A Synthesis of Optimization Approaches for Tackling Critical Information Infrastructure Survivability

Annunziata Esposito Amideo, Maria Paola Scaparra

Kent Business School, University of Kent, Canterbury, UK
{ae306, m.p.scaparra}@kent.ac.uk

Abstract. Over the years, Critical Infrastructures (CI) have revealed themselves to be extremely disaster-prone, be the disasters nature-based or man-made. This paper focuses on a specific category of CI: Critical Information Infrastructures (CII), which are commonly deemed to include communication and information networks. The majority of all the other CI (e.g. electricity, fuel and water supply, transport systems, etc.) are crucially dependent on CII. Therefore, problems associated with CII that disrupt the services they are able to provide (whether to a single end-user or to another CI) are of increasing interest. This paper discusses some recent developments in optimization models regarding CII's ability to withstand disruptive events within three main spheres: network survivability assessment, network resource allocation strategy and survivable design.

Keywords: Critical Information Infrastructures (CII) · Survivability · Resource Allocation Strategy · Survivable Network Design

1 Introduction

Infrastructures considered critical (CI) are those physical and information-based facilities, networks and assets which if damaged would have serious impacts on the well-being of citizens, proper functioning of governments and industries or result in other adverse effects [20]. The nature of these infrastructures, along with the potential threats arising from disasters, whether nature-based or man-made, has prompted what is referred to as Critical Infrastructure Protection (CIP).

This paper focuses on a specific category of CI, namely the Critical Information Infrastructures (CII), and reviews recent developments in the optimization field aimed at addressing Critical Information Infrastructure Protection (CIIP) issues.

CII are described as those systems, belonging to the Information and Communication Technology, which are critical - not just for their own sakes, but for other CI that rely on them (e.g., transportation) [36]. Examples of CII are the public telephone network, Internet, terrestrial and satellite wireless networks and so on and so forth [25].

CIIP is defined as those plans and strategies developed by network operators, infrastructure owners and others, aimed at keeping the service level of CII above a predetermined threshold, despite the occurrence of disruptive events of various natures [35]. It is clear that CII are key elements in production and service systems. Even a

local failure at the single CII level (e.g. shut down servers, interrupted cable connections, etc.) may prompt far-reaching adverse effects on the CI relying on it. Bigger disruptions may have even more catastrophic cascading consequences. For example, the 2001 World Trade Center attacks crippled communications by destroying telephone and Internet lines, electric circuits and cellular towers ([10], [18]). This caused a cascade of disruptions at all levels, from fuel shortages, to transportation and financial services interruptions.

The disruptive events that can affect CII are primarily identified as physical attacks or cyber-attacks. This paper focuses on the former. Three main issues emerge. First, what are the most critical elements of the system that, if disrupted, would interrupt or significantly degrade the system's normal functioning? Second, how can such an interruption be prevented or mitigated by resource allocation plans, aimed either at hardening system elements or at recovering service? Third, is it possible and worthwhile to design and establish infrastructures that are intrinsically able to resist service failure when a disruptive event occurs?

The main optimization models developed to address these issues can be categorized as follows:

1. Survivability-oriented interdiction models, aimed at identifying interdiction scenarios of CII and quantifying the consequences deriving from potential losses of system critical components in terms of ability to provide service;
2. Resource allocation strategy models, aimed at optimizing the allocation of resources (i.e., budget) among the components of already existent systems in order to either protect them or to re-establish service level; and
3. Survivable design models, aimed at planning new CII which are able to meet survivability criteria when disruptive events occur.

In this paper, we provide a description of the seminal models in each category and suggest how these models can be taken as the starting point for further development in the CIIP field.

The remainder of this paper is organized as follows. Survivability-oriented interdiction, resource allocation strategy and survivable design models are described in Sections 2, 3 and 4, respectively. In Section 5, further research suggestions in modeling CIIP problems are discussed. Section 6 offers concluding remarks.

2 Identifying Critical Network Components: Survivability-Oriented Interdiction Models

The identification of critical components in network-based systems can be traced back to a few decades ago in the context of transportation infrastructures for military purposes [38]. More recently, [4] introduced optimization models for identifying critical facilities in service and supply systems.

Interdiction models, as referred to in the literature, identify network components which are the most critical, i.e. the ones that, if disrupted, inflict the most serious damage to the system. The importance of these kinds of models is easily understanda-

ble: they not only shed light on a system's major vulnerabilities, but also help form the basis for developing protection and/or recovery plans.

Interdiction models are driven by specified criteria (also called impact metrics). When dealing with CII, such as communication and information networks, the two important criteria are network reliability and network survivability. In [31], network reliability is defined as the probability measure that a network functions according to a predefined specification; whereas, network survivability is defined as the ability of a network to maintain its communication capabilities in the face of equipment failure. Moreover, according to [31], it is possible to subdivide network survivability into two categories: physical survivability and logical survivability. A network is physically survivable if after the physical failure of some nodes or arcs, a path connecting all the nodes still exists. Logical survivability is about survivability at higher levels of the OSI model and assumes that the underlying physical network is survivable.

Our interest is in evaluating how disruptive events impact a network's physical survivability by identifying its critical components, which can be nodes and/or arcs. In the case of communication and information networks, nodes can be switches, multiplexers, cross-connects, routers; arcs represent connections among them [31, 32].

Murray [18] identifies four metrics to evaluate network physical survivability: maximal flow ([38]), shortest path ([7]), connectivity ([14], [31]), and system flow ([17], [19]). Here we provide an example of an optimization model designed to ascertain the survivability of system flow. This model is a variation of the model introduced in [19] and later extended and streamlined in [17]. It identifies the r most vital components of a network, i.e. those components which, if disrupted, maximize the amount of flow that can no longer be routed over the network. In the specific case of CII, the flow represents data and information. In the following, we will refer to this model as the Survivability Interdiction model (SIM).

Given a network $G(N, A)$, where N is the set of nodes and A is the set of arcs, let Ω be the set of origin nodes, indexed by o; H the set of elements (nodes/arcs) that can be disrupted, indexed by h; Δ the set of destination nodes, indexed by d, P the set of paths, indexed by p; N_{od} the set of paths enabling flow between an origin-destination pair o-d; Φ_p the set of components belonging to path p; f_{od} the flow routed between an o-d pair; and r the number of components to be disabled. The decision variables are: S_h equal to 1 if component h is disrupted, 0 otherwise; and X_{od} equal to 1 if flow cannot be routed between a pair o-d, 0 otherwise. The mathematical formulation is:

$$max\ z = \sum_{o\in\Omega}\sum_{d\in\Delta} f_{od}X_{od} \quad (1)$$

s.t.

$$\sum_{h\in\phi_p} S_h \geq X_{od} \qquad \forall\ o \in \Omega, d \in \Delta, p \in N_{od} \quad (2)$$

$$\sum_{h\in H} S_h = r \quad (3)$$

$$S_h \in \{0,1\} \qquad \forall\ \mathrm{h} \in H \quad (4)$$

$$X_{od} \in \{0,1\} \qquad \forall\ o \in \Omega, d \in \Delta \quad (5)$$

The objective function (1) maximizes the total flow disrupted (or interdicted). Constraints (2) state that the flow between an o-d pair can be considered lost ($X_{od} = 1$),

only if every path connecting nodes o and d is affected by the disruption (i.e., at least one of its arc is disrupted). Constraint (3) is a typical cardinality constraint which stipulates that exactly r arcs are to be disrupted. Finally, constraints (4) and (5) represent the binary restrictions on the interdiction and flow variables, respectively.

The original SIM in [19] only considers arc disruption. It was later modified to address node disruption in [17]. This work also presents a variant of SIM which identifies lower bounds to the flow loss caused by the disruption of r nodes, thus allowing the assessment of both best-case and worst-case scenario losses. This kind of analysis is useful to build the so-called reliability envelope, a diagram originally developed in [22] to depict possible outcomes for the failure of communication systems. SIM was applied to the Abilene network, an Internet-2 backbone with 11 routers and 14 linkages connecting US institutions. The analysis shows that the worst-case interdiction of one node (Washington, D.C.) can cause a data flow decrease of over 37%; a two-node interdiction scenario (Washington, D.C. and Indianapolis) a decrease of over 73%.

One arguable aspect of existing interdiction models such as SIM is that the number of components to be disrupted is fixed to a specific and known value r. This assumption is made to capture the possible extents of disruptive events: large values of r mimic large disruptions involving the simultaneous loss of several components, while small values are used to model minor disruptions [15]. In practice, it is difficult to anticipate the extent of a disruption and therefore select a suitable r value. In addition, the critical components identified for a small r value are not necessarily a subset of the critical components identified for larger values. Consequently, these models are usually run for several values of r so as to identify the most vital components across disruption scenarios of different magnitude [17].

Another aspect worth mentioning is that the use of cardinality constraints like (3) is useful for identifying worst-case scenario losses caused by natural disasters. However, in case of malicious attacks, models must capture the fact that different amount and type of resources (e.g., human, financial etc.) may be needed in a concerted attack to fully disable network components and cause maximum damage [28]. From an attacker's perspective, in fact, resources may vary significantly according to the target. This is particularly true within the context of physical survivability as opposed to logical survivability. For example, a physical attack on a relatively small number of major switching centers for long-distance telecommunications may require considerably more resources than launching a logic denial-of-service attack on the Internet. However, the former type of attack may cause much longer lasting damage [13].

This aspect can be captured by either replacing (3) with a budget constraint (see [1] and [15] in the context of distribution systems) or by developing models that directly minimize the attacker expenditure to achieve a given level of disruption. Examples of the latter can be found in [14]. This work presents some mixed integer programming models which minimize the cost incurred by an attacker to disconnect the network according to different survivability metrics (e.g., degree of disconnectivity). These attacker models are then used to assess the robustness of two protection resource allocation strategies: a uniform allocation (the defense budget is distributed equally among the nodes) and a degree-based allocation (the budget is distributed

among the nodes proportionally to their degree of connectivity). As it will be discussed in the next section, this approach, where protection decisions are not tackled explicitly within a mathematical model but are only assessed and/or developed on the basis of the results of an interdiction model, often leads to a suboptimal allocation of protective resources.

Another aspect that interdiction models must capture is the fact that the outcome of an attack is highly uncertain. When dealing with malicious disruptions, this is a crucial issue as attackers, such as terrorists or hackers, aim at allocating their offensive resources so as to maximize their probability of success. Clearly, there is a correlation between the amount of offensive resources invested and the probability of success of an attack: the more the former, the higher the latter. Church and Scaparra [5] introduce an interdiction model for distribution systems where an interdiction is successful with a given probability and the objective is to maximize the expected disruption of an attack on r facilities. Losada et al. [15] further extend this model by assuming that the probability of success of an interdiction attempt is dependent on the magnitude/intensity of the disruption. Similar extensions could be developed for SIM to assess the survivability of physical networks to attacks with uncertain outcomes.

3 Enhancing Critical Network Survivability: Resource Allocation Strategy Models

Optimization approaches can be used to improve CII survivability by optimizing investments in protection measures and in service recovery plans.

CII protection measures may be divided into three different categories: technical (e.g. security administration), management (e.g. security awareness, technical training) and operational (e.g. physical security) (see [37]). Our interest lies in the last category. Examples of physical security measures include: alarms, motion detectors, biometric scanners, badge swipes, access codes, and human and electronic surveillance, e.g. Perimeter Intruder Detection Systems (PIDS) and Closed Circuit Television (CCTV) [20]. In a broader sense, protection strategies may include increasing redundancy and diversity [34]. Redundancy consists in creating one or more copies of the same network element/content and is key to tackle random uncorrelated failures. Diversity aims at avoiding components of a system to undergo the same kind of failure and is used to tackle correlated failures.

Service recovery is intimately connected with the concept of survivability since it involves bringing the infrastructure to the level of service it was able to provide before a disruption and, normally, as timely as possible. In this perspective, optimization approaches provide a useful tool to identify the optimal trade-off between the level of service to restore and the amount of resources to invest over a certain time horizon.

3.1 Optimization Models for Protecting CII Physical Components

Although interdiction models like SIM are instrumental for the identification of the most critical CII components, protection resource allocation approaches which solely

rely on this information to prioritize protection investments often result in suboptimal defensive strategies ([2], [6]). This is due to the fact that when a component (e.g., the most critical) is protected, the criticality of the other components may change. Protections and interdictions decisions must therefore be addressed in an integrated way. This is typically done by using bi-level optimization programs [8]. These programs are hierarchical optimization models which emulate the game between two players, referred to as leader and follower. In the CIIP context, the leader is the network operator or infrastructure owner, who decides which system components to protect; the follower represents a saboteur (hacker or terrorist) who tries to inflict maximum damage to the system by disabling some of its components. The defender decisions are modeled in the upper level program, whereas the inner-level program models the attacker decisions and, therefore, computes worst-case scenario losses in response to the protection strategy identified in the upper level.

Below we present a bi-level program for CIIP, which embeds SIM in the inner-level. We refer to it as the Survivability Protection Problem (SPP). In addition to the parameters and variables defined in Section 2, SPP uses the following notation: B is the total budget available for protection; c_h is the unit cost for protecting component h; Z_h is a decision variable equal to 1 if component h is protected, 0 otherwise.

SPP can be formulated as follows:

$$min\ H(z) \tag{6}$$

s.t.

$$\sum_{h\in H} c_h Z_h \leq B \tag{7}$$

$$Z_h \in \{0,1\} \qquad \forall\ \mathrm{h} \in H \tag{8}$$

$$H(z) = max \sum_{o\in\Omega} \sum_{d\in\Delta} f_{od} X_{od} \tag{9}$$

s.t.

(2) - (5)

$$S_h \leq 1 - Z_h \qquad \forall\ \mathrm{h} \in H \tag{10}$$

The upper level model identifies which network components to protect given limited budgetary resources (7) so as to minimize a function, $H(z)$, which represents the highest flow loss (6) resulting from the interdiction of r components. The inner-level model is the SIM with the additional set of constraints (10) which guarantee that if a component is protected, it cannot be attacked.

Protection models like SPP can be extended in a number of ways. For example, protection investments over time could be considered, given that funds for enhancing CI security usually become available at different times. An example of bi-level protection models that considers dynamic investments can be found in [33] within the context of transportation infrastructure. Probabilistic extensions of SPP should also be considered, where the protection of an element does not completely prevent its interdiction, but may reduce its probability of failure. Other issues that should be captured are the uncertainty in the number of simultaneous losses of components (see for example [11]), and the correlation among components failures [12].

Obviously, there are other approaches other than bi-level programming which can be used to optimize protection strategies. For example, Viduto et al. [37] combine a

risk assessment procedure for the identification of system risks with a multi-objective optimization model for the selection of protection countermeasures. To mitigate cyber-threats, Sawik [27] uses mixed integer models in conjunction with a conditional value-at-risk approach to identify optimal protection countermeasure portfolios under different risk preferences of the decision maker (risk-adverse vs. risk neutral).

3.2 Optimization Models for CII Service Restoration

An interesting model for the optimization of recovery investments is the Networked Infrastructure Restoration Model (NIRM) introduced in [16]. NIRM is a multi-objective optimization model for the evaluation of tradeoffs between flow restoration and system costs over time.

NIRM uses the following additional notation: Γ^n is the set of inoperable nodes, Γ^l the set of inoperable arcs, Φ_p^n the set of disrupted nodes along path p, Φ_p^l the set of disrupted arcs along path p, T the set of planning periods; f_{od} is the flow routed between the pair o-d; c_{pt} the cost of traversing path p during planning period t; λ_i and λ_j the costs of restoring operation at node i and arc j, respectively; H_t^n and H_t^l the budget for node and arc restoration during planning period t; β_t the weight for importance of repair in time t; C_{odt} is a large quantity representing the cost of a disrupted pair o-d during planning period t. The decision variables are: Y_{pt}, equal to 1 if path p is available in time t, 0 otherwise; V_{it}^n (V_{jt}^l,) equal to 1 if node i (arc j) is restored in time t, 0 otherwise; and W_{odt}, equal to 1 if connectivity does not exist between a pair o-d in time t, 0 otherwise. The formulation is the following:

$$max \ \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{p\in N_{od}}\sum_{t\in T}\beta_t f_{od} Y_{pt} \quad (11)$$

$$min \ \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{t\in T} C_{odt} W_{odt} + \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{p\in N_{od}}\sum_{t\in T} c_{pt} Y_{pt} \quad (12)$$

s.t.

$$\sum_{i\in\Gamma^n} \lambda_i V_{it}^n \le H_t^n \qquad \forall\, t \in T \quad (13)$$

$$\sum_{j\in\Gamma^l} \lambda_j V_{jt}^l \le H_t^l \qquad \forall\, t \in T \quad (14)$$

$$\sum_{t\in T} V_{it}^n \le 1 \qquad \forall\, i \in \Gamma^n \quad (15)$$

$$\sum_{t\in T} V_{jt}^l \le 1 \qquad \forall\, j \in \Gamma^l \quad (16)$$

$$Y_{pt} - \sum_{\hat{t}\le t} V_{i\hat{t}}^n \le 0 \qquad \forall\, p \in P, i \in \Phi_p^n, t \in T \quad (17)$$

$$Y_{pt} - \sum_{\hat{t}\le t} V_{j\hat{t}}^l \le 0 \qquad \forall\, p \in P, j \in \Phi_p^l, t \in T \quad (18)$$

$$\sum_{p\in N_{od}} Y_{pt} + W_{odt} = 1 \qquad \forall\, o \in \Omega, d \in \Delta, t \in T \quad (19)$$

$$Y_{pt} \in \{0,1\} \qquad \forall\, p \in P, t \in T \quad (20)$$

$$V_{it}^n \in \{0,1\} \qquad \forall\, i \in \Gamma^n, t \in T \quad (21)$$

$$V_{jt}^l \in \{0,1\} \qquad \forall\, j \in \Gamma^l, t \in T \quad (22)$$

$$W_{odt} = \{0,1\} \qquad \forall\, o \in \Omega, d \in \Delta, t \in T \quad (23)$$

The objective function (11) maximizes system flow or connectivity while objective (12) minimizes system cost and it is made up of two components, disruption and path usage. Constraints (13) and (14) are budget constraints on node and arc recovery in each planning period t. Constraints (15) and (16) restrict node and arc repair to a sin-

gle time period. Constraints (17) and (18) state that a path p is available in period t only if each of its disrupted component (node i or arc j respectively) is repaired in period t or in any of the preceding time periods. Constraints (19) track o-d pairs that are not connected in each time period and force the selection of at most one path between each o-d pair in each time period. Finally, constraints (20)-(23) represent the binary restrictions on the decision variables.

NIRM was applied to support recovery planning after a simulated High Altitude Electromagnetic Pulse attack on a sample telecommunications backbone network with 46 routers and 94 high-capacity backbones. Different restoration schedules over 6 repair periods were generated and analyzed so as to highlight the tradeoffs between flow restoration and system costs.

A limitation of NIRM is that the repair action is assumed to be instantaneous. Nurre et al. [21] consider the duration for component repair in an integrated restoration planning optimization model which identifies the network components to be installed/repaired after a disruption and schedules them to available work groups. The objective is to maximize the cumulative amount of flow that can be routed across the network over a finite planning horizon. An interesting addition to the restoration modeling literature is the model in [29] which considers the important issue of restoring multiple interdependent infrastructure systems (e.g., power, telecommunication, water). This work also presents tools to quantify the improvement in restoration effectiveness resulting from information sharing and coordination among infrastructures.

4 Planning Survivable Networks: Design Models

Given the crucial importance of CII to the vast majority of economic activities and services, telecommunication and information systems are designed in such a way that they are intrinsically survivable, i.e. they satisfy some more or less stringent connectivity criteria. The design of survivable network is a well-studied problem in the optimization field. For an early survey, the interested reader can refer to [31]. A comprehensive review of survivable network design models would be outside the scope of this paper. To provide a complete treatment of survivability related optimization problems, we only briefly discuss the Survivable Network Design (SND) model found in [32], one of the earliest and most studied models.

Given an undirected graph $G(N, E)$, where N is the set of nodes and E is the set of undirected edges (i, j), each pair of communicating nodes is identified as a commodity k (being K the set of the commodities), whose origin and destination are labeled as $O(k)$ and $D(k)$ respectively. Let c_{ij} be the design cost of edge (i, j), and q the number of node disjoint paths required for all the commodities (so the system will be able to face $q - 1$ failures at most). The decision variables are: U_{ij} equal to 1 if edge (i, j) is included in the design, 0 otherwise; and X_{ij}^{k} equal to 1 if commodity k uses edge (i, j), 0 otherwise. The formulation is the following:

$$min\ z = \sum_{(i,j)\in E} c_{ij} U_{ij} \qquad (24)$$

s.t.

$$\sum_{j\in N} X_{ij}^k - \sum_{j\in N} X_{ji}^k = \begin{cases} Q \text{ if } i \equiv O(k) \\ -Q \text{ if } i \equiv D(k) \\ 0 \text{ otherwise} \end{cases} \quad \forall\, k \in K \qquad (25)$$

$$X_{ij}^k \leq U_{ij} \qquad \forall\, k \in K, (i,j) \in E \qquad (26)$$

$$X_{ji}^k \leq U_{ij} \qquad \forall\, k \in K, (i,j) \in E \qquad (27)$$

$$\sum_{i\in N} X_{ij}^k \leq 1 \qquad \forall\, k \in K, j \in N \ \wedge j \neq D(k) \qquad (28)$$

$$X_{ij}^k, X_{ji}^k = \{0,1\} \qquad \forall\, k \in K, i,j \in N \qquad (29)$$

$$U_{ij} = \{0,1\} \qquad \forall\, i,j \in N \qquad (30)$$

The objective function (24) minimizes the cost of the topological network design. Constraints (25) guarantee network flow conservation. Constraints (26) and (27) stipulate that flow can traverse an edge only if the edge is included in the design. The combined use of constraints (25), (26) and (27) enforce the edge-disjoint paths over the network. Constraints (28) guarantee that at most one unit of flow can traverse a node that is neither a commodity origin nor destination, thus ensuring the correct number of node-disjoint paths in the network. Finally, constraints (29) and (30) represent the binary restrictions on the variables.

Many other survivable network design models can be found in the literature which differ in terms of underlying network (wired vs. wireless), network topology (e.g., ring, mesh, star, line, tree, etc.), connectivity requirements (e.g., edge and/or vertex-connectivity), path-length restrictions (e.g., hop limits [24]), cost minimization [23], and dedicated settings (e.g., path protection, link and path restoration [24]) .

Note that recent survivability design models embed interdiction models to ascertain components criticality ([3], [30]). Such models are able to identify cost-effective CII configurations which are inherently survivable without the need to specify the number of disjoint paths required between each pair of communicating nodes, like in SND.

5 Future research suggestions

The research on CIIP issues aimed at hedging against potential physical attacks is still evolving. The demand for such work has been prompted by disasters of diverse nature, with 9/11 being a seminal one.

The survivability optimization models discussed in this paper are basic models that can be extended in a number of ways. For example, interdiction and protection models could be extended to tackle both physical and logical survivability issues by incorporating routing and link capacity assignment decisions. In addition, most of the optimization models developed so far are deterministic. However, failures and disruptions are random events, often difficult to predict. The probabilistic behaviour of complex CII under disruptions would be better modelled by using stochastic models, including uncertain parameters (e.g., uncertainty on arc / node availability, extent of a disruption, stochastic repair times, etc.). Alternatively, the uncertainty characterizing disruptions could be captured in scenario-based models which incorporate robustness

measures for the identification of solutions which perform well across different disruption scenarios [26].

Future models could even combine the optimization of protection and restoration strategies in a unified framework so as to distribute resources efficiently across the different stages of the disaster management cycle (protection plans belong to the pre-disaster stage while recovery plans refer to the post-disaster stage). Other resource allocation models could consider identifying tradeoff investments in physical protection and cyber-security to mitigate the impact of both physical and logical attacks. Models which address design and restoration issues conjunctively, such as the one in [23], also deserve further investigation.

The models discussed in this paper have been solved by using a variety of optimization algorithms, including exact methods (e.g., decomposition) and heuristics (e.g. evolutionary algorithms). The development of more complex models, such as stochastic, bi-level and multi-objective models, would necessarily require additional research into the development of more sophisticated solution techniques, possibly integrating exact and heuristic methodologies.

Eventually, the ultimate challenge when developing optimization approaches for increasing CII survivability is to consider the interdependency among multiple CI and the potential cascading failures across different lifeline systems. As noted in [29], information sharing and coordination among infrastructures significantly improve the effectiveness of survivability strategies, as opposed to decentralized decision making. However, existing models that address network interdependencies are either overly simplistic or too theoretical [9]. This area certainly warrants further research.

6 Conclusions

This paper reviewed the research activities conducted over recent years in the field of CIIP aimed at mitigating the effects of physical attacks against CII components. This paper has investigated three main research areas: survivability assessment models, resource allocation strategy models (aimed at either protection or recovery plans), and survivable design models.

Each model category has been designed to identify different crucial aspects: (a) under what circumstances is the infrastructure still able to provide its service; (b) how should resources be allocated in order to protect the infrastructure physical components or to restore its level of service; (c) how should a new infrastructure be designed in order to be naturally survivable.

The optimization models hereby discussed are valuable decision-making tools in tackling CII survivability issues but future work is undoubtedly needed. The reason lies in the intrinsic nature of CII: they are large-scale, heterogeneous, distributed systems whose complexity is continuously evolving in a risky environment. As such, modeling their dynamics and interdependency with other lifeline systems requires developing cutting-edge methodologies, which integrate methods from different disciplines (e.g., optimization, simulation, risk analysis, complex network theory and statistics) in a unified framework.

References

1. Aksen D., Piyade N., Aras N.: The budget constrained r-interdiction median problem with capacity expansion. Cent.Europ.J.Oper.Re. 18, 3, 269-291 (2010).
2. Cappanera P., Scaparra M.P.: Optimal allocation of protective resources in shortest-path networks. Transport.Sci. 45, 1, 64-80 (2011).
3. Chen R.L., Cohn A., Pinar A.: An implicit optimization approach for survivable network design. In: Network Science Workshop (NSW), pp. 180-187, IEEE (2011).
4. Church R. L., Scaparra M.P., Middleton R.S.: Identifying critical infrastructure: The median and covering facility interdiction problems. Ann.Assoc.Am.Geogr. 94, 3, 491-502 (2004).
5. Church R.L., Scaparra M.P.: Analysis of facility systems' reliability when subject to attack or a natural disaster. In: Critical infrastructure, pp. 221-241. Springer (2007).
6. Church R. L., Scaparra M.P.: Protecting critical assets: The r-interdiction median problem with fortification. Geogr.Anal. 39, 2, 129-146 (2007).
7. Corley H., David Y.S.: Most vital links and nodes in weighted networks. Oper.Res.Lett. 1, 4, 157-160 (1982).
8. Dempe S.: Foundations of bilevel programming. Springer Science & Business Media (2002).
9. Fang Y.: Critical infrastructure protection by advanced modelling, simulation and optimization for cascading failure mitigation and resilience. Dissertation. Ecole Centrale Paris (2015).
10. Grubesic T. H., O'Kelly M.E., Murray A.T.: A geographic perspective on commercial internet survivability. Telematics Inf. 20, 1, 51-69 (2003).
11. Liberatore F., Scaparra M.P., Daskin M.S.: Analysis of facility protection strategies against an uncertain number of attacks: The stochastic R-interdiction median problem with fortification. Comput.Oper.Res. 38, 1, 357-366 (2011).
12. Liberatore F., Scaparra M.P., Daskin M.S.: Hedging against disruptions with ripple effects in location analysis. Omega 40, 1, 21-30 (2012).
13. Lin H.S., Patterson D.A., Hennessy J.L.: Information Technology for Counterterrorism: Immediate Actions and Future Possibilities. National Academies Press (2003).
14. Lin F.Y., Yen H., Chen P., Wen Y.: Evaluation of network survivability considering degree of disconnectivity. In: International Conference on Hybrid Artificial Intelligent Systems, pp. 51-58, Springer (2011).
15. Losada C., Scaparra M.P., Church R.L., Daskin M.S.: The stochastic interdiction median problem with disruption intensity levels. Ann.Oper.Res. 201, 1, 345-365 (2012).
16. Matisziw T. C., Murray A.T., Grubesic T.H.: Strategic network restoration. Netw.Spat.Econ. 10, 3, 345-361 (2010).
17. Murray A. T., Matisziw T.C., Grubesic T.H.: Critical network infrastructure analysis: Interdiction and system flow. J.Geogr.Syst. 9, 2, 103-117 (2007).
18. Murray A. T.: An overview of network vulnerability modeling approaches. GeoJournal 78, 2, 209-221 (2013).
19. Myung Y., Kim H.: A cutting plane algorithm for computing k-edge survivability of a network. Eur.J.Oper.Res. 156, 3, 579-589 (2004).

20. Nickolov E.: Critical information infrastructure protection: Analysis, evaluation and expectations. INFORMATION AND SECURITY 17, 105-119 (2006).
21. Nurre S. G., Cavdaroglu B., Mitchell J.E., Sharkey T.C., Wallace W.A.: Restoring infrastructure systems: An integrated network design and scheduling (INDS) problem. Eur.J.Oper.Res. 223, 3, 794-806 (2012).
22. O'Kelly M.E., Kim H.: Survivability of commercial backbones with peering: A case study of korean networks. In: Critical infrastructure, pp. 107-128. Springer (2007).
23. Orlowski S., Wessäly R.: Comparing restoration concepts using optimal network configurations with integrated hardware and routing decisions. J.Netw.Syst.Manag. 13, 1, 99-118 (2005).
24. Orlowski S., Wessäly R.: The effect of hop limits on optimal cost in survivable network design. In: Telecommunications planning: Innovations in pricing, network design and management, pp. 151-166. Springer US (2006).
25. Patterson C.A., Personick S.D.: Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. National Academies Press (2003).
26. Peng P., Snyder L.V., Lim A., Liu Z.: Reliable logistics networks design with facility disruptions. Transport. Res.B-Meth. 45, 8, 1190-1211 (2011).
27. Sawik T.: Selection of optimal countermeasure portfolio in IT security planning. Decis.Support Syst. 55, 1, 156-164 (2013).
28. Scaparra M.P., Church R.L.: Location problems under disaster events. In: Location science, pp. 623-642. Springer (2015).
29. Sharkey T. C., Cavdaroglu B., Nguyen H., Holman J., Mitchell J.E., Wallace W.A.: Interdependent network restoration: On the value of information-sharing. Eur.J.Oper.Res. 244, 1, 309-321 (2015).
30. Smith J. C., Lim C., Sudargho F.: Survivable network design under optimal and heuristic interdiction scenarios. J.Global Optim. 38, 2, 181-199 (2007).
31. Soni S., Gupta R., Pirkul H.: Survivable network design: The state of the art. Inf.Syst.Front. 1, 3, 303-315 (1999).
32. Soni S., Pirkul H.: Design of survivable networks with connectivity requirements. Telecommun.Syst. 20, 1-2, 133-149 (2002).
33. Starita S., Scaparra M.P.: Optimizing dynamic investment decisions for railway systems protection. Eur.J.Oper.Res. 248, 2, 543-557 (2016).
34. Sterbenz J. P., Hutchison D., Çetinkaya E.K., Jabbar A., Rohrer J.P., Schöller M., Smith P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Comput.Netw. 54, 8, 1245-1265 (2010).
35. Suter M., Brunner E.: International CIIP handbook 2008/2009. (2008).
36. Theron P.: Critical Information Infrastructure Protection and Resilience in the ICT Sector. IGI Global (2013).
37. Viduto V., Maple C., Huang W., López-Peréz D.: A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decis.Support Syst. 53, 3, 599-610 (2012).
38. Wollmer R.: Removing arcs from a network. Oper.Res. 12, 6, 934-940 (1964).