework to a specific example. Concluding remarks are provided in Section 5.

2 Operational Models of Interdependent Infrastructures

A CI system can be viewed as a collection of interconnected components that work together to accomplish a particular, domain-specific function. It achieves this through either human or automated decision making that responds to the demands placed on the system to deliver the best possible service in any given situation. This decision-making process is usually termed the operation of the system, and an operational model of a system is used to quantitatively evaluate the service performance of a system by explicitly embracing this decision making in its formulation.

2.1 Optimization-based System Operation Model

The operation of modern infrastructure systems is fundamentally driven by the demands that are placed on their functionality. The system as a whole needs to "work", i.e., providing service to its users, which are often seen as objectives (e.g., minimize

unmet demand of service) and, then, measured in terms of system functionality. In addition, the operation of the CI system is restricted by what is possible, due to physical, economic, or regulatory constraints, e.g., the amount of electric power that a transmission line carries cannot exceed its capacity. In this respect, constrained optimization [23] is ideally suited to model this type of decision problem: system operators make decisions, in an optimum way, about the behavior of the system in pursuing these objectives (what we want the system to do) while subject to its constraints (what the system can do).

In constrained optimization models of CI system operations, potential courses of actions are modeled by decision variables, and the solution to a particular problem indicates decisions that should be taken to reconcile objectives and constraints in an optimum manner with regard to the specified objective. Importantly, this model technique is naturally suited to represent disruptions to CI systems as changes to input data [24]. For example, the operation of an electric power transmission network can be modeled by linear programming (LP) based on the direct circuit (DC) representation, taking available generation units, transmission lines and buses, and identifies the set of power flows that minimizes unmet demand [25]. If the system loses a transmission line in a disruption, we simply need to leave the damaged transmission line "out" of the model (e.g., using an indicator variable to represent its unusable state [13, 25]) and resolve the same operation model (or slightly modified model, e.g., give more weight to the quality of system service rather than the cost of system operation in the objective function when facing disruption); then, the solution to this modified problem will indicate the best possible response of the system.

For illustration purpose, a commonly used network flow-based approach [26] is used here to model the operation of interdependent CIs, where each CI is modeled as a network and their interdependencies are represented via inter-links. Formally, the set of CIs of concern is denoted by $\boldsymbol{\kappa}$. Each infrastructure system 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 CI network $k \in \boldsymbol{\kappa}$, its resilience to a disruptive event is regarded as the system functionality level immediately after the event, normalized by the total satisfied demand level

$$R^k = \frac{\sum_{n \in N^k} d_n^k}{\sum_{n \in N^k} \hat{d}_n^k} \tag{1}$$

where d_n^k denotes the satisfied flow at node $n \in N^k$. Then, the overall resilience of interdependent CIs under this event is represented by the weighted sum of the resilience of each CI network, expressed by

$$R = \sum_{k \in \boldsymbol{\kappa}} w^k R^k \tag{2}$$

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

Then, the mathematical formulation of the operation model (OM) of CI network $k \in \boldsymbol{\kappa}$ is represented by

$$OM(k): \max_{\boldsymbol{o}^k \in \mathbb{O}^k} R^k \tag{3}$$

where the system operators seek to maximize the total satisfied demand level. Set $\mathbb{O}^k$ represents the feasible space for decision variable $\boldsymbol{o}^k$. Different feasible operation spaces $\mathbb{O}^k$ may be formulated for different CI systems with various physical, economic, and/or regulatory constraints. An example of formulation of $\mathbb{O}^k$ by applying the network flow approach is given as follows:

$$\mathbb{O}^k = \left\{ \boldsymbol{o}^k : [s_n^k, f_l^k, d_n^k] | 0 \le s_n^k \le \bar{s}_n^k, \forall n \in N^k \right. \tag{4}$$

$$0 \le d_n^k \le \hat{d}_n^k, \forall n \in N^k \tag{5}$$

$$-\bar{f}_l^k z_l^k \le f_l^k \le \bar{f}_l^k z_l^k, \forall l \in L^k \tag{6}$$

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

where constraint (4) bounds the output of flow generation at node n to its capacity. Constraint (5) ensures that the real satisfied demand cannot exceed the required demand for each node. Constraint (6) limits the flow across link l in network k to its capacity. The term z_l^k in (6) models the operation status of link l in network k, i.e., $z_l^k = 1$ if link l is operating; $z_l^k = 0$, otherwise. Finally, constraint (7) guarantees flow conservation at each node, where $o(l)$ indicates the origin or sending node of line l and $d(l)$ indicates the destination or receiving node of line l. The direction of a transmission line is predefined and given as input to the model.

If there is a centralized agent who is in charge of making decisions about the behavior of interdependent CIs, the operation model (OM) can be represented by

$$OM: \max_{\boldsymbol{o} \in \mathbb{O}} R \tag{8}$$

where $\boldsymbol{o} = \bigcup_{k \in \boldsymbol{\kappa}} \boldsymbol{o}^k$. The objective function is now modified to the overall resilience of all CI networks in $\boldsymbol{\kappa}$. It is noted that $\mathbb{O} = \bigcup_{k \in \boldsymbol{\kappa}} \mathbb{O}^k$ does not necessarily hold when we consider the interdependencies among different CIs, i.e., additional constraints may be posed to the operations of individual CI systems. For example, load

shedding for a substation bus in an electrical power system is allowed when considering only the power system itself; this may not be permitted (e.g., due to regulatory constraints) when this bus provides power to some critical compressor stations of a national gas transmission system.

2.2 Infrastructure Interdependency Model

Different types of interdependencies exist among CI networks. Rinaldi *et al.* [5] defined four principal classes of interdependencies: physical, cyber, geographic, and logical. Physical interdependency means the state of one CI depends on the material output(s) of the other; cyber interdependency means the state of one CI depends on information transmitted by the information infrastructure; geographical interdependency means a local environmental event can create state changes in multiple CIs; logical interdependency means the state of each CI depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. For a detailed and comprehensive discussion about CI interdependency, interested readers can refer to recent surveys [6, 27].

For illustration purpose, we discuss here how to model CI interdependency quantitatively by referring to interdependent power and gas networks (IPGNs). For IPGNs, typical connections include: i) *sink-source* connections where a gas city gate can fuel a gas turbine engine, which is an electric generator, ii) *sink-sink* connections where a city gate requires some energy from an electrical load to regulate its valves, and iii) *sink-transmit* connections where compressors consume electricity from an electrical load to increase the pressure on a gas pipeline, as sufficient line pressure is a feasibility requirement for the gas network.

All these interdependencies can be modeled by defining a set of ordered components pairs (i, j) associated with node i in one CI network and component (node or line) j in another network, where the interdependency relation for (i, j) works if the flow demand of node i is fully satisfied [28-30]. We use the following notations to facilitate explanation:

$L_n^{k,nbr}$	Set of neighboring lines of node $n \in N^k$, i.e., $L_n^{k,nbr} = \{l \mid l \in L^k : o(l) = n \text{ or } d(l) = n\}$
$F_{i,j}^{k \to m}$	Set of ordered pairs (i, j) associated with node i in CI network k and node j in CI network m, and node j is operational only when the demand of flow of node i in network k can be fully satisfied
$M_{i,j}^{k \to m}$	Set of ordered pairs (i, j) associated with node i in CI network k and line j in CI network m, and line j operates with its full capacity when the demand of flow of node i in network k is fully satisfied; otherwise line j operates with a reduced capacity $\tilde{f}_j^m$

For the former two types of interdependencies in IPGNs, component j will be completely failed if the interdependency relation for (i, j) does not work. The *sink-*

transmit connections in IPGNs are modeled as capacity reduction, i.e., the capacity of line j is reduced if the interdependency relation for (i,j) does not work [31]. For this, we define a binary variable $\delta_{ij}^{k\to m}$ to represent the interdependency from node i in network k to component (node or line) j in network m: $\delta_{ij}^{k\to m}=1$ if the interdependency works normally and $\delta_{ij}^{k\to m}=0$ otherwise. For each ordered pair $(i,j)\in F_{i,j}^{k\to m}\cup M_{i,j}^{k\to m}$, the interdependency works normally, i.e., $\delta_{ij}^{k\to m}=1$, only if the demand level at node i in network k is fully satisfied, i.e., $d_i^k=\hat{d}_i^k$, as described by the following constraint:

$$d_i^k-\delta_{ij}^{k\to m}\hat{d}_i^k\geq 0,\forall(i,j)\in F_{i,j}^{k\to m}\cup M_{i,j}^{k\to m} \tag{9}$$

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 (10), and its demand level is bounded by zero or the required demand, as stated by constraint (11):

$$g_j^m-\delta_{ij}^{k\to m}\bar{g}_j^m\leq 0,\forall(i,j)\in F_{i,j}^{k\to m} \tag{10}$$

$$d_j^m-\delta_{ij}^{k\to m}\hat{d}_j^m\leq 0,\forall(i,j)\in F_{i,j}^{k\to m} \tag{11}$$

Furthermore, if node j is not functioning, all its attached lines will not work and the flow on these lines should be zero, as described by constraint (12):

$$-\delta_{ij}^{k\to m}\bar{f}_l^m\leq f_l^m\leq\delta_{ij}^{k\to m}\bar{f}_l^m,\forall(i,j)\in F_{i,j}^{k\to m},l\in L_j^{m,nbr} \tag{12}$$

Finally, constraint (13) models the *sink-transmit* interdependencies in IPGNs; the capacity of line j in network m decreases from its normal level $\bar{f}_j^m$ to a reduced level $\tilde{f}_j^m$ ($\tilde{f}_j^m<\bar{f}_j^m$) if the demand of its dependent node i in network k is not fully satisfied ($\delta_{ij}^{k\to m}=0$):

$$\begin{aligned}-\delta_{ij}^{k\to m}\bar{f}_j^m-\left(1-\delta_{ij}^{k\to m}\right)\tilde{f}_j^m\leq f_{jt}^m\\ \leq\delta_{ij}^{k\to m}\bar{f}_j^m+\left(1-\delta_{ij}^{k\to m}\right)\tilde{f}_j^m,\forall(i,j)\in M_{i,j}^{k\to m}\end{aligned} \tag{13}$$

Until now, we have shown that the interdependency relations in IPGNs can be formally represented by constraints (9)-(13). These constraints can, then, be added into the operation models of the interdependent networks, i.e., model (8) if we are considering the context of the centralized decision making. The feasible operation space $\mathbb{O}$ is, therefore, given by:

$$\mathbb{O}=\left\{\boldsymbol{o}:\left[s_n^k,f_l^k,d_n^k\right]|(4)-(7),(9)-(13),\forall k\right\} \tag{14}$$

3 System Resilience under Disruptions

3.1 Impact Models of Disruptions

In practice, CI systems face various types of internal/external shocks, e.g., technical failures, accidents, natural hazards, and deliberate attacks. The study of failures in engineering systems has yielded an extensive literature on system reliability and probabilistic risk analysis [32-34]. However, the concept of resilience is usually discussed in the context of high-impact low-probability (HILP) events [35, 36], i.e., the risks that are difficult or even impossible to foresee (e.g., due to a lack of statistically evident historical data of the event); therefore, probabilistic assessment may not be applicable in this case. Furthermore, for deliberate threats induced by an intelligent, goal-oriented terrorist, probabilities may not be suitable for modeling the behavior of the adversary [37]. Brown and Cox [38] show that probabilistic assessment of terrorism risk can even lead to misleading results.

Instead of focusing on the source of a disruption, we look at the problem form the point of view of the system functionality. Specifically, we consider disruptions as the simultaneous losses of one or more system components and assess the performance of CIs under the worst-case disruptions. To identify the worst-case disruptions, a hypothetical intelligent adversary (an attacker) is considered to have perfect knowledge and capable of using limited resources to intentionally damage the CIs. From the point of view of system operators, the attacker is not necessarily a real human being. Instead, it could be mother nature, a terrorist, simple bad luck, or anything else that causes the simultaneous loss of components; the operators are concerned with doing the best they can to maintain the functionalities of CIs following the loss of these components. We emphasize that the purpose of assuming a personalized attacker here is simply to identify worst-case disruptions, not to model the actual behavior of any particular adversary.

Formally, the damage of CI systems in a disruption is represented by the state variables of the systems components, e.g., z_l^k for network line $l \in L^k$ where $z_l^k = 0$ if link l is attacked; $z_l^k = 0$ otherwise, as explained in constraint (6). It is noted that here we consider only the failure of network links since the failure of a network node is equivalent to the simultaneous failures of all the links connecting to it. Then, the impact of disruptions to interdependent CI systems is represented by the following attacker-defender (AD) model [13, 22, 24, 25]

$$\min_{\boldsymbol{z}\in\mathbb{Z}} \max_{\boldsymbol{o}\in\mathbb{O}(\boldsymbol{z})} R \tag{15}$$

where the state variable $\boldsymbol{z}$ is now determined by the attacker, and $\mathbb{Z}$ represents the set of all possible links attacks. The system operators still face the same functionality maximization problem, i.e., the operation model (8), whose feasible operation space $\mathbb{O}(\boldsymbol{z})$ is now a function of the system state $\boldsymbol{z}$ obtaining from the attacker's

behavior. In other words, after the realization of the attacks, the systems will adapt their behaviors to maintain continuity of functionality in presence of the disruptions caused by the attacks.

3.2 Resilience Assessment

The above-introduced AD model can be used to assess the resilience of interdependent CI systems to the worst-case disruptions. Before that, we should carefully define the constraints on $\boldsymbol{z}$, to avoid that the obvious "absolute worst-case" turns out to be that with the simultaneous loss of all system components that leads to complete failure of the systems. A straightforward idea would be to limit the maximum number of lost components by a cardinality constraint, as follows:

$$\sum_{k\in\boldsymbol{\kappa}}\sum_{l\in L^k}\left(1-z_l^k\right)\leq B_A \tag{16}$$

where B_A characterizes the disruption "magnitude" of the attack in terms of the maximum number of links that can simultaneously fail in the attack. This parameterization is useful because it allows considering different levels of disruptions and assessing the best achievable worst-case functionality of CI systems as a function of the disruption "magnitude" B_A, obtaining the so-called "resilience curve" [24].

Furthermore, the cardinality constraint (16) can be generalized to any notion of "budget" by specifying a cost associated with attacking each component in the systems. Furthermore, any available information of the attacker's intent of attacking, or on the disruptive event's threat profile to the systems, can be carefully formulated in terms of additional constraints on $\boldsymbol{z}$ to narrow down the space $\mathbb{Z}$. For instance, the impact of a natural hazard like a hurricane on CI system components is usually quantified, in a probabilistic manner, based on the physical model of the hurricane threat (e.g., gust wind speed) [39] and the fragility models of system components [40]. The resulting failure probabilities of system components can be related to their binary damage state variables $\boldsymbol{z}$ through Shannon's information theory. Interested readers can refer to Ref. [41] for a detailed formulation of this model.

3.3 Resilience Improvement

The usefulness of resilience assessment is limited unless it is used to guide the planning for the resilience improvement of interdependent CIs: to build and enhance resilience of the CI systems is the ultimate goal. In the context of the AD model, this means improving the functionality of CI systems under the worst-case simultaneous losses of system components. Nevertheless, doing so will require investment on certain actions, e.g., hardening and upgrading weak system components to increase their chances of survival under disruptions. To quantify this pre-disruption

decision, the AD model is extended to the so-called defender-attacker-defender (DAD) model, as follows [22, 24, 25, 41, 42]:

$$\max_{\boldsymbol{y}\in\mathbb{Y}} \min_{\boldsymbol{z}\in\mathbb{Z}} \max_{\boldsymbol{o}\in\mathbb{O}(\boldsymbol{y},\boldsymbol{z})} R \tag{17}$$

where $\boldsymbol{y}$ is a decision variable representing defensive investments and $\mathbb{Y}$ represents the set of all feasible investments. These investment decisions potentially change the set of feasible system operations $\boldsymbol{o} \in \mathbb{O}(\boldsymbol{y}, \boldsymbol{z})$. The first level problem in (17) is to identify the optimal set of network lines to protect so that the overall resilience of the interdependent CIs is maximized. The worst case system disruptions and the successive adaptive actions are considered in the middle-low level problem $\mathcal{H}(\boldsymbol{y}) = \min_{\boldsymbol{z}\in\mathbb{Z}} \max_{\boldsymbol{o}\in\mathbb{O}(\boldsymbol{y},\boldsymbol{z})} R$, which is almost identical to the prior model (15), except that the feasible system operation space $\mathbb{O}(\boldsymbol{y}, \boldsymbol{z})$ now depends also on the investment decisions $\boldsymbol{y}$.

For illustrative purpose, this chapter considers a typical ex-ante resilience strategy, i.e., protecting CI network lines. Protected lines are assumed to be invulnerable and cannot be damaged in a disruption. Other possible resilience improvement actions like constructing new components [25] can be easily incorporated into this analysis framework. Formally, we let binary variable y_l^k represent the investment decision that $y_l^k = 1$ if link l in network k is protected, 0 otherwise. The ability to invest in improvements is constrained by limited resources. Therefore, the set of feasible investments $\mathbb{Y}$ can be represented by

$$\mathbb{Y} = \Big\{\boldsymbol{y} | y_l^k \in \{0,1\}, \forall l \in L^k, k \in \boldsymbol{\kappa} \\ \sum_{k\in\boldsymbol{\kappa}} \sum_{l\in L^k} c_l^{k,P} y_l^k \le B_P \Big\} \tag{18}$$

where $c_l^{k,P}$ denotes the cost of protecting link l in network k, and B_P parametrizes the total protection budget.

The feasible system opeartions space $\mathbb{O}(\boldsymbol{y}, \boldsymbol{z})$ can now be specified by considering the real function state of a network link l in network k: if the link is protected $y_l^k = 1$, it will be always functional no matter if it is attacked ($z_l^k = 0$) or not ($z_l^k = 1$); otherwise, its function state will depend on whether it is attacked. Therefore, the real function state of the link can be represented by $\left[y_l^k + (1 - y_l^k) z_l^k\right]$, and $\mathbb{O}(\boldsymbol{y}, \boldsymbol{z})$ is given by

$$\mathbb{O}(\boldsymbol{y}, \boldsymbol{z}) = \Big\{\boldsymbol{o}: \left[s_n^k, f_l^k, d_n^k\right] | (4)(5)(7), (9) - (13), \forall k \\ -\bar{f}_l^k \left[y_l^k + (1 - y_l^k) z_l^k\right] \le f_l^k \le \bar{f}_l^k \left[y_l^k + \left(1 - y_l^k\right) z_l^k\right], \forall l \in L^k, \forall k\Big\} \tag{19}$$

The max-min-max formulation (17) configures a mixed-integer nonlinear tri-level programming problem, whose solution is challenging. 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 [43]. In this regard, sophisticated decomposition or approximation methods are required for the model solutions, e.g., the recently developed "Column-and-Constraint Generation" (C&CG) method [44], is proven to be effective in dealing with mixed integer programming recourse problems [13, 25, 42].

4 Numerical Example

This section presents a simple numerical study involving IPGNs, adapted from [42]; the network layouts of the two systems are shown in Fig. 1. The interdependency relations are described as follows: the gas node g8 depends on the power demand node p11; the gas node g7 depends on the power demand node p10; the gas node g1 depends on the power demand node p4; the gas node g3 depends on the power demand node p9; the power generation node p1 depends on the gas demand node g9 [42].

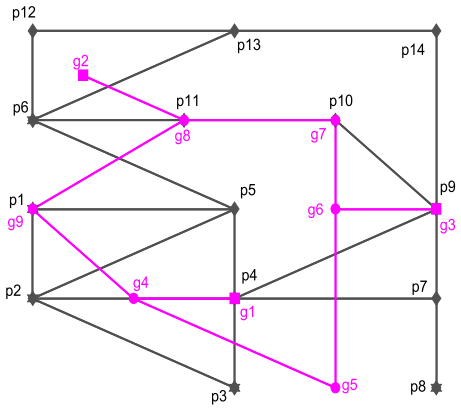

Fig. 1. The layout of the interdependent power and gas systems [42]

For simplicity, we assume that protecting one link in the interdependent CIs needs one unit of protection resources and set the cardinality constraint (16) to all possible link attacks. The weighting factor w^k is set as 0.5 for the resilience of both the power and gas systems.

We first investigate the resilience assessment of the IPGNs. Fig. 2 illustrates the worst-case system disruptions by attacking from one to five links and Fig. 3 shows the combined power and gas systems resilience associated with the worst attack disruptions, and the second worst (i.e., rank order 2) through fifth-worst (i.e., rank order 5) combination of system resiliences 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 overall system resilience to attacks.

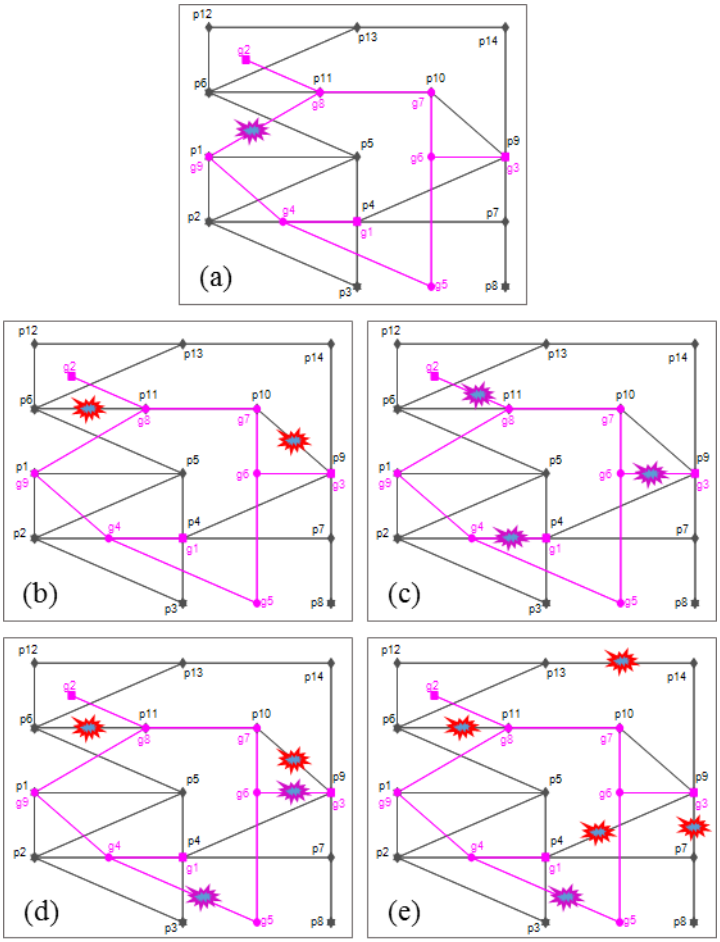

Fig. 2. Worst-case link attacks. (a) The worst-case single link attack is of link g8-g9, resulting in a combined power and gas system resilience R=0.782, i.e., 21.8% power and gas demands cannot be satisfied. (b) The worst-case two-link attack is of links p6-p11 and p9-p10, resulting in R=0.586. (c) The worst-case three-link attack is of links g1-g4, g2-g8, and g3-g6, resulting in

R=0.451. (d) The worst-case four-link attack is of links g3-g6, g4-g5, p6-p11, and p9-p10, resulting in R=0.429. (e) The worst-case five-link attack is of links p4-p9, p6-p11, p7-p9, p13-p14, and g4-g5, resulting in R=0.352.

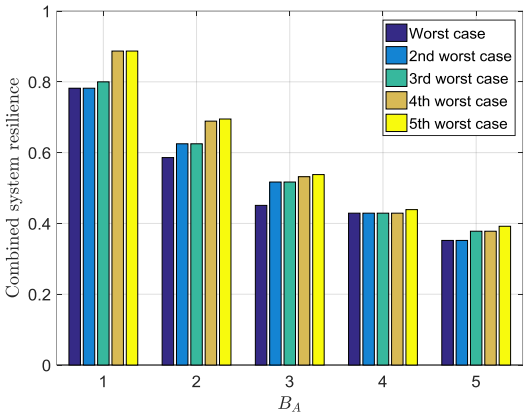

Fig. 3. The combined power and gas system resilience associated with the worst-case, the second-worst through the fifth-worst attacks for each attack budget

Second, when the protection investment is considered, we solve the DAD model for different combinations of protection budget B_P and attack budget B_A. Fig. 4 shows the combined power and gas 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.

Then, we investigate the importance of considering interdependency for system protection decisions. In practice, a coordinated protection 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 budget evenly to the power and gas 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 "separate protection" to differentiate it from the "coordinated protection" where the interdependent systems are protected as a whole. Fig. 5(a) shows the combined power and gas 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 those 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. Fig. 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 potential disruptions, especially when the protection budget is relatively high.

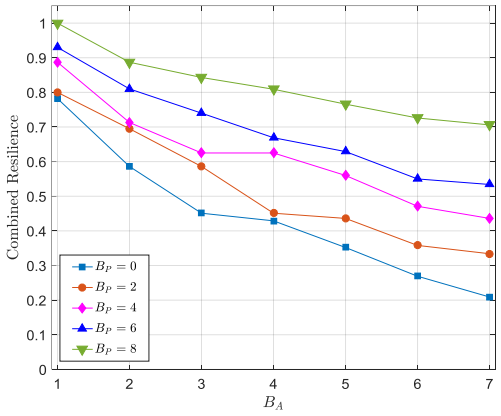

Fig. 4. The combined resilience of the interdependent power and gas systems

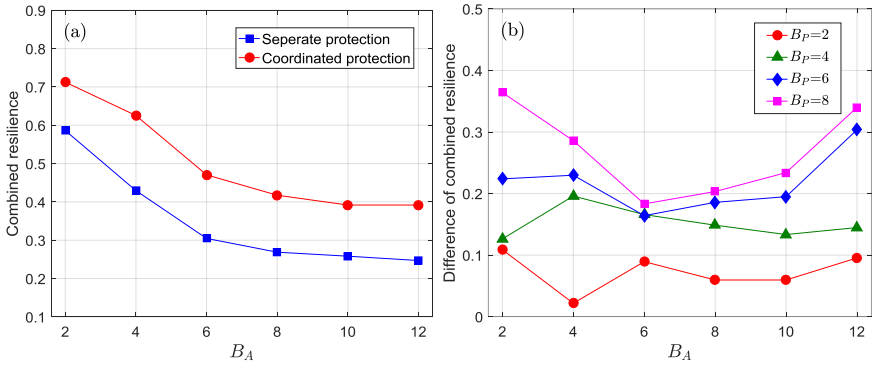

Fig. 5. (a) The combined system resilience curves as a function of the attack budget B_A for the separate protection and the coordinated protection when $B_P = 4$; (b) The combined resilience difference between the separate protection and the coordinated protection as a function of the attack budget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

5 Concluding Remarks

This chapter has introduced a set of quantitative models of operation of interdependent CI systems and their functional interdependencies. The game-theoretic AD and DAD models are introduced and advocated to be used for assessing and improving the resilience of interdependent CIs under worst-case disruptions. By assuming an intelligent attacker and exploiting its optimization, these multi-level defender-attacker models aim to estimate a worst case damage scenario for any feasible protection strategy. It is noted that the tri-level DAD game takes the identical form of two-stage adaptive robust optimization (ARO) [45, 46], albeit the DAD game model and the two-stage ARO have different origins. This modeling framework has been successfully applied to identify the optimum resilience strategies for electric power grids [25, 47, 48], rail systems [49], commodity distribution networks [24], and facility networks [50].

Although in the present models we restrict the adaptive behavior of the systems to the normative decisions (i.e., only network flow can be re-dispatched), the framework is also flexible enough to incorporate other adaptive behaviors/decisions in the presence of disruption, to the extent that one can describe the way in which this might happen. For example, we have shown in [13] that the decisions about the repair sequence of damaged components under limited repair resources can be carefully defined and incorporated into the third level system operation model after disruptions, resulting in a more comprehensive consideration of system resilience.

By considering the simultaneous losses of system components, the present model is agnostic about the source of a disruption, providing a rapid and objective way of calculating the consequence of damage to any set of components, and can, therefore, be used to identify vulnerabilities and to evaluate the improvement in resilience provided by any protection plan. Furthermore, as we have mentioned at the end of Section 3.2, when we are able to calculate the failure probabilities of system components, this information can be carefully formulated as additional constraints on $\boldsymbol{z}$, e.g., through Shannon's information theory, to narrow down the space $\mathbb{Z}$ and obtain the "most-likely" (informed by the failure probabilities) worst case disruptions.

Finally, our results of the numerical example demonstrate the significance of having a centralized decision maker to protect interdependent CIs as a whole against potential disruptions. However, in practice, many CI systems are owned or operated by the private sector and a centralized decision-making agent does not exist. Therefore, in terms of future research, it would be interesting to investigate whether and how different kinds of interaction/collaboration mechanisms among these independent decision-makers will improve the resilience of individual CI systems and all the interdependent CIs as a whole.

References

[1] Ellis, J., et al., *Report to the President's Commission on critical infrastructure protection.* 1997.

[2] Moteff, J., C. Copeland, and J. Fischer. *Critical infrastructures: What makes an infrastructure critical?* 2003. Library of Congress Washington DC Congressional Research Service.

[3] Zio, E., *Challenges in the vulnerability and risk analysis of critical infrastructures.* Reliability Engineering & System Safety, 2016. **152**: p. 137-150.

[4] Kröger, W. and E. Zio, *Vulnerable systems*. 2011: Springer Science & Business Media.

[5] 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.

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

[7] Vespignani, A., *Complex networks: The fragility of interdependency.* Nature, 2010. **464**(7291): p. 984.

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

[9] Council, N.I.A., *Critical Infrastructure Resilience: Final Report and Recommendations*. 2009: National Infrastructure Advisory Council.

[10] Government, A., *Australian Government's Critical Infrastructure Resilience Strategy*. 2010.

[11] Environment, S.o.S.f., *Food and Rural Affairs by Command of Her Majesty, Climate Resilient Infrastructure: Preparing for a Changing Climate.* 2011.

[12] Hosseini, S., K. Barker, and J.E. Ramirez-Marquez, *A review of definitions and measures of system resilience.* Reliability Engineering & System Safety, 2016. **145**: p. 47-61.

[13] Ouyang, M. and Y. Fang, *A mathematical framework to optimize critical infrastructure resilience against intentional attacks.* Computer‐Aided Civil and Infrastructure Engineering, 2017. **32**(11): p. 909-929.

[14] Fang, Y., *Critical infrastructure protection by advanced modelling, simulation and optimization for cascading failure mitigation and resilience*. 2015, Ecole Centrale Paris.

[15] 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.

[16] Westrum, R., *A typology of resilience situations*, in *Resilience engineering*. 2017, CRC Press. p. 67-78.

[17] Zolli, A. and A.M. Healy, *Resilience: Why things bounce back*. 2013: Simon and Schuster.
[18] Park, J., et al., *Integrating risk and resilience approaches to catastrophe management in engineering systems.* Risk Analysis, 2013. **33**(3): p. 356-367.
[19] Ayyub, B.M., *Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making.* Risk Analysis, 2014. **34**(2): p. 340-355.
[20] Francis, R. and B. Bekera, *A metric and frameworks for resilience analysis of engineered and infrastructure systems.* Reliability Engineering & System Safety, 2014. **121**: p. 90-103.
[21] Franchin, P. and F. Cavalieri, *Probabilistic assessment of civil infrastructure resilience to earthquakes.* Computer‐Aided Civil and Infrastructure Engineering, 2015. **30**(7): p. 583-600.
[22] Brown, G., et al., *Defending critical infrastructure.* Interfaces, 2006. **36**(6): p. 530-544.
[23] Bertsekas, D.P., *Constrained optimization and Lagrange multiplier methods*. 2014: Academic press.
[24] Alderson, D.L., G.G. Brown, and W.M. Carlyle, *Operational models of infrastructure resilience.* Risk Analysis, 2015. **35**(4): p. 562-586.
[25] Fang, Y. and G. Sansavini, *Optimizing power system investments and resilience against attacks.* Reliability Engineering & System Safety, 2017. **159**: p. 161-173.
[26] 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.
[27] Pederson, P., et al., *Critical infrastructure interdependency modeling: a survey of US and international research.* Idaho National Laboratory, 2006. **25**: p. 27.
[28] Ouyang, M., *A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks.* European Journal of Operational Research, 2017. **262**(3): p. 1072-1084.
[29] Gong, J., et al., *An interdependent layered network model for a resilient supply chain.* Omega, 2014. **46**: p. 104-116.
[30] González, A.D., et al., *The interdependent network design problem for optimal infrastructure system restoration.* Computer‐Aided Civil and Infrastructure Engineering, 2016. **31**(5): p. 334-350.
[31] Coffrin, C., P. Van Hentenryck, and R. Bent. *Last-Mile Restoration for Multiple Interdependent Infrastructures*. in *AAAI*. 2012.
[32] Zio, E., *Reliability engineering: Old problems and new challenges.* Reliability Engineering & System Safety, 2009. **94**(2): p. 125-141.

[33] Enrico, Z., *An introduction to the basics of reliability and risk analysis*. Vol. 13. 2007: World scientific.

[34] Aven, T. and E. Zio, *Some considerations on the treatment of uncertainties in risk assessment for practical decision making.* Reliability Engineering & System Safety, 2011. **96**(1): p. 64-74.

[35] DEng, P.G. and F. FEI, *Infrastructure resilience for high-impact low-chance risks.* Proceedings of the Institution of Civil Engineers, 2012. **165**(6): p. 13.

[36] Panteli, M. and P. Mancarella, *The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience.* IEEE Power and Energy Magazine, 2015. **13**(3): p. 58-66.

[37] Council, N.R., *Committee to Review the Department of Homeland Security's Approach to Risk Analysis. Review of the Department of Homeland Security's Approach to Risk Analysis*. 2010, Washington, DC: National Academies Press.

[38] Brown, G.G. and L.A.T. Cox Jr, *How probabilistic risk assessment can mislead terrorism risk analysts.* Risk Analysis, 2011. **31**(2): p. 196-204.

[39] Davis, C., et al., *Prediction of landfalling hurricanes with the advanced hurricane WRF model.* Monthly weather review, 2008. **136**(6): p. 1990-2005.

[40] Booker, G., et al., *Estimating cellular network performance during hurricanes.* Reliability Engineering & System Safety, 2010. **95**(4): p. 337-344.

[41] Fang, Y., G. Sansavini, and E. Zio, *An Optimization-Based Mathematical Framework for the Identification of Infrastructure Vulnerabilities under Natural Hazards.* Under Review, 2018.

[42] Fang, Y. and E. Zio. *Optimizing the resilience of interdependent infrastructure systems against intentional attacks*. in *ICSRS 2017*. 2017.

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

[44] 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.

[45] Bertsimas, D., D.B. Brown, and C. Caramanis, *Theory and applications of robust optimization.* SIAM review, 2011. **53**(3): p. 464-501.

[46] Ruiz, C. and A.J. Conejo, *Robust transmission expansion planning.* European Journal of Operational Research, 2015. **242**(2): p. 390-401.

[47] Alguacil, N., A. Delgadillo, and J.M. Arroyo, *A trilevel programming approach for electric grid defense planning.* Computers & Operations Research, 2014. **41**: p. 282-290.

[48] Yuan, W., et al., *Robust optimization-based resilient distribution network planning against natural disasters.* IEEE Transactions on Smart Grid, 2016. **7**(6): p. 2817-2826.

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

[50] Losada, C., M.P. Scaparra, and J.R. O'Hanley, *Optimizing system resilience: a facility protection model with recovery time.* European Journal of Operational Research, 2012. **217**(3): p. 519-530.