European Journal of Operational Research 283 (2020) 797–811

Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Invited Review

A survey of network interdiction models and algorithms

J. Cole Smith*, Yongjia Song

Department of Industrial Engineering, Clemson University, United States

ARTICLE INFO

Article history:
Received 24 December 2018
Accepted 13 June 2019
Available online 18 June 2019

Keywords:
Networks
Network interdiction
Min-max games
Mixed integer programming formulations
Decomposition algorithms

ABSTRACT

This paper discusses the development of interdiction optimization models and algorithms, with an emphasis on mathematical programming techniques and future research challenges in the field. After presenting basic interdiction concepts and notation, we recount the motivation and models behind founding research in the network interdiction field. Next, we examine some of the most common means of solving interdiction problems, focusing on dualization models and extended formulations solvable by row-generation techniques. We then examine contemporary interdiction problems involving incomplete information, information asymmetry, stochasticity, and dynamic play. We conclude by discussing several emerging applications in the field of network interdiction.

1. Introduction

In the defense context, *interdiction* refers to actions that serve to block or otherwise inhibit an adversary's operations, and often regards attacks against supply chain operations or communications. The optimization literature regards interdiction problems as leader–follower games in which the leader takes interdiction actions to maximize the minimum objective that a follower can obtain in solving its optimization problem. The leader's interdiction actions can impact the follower's objective, feasible region, or both. (Interdiction also refers to a leader's minimization of a follower's maximization problem, such as in the interdiction of maximum flow problems.) Because of the origins of interdiction study, most such problems in the literature focus on *network* interdiction.

Numerous variations on interdiction problems have appeared in the literature in the past few decades, due both to the rapid growth in employing these models in practical settings and to the number of theoretical and algorithmic innovations in solving them. The purpose of this paper is to give an introduction to interdiction problems along with a brief history of their development, before exploring the next generation of interdiction problems and their solution approaches.

We begin this paper by describing fundamental assumptions pertaining to interdiction problems in Section 1.1; providing basic interdiction formulations and terminology for these problems in Section 1.2; comparing interdiction models to bilevel and robust optimization models in Section 1.3; and previewing the remainder of this paper in Section 1.4.

1.1. Basic interdiction setup

Many interdiction studies in the literature make a common set of key assumptions regarding the game being examined. Some of these are enumerated below.

A1. All problem data is known to both the leader and the follower.
A2. The leader is certain of the effect that its interdiction actions have on the follower's problem.
A3. The leader and follower play a zero-sum game in the sense that the value of the game is given by the follower's objective, with the leader seeking to maximize (or minimize) the minimum (or maximum) value that the follower can achieve via constrained optimization.
A4. In each round of the interdiction game, the leader and follower each make one set of decisions, with the leader making all of its decisions before the follower makes its set of decisions. (This setup is often referred to as a "defender–attacker" or "attacker–defender" game, depending on the context of the game.)
A5. Only one round of the game is played.

These problems belong to the more general class of *Stackelberg games* (von Stackelberg, 1952), which involve a single leader and one or more followers, not necessarily playing a zero-sum game. As in assumption A4, in a Stackelberg game the leader makes its move first, and then the follower(s) make their decisions in response to the leader's decisions.

* Corresponding author.
E-mail addresses: jcsmith@clemson.edu (J.C. Smith), yongjis@clemson.edu (Y. Song).

https://doi.org/10.1016/j.ejor.2019.06.024
0377-2217/© 2019 Elsevier B.V. All rights reserved.

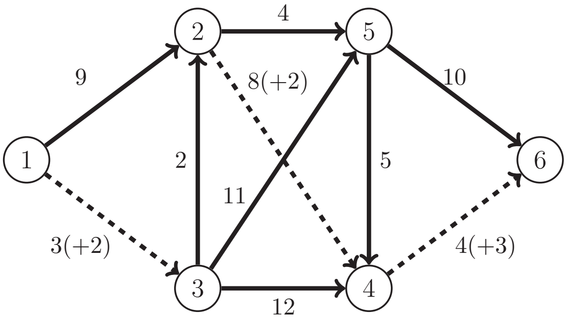

Fig. 1. An illustration of the shortest path interdiction problem.

Example 1. For instance, one well-studied class of such problems is the shortest path interdiction problem (Israeli & Wood, 2002). Here, a leader attacks arcs with the goal of maximizing the shortest path cost (distance) that the follower can obtain. An arc that is attacked has its cost increased from some nominal value. (The leader is constrained by the number of arcs it can attack, or else there exists a trivial optimal solution in which all arcs are interdicted.) By assumption A1, the leader knows the follower's origin and destination nodes, along with the nominal arc costs and the increased values of those arc costs if attacked. Assumption A2 guarantees that the leader's attacks will lengthen the targeted arcs as anticipated. Assumption A3 assures that both players agree on the objective and that they play a max-min game. Assumption A4 states that the leader must commit all of its attacks before the follower chooses a path, and that the follower's path choice is the only decision that the follower makes. Assumption A5 states that this game is played only once. Fig. 1 illustrates a feasible interdiction solution (the set of dashed arcs) to an instance of the shortest path interdiction problem, where the follower takes the shortest path from node 1 to node 6, and the leader's budget allows it to interdict up to three arcs. The values in parentheses correspond to interdiction effects. Prior to the interdiction, the shortest path taken by the follower is $1 \to 3 \to 2 \to 4 \to 6$, with a value of 17; after the interdiction, the shortest path becomes $1 \to 3 \to 2 \to 5 \to 6$, with a value of 21. □

Besides the shortest path interdiction problem described above, there are many other variants of basic interdiction problems where assumptions A1–A5 are satisfied, including:

(i) The binary knapsack interdiction problem (Caprara, Carvalho, Lodi, & Woeginger, 2016; Fischetti, Ljubic, Monaci, & Sinnl, 2019), where the leader and the follower each pick items according to their own knapsack constraints, but instead of maximizing its own profit, the leader minimizes the follower's maximum profit by blocking items that the follower can choose;

(ii) The clique interdiction problem (Mahdavi Pajouh, Boginski, & Pasiliao, 2014), where the leader selects a set of edges up to a given cardinality limit to remove from an undirected graph so that the size of a maximum clique in the remaining graph is minimized;

(iii) The matching interdiction problem (Zenklusen, 2010), where the leader removes a limited subset of vertices or edges in an undirected network under a given budget, such that the weight of a maximum matching in the remaining graph is minimized;

(iv) The project interdiction problem (Brown, Carlyle, Harney, Skroch, & Wood, 2009), where the interdictor attempts to maximally delay the completion time of a project by allocating resources to disrupt its process.

In addition, as we discuss later in Section 4, there also exist several recent variations of interdiction problems in which assumptions A1–A5 do not all hold.

1.2. Interdiction formulations

We adopt the convention that the leader's variables are denoted by variables $\mathbf{x} \in \mathbb{R}^{n_L}$ (where $\mathbb{R}^{n_L}$ is the set of n_L-dimensional real vectors) and the follower's variables by $\mathbf{y} \in \mathbb{R}^{n_F}$, where n_L and n_F are both positive integers. Letting the function $\Theta(\mathbf{x})$ represent the value of interdiction decision $\mathbf{x}$, a general form of the interdiction problem is given by:

$$\max \quad \Theta(\mathbf{x}) \tag{1a}$$

$$\text{s.t.} \quad \mathbf{x} \in X, \tag{1b}$$

where X is a non-empty (and usually bounded) set in $\mathbb{R}^{n_L}$. The value of interdiction decision $\mathbf{x}$, $\Theta(\mathbf{x})$, is defined as:

$$\Theta(\mathbf{x}) = \min \quad f(\mathbf{x}, \mathbf{y}) \tag{2a}$$

$$\text{s.t.} \quad \mathbf{y} \in Y(\mathbf{x}), \tag{2b}$$

where $f(\mathbf{x}, \mathbf{y})$ represents the follower's objective function (affected by the leader's action $\mathbf{x}$). We define $Y(\mathbf{x}) \subseteq \mathbb{R}^{n_F}$ as the set of feasible actions for the follower given any leader's action $\mathbf{x} \in X$. Condensed, this model becomes simply

$$z^* = \max_{\mathbf{x} \in X} \left\{ \min_{\mathbf{y} \in Y(\mathbf{x})} \{ f(\mathbf{x}, \mathbf{y}) \} \right\}. \tag{3}$$

To illustrate this general form, consider the shortest path interdiction model in Example 1. Define $G = (V, A)$ to be the network over which the problem is solved, with node set V and arc set A. Let T be the node-arc incidence matrix having a row corresponding to every node and a column corresponding to every arc. The column corresponding to arc $(i, j) \in A$ has a 1 in row i, a -1 in row j, and zeros elsewhere in the column. Let $\mathbf{b} \in \mathbb{Z}^{|V|}$ be the vector of all zeros except for a 1 in the row corresponding to the origin and a -1 in the row corresponding to the destination, where $\mathbb{Z}^{|V|}$ is the set of all $|V|$-dimensional integer vectors. It is well-known that there exists an optimal integer solution, which corresponds to an origin-destination path, to any linear program constrained (only) by $T\mathbf{y} = \mathbf{b}$ and $\mathbf{y} \geq \mathbf{0}$, if the objective coefficients on the y-variables are nonnegative (or, more generally, if no negative-cost cycle exists). Let $c_{ij} \in \mathbb{R}_+$ be the nominal cost of using arc $(i, j) \in A$, and $d_{ij} \in \mathbb{R}_+$ be the amount by which arc (i, j) is lengthened if it is interdicted, where $\mathbb{R}_+$ denotes the set of nonnegative real numbers. That is, the cost of using arc (i, j) is $c_{ij} + d_{ij}x_{ij}$, where $x_{ij} = 1$ if arc (i, j) is interdicted, and $x_{ij} = 0$ otherwise. We express:

$$\Theta(\mathbf{x}) = \min \quad \sum_{(i,j) \in A} \left(c_{ij} + d_{ij} x_{ij} \right) y_{ij} \tag{4a}$$

$$\text{s.t.} \quad T\mathbf{y} = \mathbf{b} \tag{4b}$$

$$\mathbf{y} \geq \mathbf{0}. \tag{4c}$$

Note in this example that (4) is a simple shortest path problem when $\mathbf{x}$ is fixed, and that $Y(\mathbf{x})$ does not actually depend on $\mathbf{x}$. To finish this model, we need only to represent the set X. Typically, interdiction decisions are "all-or-nothing" (binary) decisions, and can be constrained by a single cardinality constraint, by a knapsack constraint, or via a more general set of constraints. If, for instance, the leader were restricted to interdict no more than γ arcs, where $\gamma \in \mathbb{Z}_+$, then

$$X = \left\{ \mathbf{x} \in \{0, 1\}^{|A|} : \sum_{(i,j) \in A} x_{ij} \leq \gamma \right\}. \tag{5}$$

Network interdiction problems (1) with $\Theta(\mathbf{x})$ defined in (4) are NP-hard in general. Ball, Golden, and Vohra (1989) have shown that even for the special case when X is defined as (5), and d_{ij} is arbitrarily large for all $(i, j) \in A$ (effectively removing arc (i, j) from the network), the problem remains NP-hard. (This problem is known as the k-most-vital-arcs problem.)

Remark 1. The interdiction problem given in (1) maximizes the interdiction effect subject to an interdiction cost budget. From a strategic planning perspective, where one pursues the best tradeoff between maximizing the interdiction effect and minimizing interdiction cost by finding the Pareto-optimal solutions associated with the two objectives, a multi-objective network interdiction model can be formulated and solved (Rocco & Ramirez-Marquez, 2010; Rocco, Ramirez-Marquez, & Salazar, 2010; Royset & Wood, 2007).

1.3. Relationship to bilevel and robust optimization

Two areas closely related to interdiction models are bilevel optimization and robust optimization. For completeness, we discuss those modeling strategies here in order to contrast them with interdiction studies.

1.3.1. Bilevel optimization models

Bilevel optimization models regard a leader and a follower playing a two-stage game just as in the interdiction model. However, these models are more general than interdiction models in the following ways: (i) the leader's objective does not necessarily maximize the minimum objective obtainable by the follower, and (ii) the follower's actions may now affect the leader's objective and feasible region. Hence, we denote the leader's objective function as f^L and the follower's objective function as f^F. Because the leader's feasible region now depends on the follower's decisions, it is denoted as $X(\mathbf{y})$. The interdiction model given by (1) and (2) becomes:

$$\max \quad f^L(\mathbf{x}, \mathbf{y}) \tag{6a}$$

$$\text{s.t.} \quad \mathbf{x} \in X(\mathbf{y}) \tag{6b}$$

$$\mathbf{y} \text{ is an optimal solution to the follower's problem,} \tag{6c}$$

where the follower's problem is given as follows, with $\mathbf{x}$ being a fixed vector:

$$\min \quad f^F(\mathbf{x}, \mathbf{y}) \tag{7a}$$

$$\text{s.t.} \quad \mathbf{y} \in Y(\mathbf{x}). \tag{7b}$$

Note that the choices of maximization and minimization for the leader and follower, respectively, are arbitrary. The leader chooses $\mathbf{x}$ knowing that the follower will choose a $\mathbf{y}$ that optimizes problem (7). The leader anticipates the follower's behavior in (6c), seeking to maximize the objective function (6a) and remain feasible to (6b) based on knowledge of the follower's behavior. Note that because (6c) requires the existence of a solution $\mathbf{y}$ that optimizes the follower's problem, the leader is forced to choose an $\mathbf{x}$ such that (7) has such an optimal solution.

For the special case in which f^L and f^F are the same function, and in which $X(\mathbf{y})$ does not change based on $\mathbf{y}$, we recover exactly the interdiction model (2). However, the more general bilevel optimization model can capture the situation in which agents simply optimize based on their own self-interests. Dempe, Kalashnikov, Pérez-Valdés, and Kalashnykova (2015) provide a comprehensive survey on bilevel optimization. See DeNegre and Ralphs (2009), Lozano and Smith (2017), Mitsos (2010), Saharidis and Ierapetritou (2009), and Xu and Wang (2014) for a sampling of contemporary algorithmic approaches in this area. Bilevel optimization models facilitate one of the recent advances in network interdiction that incorporates information asymmetry, as we will describe in Section 4.4.

1.3.2. Robust optimization models

In a robust (maximization) optimization model, the leader makes decisions under uncertain information. This uncertainty can affect the leader's objective and feasible region. The standard assumption in robust optimization is that uncertainty outcomes occur in a way that minimizes the leader's objective. Furthermore, when uncertainty affects the feasible region, uncertainty reveals itself in a way that will make the leader's decisions infeasible if possible. For brevity in this discussion, however, we assume that uncertainty is confined to the leader's objective. Also, we assume that the objective function is linear. The problem can be written in the form

$$\max \quad \mathbf{c}^\top \mathbf{x} \tag{8a}$$

$$\text{s.t.} \quad \mathbf{x} \in X. \tag{8b}$$

Here, we assume that $\mathbf{c} \in \mathbb{R}^n$ is unknown and that X is known. (See, e.g., Ben-Tal, El Ghaoui, & Nemirovski, 2009 for a more general analysis of robust equivalent formulations in which constraints that describe the set X have uncertain data.) Although $\mathbf{c}$ is not known precisely, the robust optimization model assumes that it belongs to an *uncertainty set*, $\mathcal{C} \subseteq \mathbb{R}^n$. Furthermore, given any decision $\hat{\mathbf{x}}$ selected by the leader, we assume in robust optimization that $\mathbf{c}$ takes on the value of a vector in $\mathcal{C}$ that *minimizes* $\mathbf{c}^\top \hat{\mathbf{x}}$.

In practice, $\mathcal{C}$ often represents a polyhedral set of potential vectors for $\mathbf{c}$. For instance, let $\bar{\mathbf{c}}$ be a nominal objective vector, perhaps representing the anticipated objective coefficients. The budgeted uncertainty set of Bertsimas and Sim (2004) assumes that $\mathbf{c}$ belongs to a hyperrectangle (simple lower and upper bounds on each element of the vector), along with a side constraint that restricts $\mathbf{c}$ to be sufficiently close to $\bar{\mathbf{c}}$. The distance between $\mathbf{c}$ and $\bar{\mathbf{c}}$ is defined by a weighted 1-norm, e.g., $\sum_{i=1}^n w_i |c_i - \bar{c}_i|$ for some $\mathbf{w} \in \mathbb{R}^n_+$, which can typically be represented as a single additional constraint. More generally, we can define

$$\mathbf{c} = \bar{\mathbf{c}} - \mathbf{y}, \tag{9}$$

where $\mathbf{y}$ represents the possible deviation from $\bar{\mathbf{c}}$, and is constrained to belong to some set $Y := \{\mathbf{y} \in \mathbb{R}^n \mid \sum_{i=1}^n w_i |y_i| \leq \Gamma\}$ for some $\Gamma > 0$. The robust optimization model becomes:

$$\max_{\mathbf{x} \in X} \left\{ \min_{\mathbf{y} \in Y} \left\{ (\bar{\mathbf{c}} - \mathbf{y})^\top \mathbf{x} \right\} \right\}. \tag{10}$$

Note that this model takes the form of (3), except that a linear objective is assumed in (10), and the set of possible objective coefficient deviations given by Y is not a function of the leader's variables.

Although the basic interdiction setting considered has a similar form to robust optimization problems with uncertain objective coefficients, they model different situations in practice. In network interdiction problems, the agent that solves the network optimization problem is the follower, with the leader acting first to inhibit components of that network (such as lengthening the arc costs in Example 1). In robust optimization problems, the network operator acts first as the leader, and the follower simply degrades system components based on the leader's action to worsen the leader's objective. Thus, in a robust shortest path problem, the leader commits to a path first and then the follower lengthens a worst-case set of arcs with knowledge of the leader's path choice.

We refer the reader to the book of Ben-Tal et al. (2009), tutorial chapters by Bertsimas and Thiele (2006) and Delage and Iancu (2015), and an introductory article on basic robust optimization principles in Smith and Ahmed (2011). The relationship between interdiction problems and robust optimization problems has been utilized in the dynamic network interdiction setting, one of the recent advances in network interdiction that we will describe in Section 4.3.

1.4. Paper overview

The remainder of this paper is organized as follows. Section 2 presents a brief history of network interdiction studies, providing context for discussing recent studies in the interdiction field. Section 3 examines major categories of algorithms that are used to solve network interdiction problems. Section 4 explores several types of contemporary and emerging studies on network interdiction problems, showing how they differ from the assumptions stated earlier in this section. Section 5 then discusses interdiction models for modern and future applications.

2. Origins of network interdiction models and algorithms

Although the focus of this paper is on recent and emerging interdiction applications and algorithms, we first cover some of the classic network interdiction literature in this section.

One early example of a study on network flow problems having strong implications for the interdiction field stems from the max-flow min-cut theorem established in the 1950s (Elias, Feinstein, & Shannon, 1956; Ford & Fulkerson, 1956). This theorem considers a network $G(V, A)$ with a source node s and destination node t, where each arc $(i, j) \in A$ has a (positive, integer) capacity u_{ij}. The maximum flow value over G is the largest amount of flow that can be sent from node s through the network such that flow is conserved at all nodes $i \in V\backslash\{s, t\}$, all flow emanating from s terminates at t, and the amount of flow on each arc $(i, j) \in A$ is not negative and not more than u_{ij}. A cut in G is a set of arcs A' such that there exists no directed path from s to t in $G(V, A\backslash A')$; the capacity of that cut is given by $\sum_{(i,j)\in A'} u_{ij}$. A minimum cut is a cut having the smallest capacity. With this notation thus defined, the max-flow min-cut theorem states that the maximum flow value in G equals the capacity of a minimum cut in G. One particularly elegant proof of this theorem (Dantzig & Fulkerson, 1955) shows that the dual problem of the maximum flow linear programming formulation is exactly the minimum cut formulation. Indeed, as we will see later in this article, duality is one of the most important tools used within interdiction studies.

The implication of this theorem is that if the interdiction goal is to disconnect two terminals of a network by removing arcs, and the effort required to remove a set of arcs is equal to the sum of their arc capacities, then the interdiction problem can be cast as a min-cut problem (and thus solved as a max-flow problem). Harris and Ross (1955) exploit this equivalence and apply it in the interdiction context for disconnecting rail networks.

The more general *maximum flow interdiction problem* regards an interdictor who seeks to minimize the maximum flow that can occur across the network, by removing a set of arcs from the network according to some budget constraints. Wollmer (1964) examines the case in which G is planar, and an interdictor can remove up to a limited number ℓ of arcs from the network. These two assumptions (planarity and a cardinality-constrained interdiction budget) are essential to devising a polynomial-time algorithm for the problem.

Wollmer's approach utilizes a *topological dual* graph. For simplicity in defining this dual, we assume that the maximum flow problem takes place on a bidirected network, in which $(i, j) \in A$ if and only if $(j, i) \in A$ as well, where $u_{ij} = u_{ji}$. The results hold for directed networks as well with modifications; see Lawler (1976) for a discussion of topological duals. After embedding G in the plane, define a *face* of G as a maximal subset of the plane that contains no edges in its interior. We first add an artificial edge from the origin to the destination in G, and then initialize the topological dual by placing one dual node in every face of G. An (undirected) edge connects two nodes in the dual graph if the nodes' corresponding faces are separated by a single edge in the primal graph, not counting the artificial edge. One dual node located on the exterior of the primal graph is the origin, and one dual node belonging to the face bounded by the artificial edge is the destination. Fig. 2 illustrates a primal graph with (lettered and shaded) dual nodes assigned to each face. The corresponding topological dual network is shown on the right side of this figure.

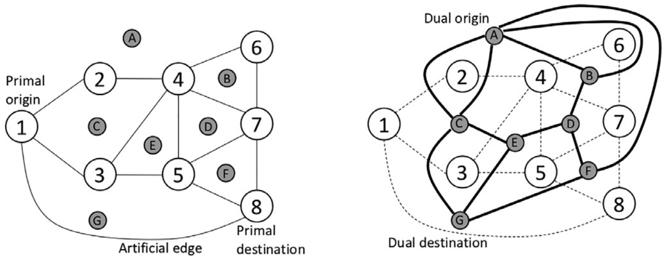

Fig. 2. An illustration of a topological dual graph.

For each dual edge e, define (i_e, j_e) as the primal edge intersected by e. The traversal of dual edge e corresponds to placing primal edge (i_e, j_e) in the minimum cut for the primal. Therefore, every dual origin-destination path corresponds to a primal cut set. For instance, the dual path A–C–E–G in Fig. 2 corresponds to cut set $\{(2, 4), (3, 4), (3, 5)\}$. The capacity of each edge placed in the cut depends on whether or not it has been interdicted: primal edge (i, j) has capacity 0 if interdicted, and u_{ij} if not. Thus, Wollmer's approach solves the minimum cut problem by solving a shortest path problem in the dual network, where the cost of using edge e depends on whether or not (i_e, j_e) is interdicted.

Wollmer's method creates an expanded dual network $G^E(V^E, A^E)$ comprised of $\ell + 1$ copies of the dual network, where ℓ is the number of edges that the leader can interdict. For each node i in the dual network, we place corresponding nodes $i^0, \ldots, i^\ell$ in V^E. A path on the dual graph reaching i^k, the kth copy of dual node i, indicates that k edges in that path correspond to interdicted edges. For each dual edge e we place edges (i_e^k, j_e^k) in A^E for all $k = 0, \ldots, \ell$ and (i_e^k, j_e^{k+1}) in A^E for all $k = 0, \ldots, \ell - 1$. Edge (i_e^k, j_e^k) corresponds to an uninterdicted primal edge, and so its cost is given by $c_{i_e^k j_e^k} = u_e$. Edge (i_e^k, j_e^{k+1}) corresponds to an interdicted primal edge, and so its cost is given by $c_{i_e^k j_e^{k+1}} = 0$. The cost of the shortest path in G^E from copy zero of the source node to copy k of the destination node corresponds to the minimum cut value in the primal graph if the leader interdicts exactly k edges; thus, taking the minimum of these values over all k at the destination node in G^E corresponds to the optimal objective value of this problem.

Note that planarity allows the existence of the topological dual, and the polynomiality of this procedure depends on the fact that only $\ell + 1$ copies of the dual network are required in G^E (recalling that $\ell \le |A|$). If a more general knapsack budget were used on a planar graph, i.e., interdicting primal arc (i, j) costs some positive integer $r_{i'j'}$, and the total budget for interdiction is given by b, then an adaptation of this procedure would become pseudopolynomial, because we would require $b + 1$ copies of the planar dual network in G^E. In fact, McMasters and Mustin (1970) examine exactly this case for the problem of inhibiting the capability of a combatant force's resupply operations. Their algorithm relies on the generation of minimal cuts and runs in exponential time. Phillips (1993) proves that the maximum flow interdiction problem is NP-hard (though of course not in the strong sense) under a knapsack budget constraint. If G were not planar, then the topological dual graph could not be constructed at all. For this general case, Ghare, Montgomery, and Turner (1971) and Ratliff, Sicilia, and Lubore (1975) develop combinatorial (and worst-case exponential) schemes for the problem. Wood (1993) proves that the (cardinality-constrained) interdiction problem is indeed strongly NP-hard for non-planar networks. Altner, Ergun, and Uhan (2010) provide improved bounds on the approximability of this class of interdiction problems.

Fulkerson and Harding (1977) consider a shortest path interdiction model in which each arc can be lengthened by any continuous amount. The effort required to lengthen an arc is given by a linear function of the amount by which the arc is lengthened, and the leader is assumed to have a budget that constrains total interdiction effort. The problem can be solved using parametric linear programming analysis, and Fulkerson and Harding (1977) show the equivalence of this problem to solving a minimum cost network flow problem, which is polynomial-time solvable. An alternative characterization of this problem, which can also be solved by minimum cost network flows, appears in Golden (1978). This problem seeks to minimize the total interdiction effort required to increase the follower's shortest path to a certain threshold value. However, when the interdiction decisions are binary, Ball et al. (1989) show that the shortest path interdiction problem is NP-hard.

These studies led to the seminal work of Wood (1993), who provides a general mathematical programming modeling technique for network interdiction problems. The contributions are general enough to handle situations in which interdiction actions can be discrete or continuous, and in which there may exist multiple interdiction resources and flow commodities. Wood (1993) also accounts for networks having directed or undirected edges, and for those having multiple sources and destinations.

Early applications of network interdiction problems focused on defense strategies, as described above. Currently, interdiction is applied in many different settings to model situations in which one wishes to identify vulnerabilities to accidental or intentional disruptions to infrastructure. In many other studies, the interdictor is taken to be the protagonist in the problem scenario, such as in the study of Washburn and Wood (1995) where the interdictor seeks to detect evaders (see also Morton, Pan, & Saeger, 2007; Sullivan, Morton, Pan, & Smith, 2014a for studies in which the interdictor's aim is to thwart nuclear smuggling efforts). As another example, hospital infection containment is considered by Assimakopoulos (1987), where interdiction actions seek to limit the spread of infection.

3. Common algorithmic approaches for network interdiction

In this section, we survey various algorithms in the network interdiction literature that rely on different assumptions made on the interdiction problems, using the basic interdiction setup presented in Section 1.1. In Section 3.1 we examine the case in which the follower's problem (2) can be modeled as a convex optimization problem, and then describe the more complicated case when the follower's problem is nonconvex in Section 3.2.

3.1. Network interdiction with convex follower's problem

We start by reviewing solution approaches for network interdiction problems where the follower's problem can be formulated as a convex optimization problem. The convexity assumption enables duality-based approaches such as dualize-and-combine and Benders decomposition, as we examine here.

3.1.1. Dualize-and-combine

For simplicity, we consider the shortest path interdiction problem where the inner problem is a shortest path problem (4) given any fixed interdiction decision **x**. The simple idea of the "dualize-and-combine" approach is to first take the dual formulation of the follower's problem given a fixed **x**, so that both players' problems share the same direction of optimization, and then release **x** as a decision vector, making it a single-level optimization problem. Specifically, let vector $\boldsymbol{\pi}$ be the dual vector associated with constraints (4b). The dual formulation for (4) can be written as:

$$\Theta(\mathbf{x}) = \max \quad \mathbf{b}^\top \boldsymbol{\pi} \tag{11a}$$

$$\text{s.t.} \quad T^\top \boldsymbol{\pi} \le \mathbf{c} + D\mathbf{x}, \tag{11b}$$

where $D = \text{diag}\big(\{d_{ij} : (i,j) \in A\}\big)$. Combining (11) with the leader's problem (1) gives the following single-level problem:

$$\max \quad \left\{ \mathbf{b}^\top \boldsymbol{\pi} \mid T^\top \boldsymbol{\pi} \le \mathbf{c} + D\mathbf{x}, \ \mathbf{x} \in X \right\}, \tag{12}$$

which can be readily solved via a standard optimization solver. We remark that problem (12) belongs to a general class of optimization problems called "reverse optimization problems" (see, e.g., Nguyen, 2016). For a given optimization problem, the corresponding reverse problem is to modify some parameters under a budget constraint so that the optimal value is improved as much as possible.

When interdiction affects the feasible region of the follower's optimization problem (according to $Y(\mathbf{x})$) instead of the objective function, one could still apply the "dualize-and-combine" approach, but with a little more effort. This situation typically arises in network flow interdiction problems in which interdiction decisions reduce or eliminate arc capacities. For example, consider the formulation:

$$\Theta(\mathbf{x}) = \min \quad \mathbf{c}^\top \mathbf{y} \tag{13a}$$

$$\text{s.t.} \quad T\mathbf{y} = \mathbf{b} \qquad (\pi) \tag{13b}$$

$$y_{ij} \le u_{ij}(1 - x_{ij}), \ \forall (i,j) \in A \qquad (-\beta_{ij}) \tag{13c}$$

$$y_{ij} \ge 0, \ \forall (i,j) \in A, \tag{13d}$$

where parameters u_{ij} are simple upper bounds on y_{ij} (e.g., all $u_{ij} = 1$ for the shortest path interdiction problem). Hence, (13c) enforce the condition that $y_{ij} \le u_{ij}$ unless arc (i, j) is interdicted, in which case y_{ij} is forced to equal zero.

Following the "dualize-and-combine" approach directly, we associate constraints (13b) with dual vector $\boldsymbol{\pi}$ and each constraint in (13c) with a dual variable $-\beta_{ij}$. The resulting single-level optimization problem becomes:

$$\max \quad \mathbf{b}^\top \boldsymbol{\pi} - \sum_{(i,j)\in A} u_{ij}\beta_{ij}(1 - x_{ij}) \tag{14a}$$

$$\text{s.t.} \quad T^\top \boldsymbol{\pi} - \mathbf{I}_{|A|}\beta \le \mathbf{c} \tag{14b}$$

$$\beta_{ij} \ge 0, \ \forall (i,j) \in A \tag{14c}$$

$$\mathbf{x} \in X, \tag{14d}$$

where $\mathbf{I}_{|A|}$ is the $|A| \times |A|$ identity matrix. Although a complicating bilinear term $\beta_{ij}(1 - x_{ij})$ shows up in the objective function (14a), when the interdiction decision x_{ij} is restricted to be a binary variable (which is typically true for network interdiction problems), we could linearize the bilinear term using standard McCormick inequalities given upper bounds M_{ij} on β_{ij}. This linearization strategy would (i) add a new variable w_{ij} to replace $\beta_{ij}(1 - x_{ij})$ in (14a), and (ii) add the following inequalities to (14):

$$w_{ij} \ge \beta_{ij} - M_{ij}x_{ij}, \ \text{and} \ w_{ij} \ge 0, \ \forall (i,j) \in A.$$

The typical linearization inequalities $w_{ij} \le \beta_{ij}$ and $w_{ij} \le M_{ij}(1 - x_{ij})$ are not necessary here because w_{ij} will take the smallest value possible at optimality, and these upper bounds on w_{ij} can thus be omitted from the formulation.

An alternative reformulation of (13) is to penalize the use of an interdicted arc rather than by prohibiting the use of an interdicted arc within the constraint set. The validity of this reformulation again relies on the binary restriction on decision variables x_{ij}. For all $(i, j) \in A$, given an upper bound M_{ij} on the optimal dual multiplier β_{ij} associated with (13c) for all feasible $x \in X$, formulation (13) can be reformulated as:

$$\Theta(\mathbf{x}) = \min \quad \mathbf{c}^\top \mathbf{y} + \mathbf{x}^\top \mathbf{M}\mathbf{y} \tag{15a}$$

$$\text{s.t.} \qquad T\mathbf{y} = \mathbf{b} \tag{15b}$$

$$0 \le y_{ij} \le u_{ij}, \quad \forall (i, j) \in A, \tag{15c}$$

where $\mathbf{M} = \mathrm{diag}\big(\{M_{ij} : (i, j) \in A\}\big)$. One can then apply "dualize-and-combine" for formulation (15).

We now show that this reformulation is valid, i.e., formulation (15) is equivalent to formulation (13). Given a fixed $\mathbf{x}^* \in \{0, 1\}^{|A|}$, let $z_1(\mathbf{x}^*)$ and $z_2(\mathbf{x}^*)$ be the optimal objective value of (13) and (15), respectively. We show that $z_1(\mathbf{x}^*) = z_2(\mathbf{x}^*)$. First, let $\mathbf{y}^*$ be an optimal solution to (13) with $\mathbf{x} = \mathbf{x}^*$. Observe that Eq. (13c) implies that $\mathbf{x}^{*\top}\mathbf{M}\mathbf{y}^* = 0$, so $\mathbf{y}^*$ is feasible to (15) with an objective value of $z_1(\mathbf{x}^*) = \mathbf{c}^\top \mathbf{y}^*$, thus $z_1(\mathbf{x}^*) \ge z_2(\mathbf{x}^*)$. On the other hand, let $\bar{\mathbf{y}}^*$ be an optimal solution to (15) with $\mathbf{x} = \mathbf{x}^*$. We claim that $\bar{y}^*_{ij} = 0$ whenever $x^*_{ij} = 1$. This is because the dual price for constraint (13c), which can be interpreted as the profit of having one extra unit of resource y_{ij}, is upper bounded by the cost M_{ij}. Therefore, $z_2(\mathbf{x}^*) = \mathbf{c}^\top \bar{\mathbf{y}}^*$, and $\bar{\mathbf{y}}^*$ is feasible to (13) with $\mathbf{x} = \mathbf{x}^*$, implying that $z_2(\mathbf{x}^*) \ge z_1(\mathbf{x}^*)$. This idea was first proposed by Morton and Wood (1999), and has been a popular reformulation tool for solving maximum flow interdiction problems (Cormican, Morton, & Wood, 1998).

In both of the above approaches, the upper bound M_{ij} for β_{ij} variables is crucial. In practice, it is important to find a relatively tight bound M_{ij} on β_{ij}, in order to obtain a strong linear programming relaxation bound. These bounds can be obtained by gleaning insights from the follower's problem structure. For example, Cormican et al. (1998) provide such upper bounds for maximum flow interdiction problems, and Lim and Smith (2007) derive dual upper bounds for multi-commodity network flow interdiction problems.

Continuous interdiction. When the interdiction decisions $\mathbf{x}$ are modeled as continuous variables, neither the standard linearization approach nor the penalty-based approach described above can be applied when the interdiction affects the feasible region of the follower's problem. (When interdiction only affects the follower's objective, the duality-based reformulation (12) is still valid.) Recognizing that variables involved in the bilinear terms are disjointly constrained, specialized finitely convergent algorithms proposed in, e.g., Sherali and Shetty (1980) or Alarie, Audet, Jaumard, and Savard (2001) can be applied, although these algorithms may suffer from computational and implementation challenges. When the leader's feasible set X is a polyhedron characterized as a single-row budget constraint, Lim and Smith (2007) take advantage of the extreme point solution structure of this polyhedron, noting that all but one of the variables are nonbasic. They propose a partitioning algorithm by designating one variable at a time as the basic variable, while all others are fixed at either of their bounds, i.e., 0 or 1, which can therefore be modeled as binary variables. Standard linearization approaches such as McCormick inequalities can then be applied to reformulate the problem as a mixed integer linear program.

Ad-hoc formulation example. In the "dualize-and-combine" approach, optimality of the follower's decision is enforced by the dual formulation via strong duality. Depending on the problem structure, an alternative characterization of the follower's optimal decisions can be utilized to construct ad-hoc formulations. A classic example of these ad-hoc formulations is the one proposed for the uncapacitated facility interdiction problems by Church, Scaparra, and Middleton (2004). This problem examines a set of facilities F that is under attack from an interdictor that can essentially eliminate some $r \in \mathbb{Z}_+$ facilities $(0 < r < |F|)$. There exists a set N of demand points, and the follower assigns each point to the closest facility that is not attacked, so that the total routing cost is minimized. Letting d_{ij} denote the distance from demand point i to facility j, the facility interdiction problem can be formulated as the following max-min problem:

$$\max_{\mathbf{x}\in X} \; \min \sum_{i\in N}\sum_{j\in F} d_{ij}y_{ij} \tag{16a}$$

$$\text{s.t.} \sum_{j\in F} y_{ij} = 1, \qquad \forall i \in N \tag{16b}$$

$$y_{ij} \le 1 - x_j, \qquad \forall i \in N, j \in F \tag{16c}$$

$$y_{ij} \in \{0, 1\}, \qquad \forall i \in N, j \in F, \tag{16d}$$

where $X = \{\mathbf{x} \in \{0, 1\}^{|F|} \mid \sum_{j\in F} x_j \le r\}$. The constraint matrix of the inner problem for (16) is totally unimodular, implying that the integrality restrictions on y_{ij} variables can be relaxed without changing the optimal objective value of the inner problem. Thus the follower's problem can be treated as a linear program. Instead of dualizing this inner problem, Church et al. (2004) control both the leader's decision $\mathbf{x}$ and the follower's decision $\mathbf{y}$ in a single-level formulation, and explicitly enforce optimality conditions for the follower's decision $\mathbf{y}$ as follows. Given any $\hat{\mathbf{x}} \in X$, there exists an optimal $\mathbf{y}^*$ so that for each demand point $i \in N$, there is only one index j^*_i that $y^*_{ij^*_i} = 1$ and $y^*_{ij} = 0$ for all $j \neq j^*_i$. This index j^*_i is one belonging to the set:

$$\arg\min\nolimits_{j\in F(\hat{\mathbf{x}})}\{d_{ij}\},$$

where $F(\hat{\mathbf{x}}) := \{k \in F : \hat{x}_k = 0\}$. Define $T_{ij} := \{k \in F | d_{ik} > d_{ij}\}$ as the set of facilities that are farther from point i than facility j. Together with (16b), logical constraints $x_j = 0 \Rightarrow y_{ik} = 0$ for all $k \in T_{ij}$ ensures that $\mathbf{y}$ is optimal to the follower's optimization problem. Using linear constraints (17d) below to model these logical constraints, the uncapacitated facility interdiction problem can be reformulated by the following single-level integer programming problem:

$$\max \sum_{i\in N}\sum_{j\in F} d_{ij}y_{ij} \tag{17a}$$

$$\text{s.t.} \sum_{j\in F} x_j = r \tag{17b}$$

$$\sum_{j\in F} y_{ij} = 1, \qquad \forall i \in N \tag{17c}$$

$$\sum_{k\in T_{ij}} y_{ik} \le x_j, \qquad \forall i \in N, j \in F \tag{17d}$$

$$x_j \in \{0, 1\}, \qquad \forall j \in F \tag{17e}$$

$$y_{ij} \in \{0, 1\}, \qquad \forall i \in N, \; j \in F. \tag{17f}$$

3.1.2. Benders decomposition

Benders decomposition is an outer-approximation technique for the hypograph defined by $\{(\mathbf{x}, \theta) | \theta \le \Theta(\mathbf{x})\}$, which is a convex closed set when the value function $\Theta(\mathbf{x})$ is concave. Benders decomposition starts from a reformulation of the follower's problem defined in terms of all its extreme point solutions. Taking again the shortest path interdiction problem as an example, let Y denote the feasible region of the follower's problem (4), and let $\hat{Y}$ be the set of all extreme points of Y. Then the leader's problem (1) can be reformulated as:

$$\max \quad \theta \tag{18a}$$

$$\text{s.t.} \quad \theta \le \sum_{(i,j)\in A} \left(c_{ij} + d_{ij}x_{ij}\right)\hat{y}_{ij}, \quad \forall \hat{\mathbf{y}} \in \hat{Y} \tag{18b}$$

$$\mathbf{x} \in X. \tag{18c}$$

There are typically exponentially many extreme point solutions contained in the set $\hat{Y}$, preventing a direct use of formulation (18). In Benders decomposition, a master problem that enforces constraints of the form (18b) for only a subset of the extreme points $\bar{Y} \subseteq \hat{Y}$ is constructed. This master problem is therefore a relaxation of (18). Given a solution $\hat{\mathbf{x}}$ to the master problem, the following subproblem is solved, and the corresponding optimal solution $\hat{\mathbf{y}}$ is then added to the subset $\bar{Y}$:

$$\min \quad \left\{ \sum_{(i,j)\in A} (c_{ij} + d_{ij}\hat{x}_{ij})y_{ij} \mid \mathbf{y} \in Y \right\}. \tag{19}$$

The master problem (18) with $\bar{Y}$ and the subproblem (19) are iteratively solved in an alternating fashion until convergence. The convergence of Benders decomposition is guaranteed by the finiteness of $\hat{Y}$. Interpreted as a cutting plane approach, Benders decomposition can be potentially accelerated via various stabilization approaches such as the level bundle method (Lemaréchal, Nemirovski, & Nesterov, 1995), cut selection strategies (Magnanti & Wong, 1981; Smith, Lim, & Alptekinoglu, 2009), etc., and can be integrated within the branch-and-bound algorithm for solving (18) when X involves integer restrictions.

Enhancements of Benders decomposition via combinatorial structures. When the leader's feasible set X involves integrality restrictions, one could further strengthen the formulation by generating inequalities that cut off not only (fractional) relaxation solutions but also integer feasible solutions, so long as at least one optimal solution has either been recorded by the algorithm or is not made infeasible by the cut. These cuts are referred to as *super-valid inequalities* by Israeli and Wood (2002). Given an integer feasible solution $\hat{\mathbf{x}}$, a cut corresponding to $\hat{\mathbf{y}}$ is generated by solving subproblem (19), and the following super-valid inequality is added to the Benders master problem:

$$\sum_{a\in A(\hat{\mathbf{y}})} x_a \ge 1, \tag{20}$$

where $A(\hat{\mathbf{y}}) := \{a \in A \mid \hat{y}_a = 1\}$, i.e., the set of arcs corresponding to the shortest path chosen by the follower in response to the leader's decision $\hat{\mathbf{x}}$. The underlying idea behind (20) is that given an incumbent interdiction decision, $\hat{\mathbf{x}}$, at least one arc on the shortest path corresponding to $\hat{\mathbf{x}}$ must be interdicted in order to potentially increase the follower's shortest path value. Super-valid inequalities (20) can be further strengthened based on the best upper bound obtained so far. Substantial computational time reduction from utilizing super-valid inequalities in Benders decomposition was observed by Israeli and Wood (2002) for the shortest path interdiction problem.

Global Benders decomposition. Salmerón, Wood, and Baldick (2009) extend the scope of Benders decomposition to models where the value function $\Theta(\mathbf{x})$ of the interdiction decision $\mathbf{x}$ is not necessarily concave. For example, this is the case for network flow interdiction problems in which interdictions reduce or eliminate arc capacities, where the value function $\Theta(\mathbf{x})$ is a convex function of $\mathbf{x}$, because it can be written as the maximum of a set of affine functions. More complicated cases include the optimal power flow interdiction problem that motivates the idea of Salmerón et al. (2009), where $\Theta(\mathbf{x})$ is a multilinear nonconvex function. The key is to find a valid "penalty vector" $\nu(\hat{\mathbf{x}})$ so that the following *global Benders cut* is valid for all $x \in X$:

$$\theta \le \Theta(\hat{\mathbf{x}}) + \nu(\hat{\mathbf{x}})^\top(\mathbf{x} - \hat{\mathbf{x}}). \tag{21}$$

When the value function $\Theta(\mathbf{x})$ is concave, and standard Benders decomposition can be applied, vector $\nu(\hat{\mathbf{x}})$ corresponds to the gradient or subgradient of $\Theta(\mathbf{x})$, obtained by solving the follower's problem with a fixed $\hat{\mathbf{x}}$. However, when $\Theta(\mathbf{x})$ is not concave, in order to construct a valid inequality (21) with a valid coefficient vector $\nu(\hat{\mathbf{x}})$, one must exploit specific problem structures such as the binary property of the interdiction decisions.

Salmerón et al. (2009) apply the idea of global Benders decomposition for interdiction problems in electric power grid networks, where interdiction is interpreted as a way to perform a worst-case vulnerability analysis for a power grid. The primary goal of an imaginary interdictor is to maximize the minimum power generation cost and load shedding. In this case, the value of $\nu(\hat{\mathbf{x}})$ for each component i in the power grid can be chosen by finding the maximum possible load that can be recovered from "un-interdicting" component i, i.e., changing $\hat{x}_i = 1$ to $\hat{x}_i = 0$, and the maximum possible load shedding from interdicting component i, i.e., changing $\hat{x}_i = 0$ to $\hat{x}_i = 1$. Power generation capacity on each component i helps to identify these bounds.

3.2. Network interdiction with a nonconvex follower's problem

In this section, we relax the convexity assumption on the follower's problem, which is crucial for the "dualize-and-combine" approach introduced in Section 3.1 (and may also be needed for the Benders decomposition approach). Network interdiction problems involving a nonconvex follower's problem remain challenging to solve; however, much progress has recently been made on important special cases of these problems.

Defender–attacker–defender problems. One important class of problems in which the follower's problem is nonconvex is the defender–attacker–defender model (DAD), see, e.g., Brown, Carlyle, Salmerón, and Wood (2006). This model extends the classical leader–follower paradigm in network interdiction, which is also known as an attacker–defender (AD) model (if one considers the interdicting agent as the "attacker"). In DAD models the defender makes a preliminary set of "fortification" decisions *before* the attacker–defender game takes place, resulting in a three-stage game. The defender's fortification decisions typically serve to protect infrastructure against potential interdictions.

For instance, in the shortest path interdiction example formulated in (14), a DAD model may allow the defender to first select some $\delta \in \mathbb{Z}_+$ arcs to fortify, where a fortified arc cannot be interdicted. The DAD model can be formulated as the following two-stage min-max model:

$$\min_{\mathbf{w}\in W} \max \ \mathbf{b}^\top \boldsymbol{\pi} - \sum_{(i,j)\in A} u_{ij}\beta_{ij}(1 - x_{ij}) \tag{22a}$$

$$\text{s.t.} \quad T^\top \boldsymbol{\pi} - \mathbf{I}_{|A|}\beta \le \mathbf{c} \tag{22b}$$

$$\beta_{ij} \ge 0, \qquad \forall (i,j) \in A \tag{22c}$$

$$x_{ij} \le 1 - w_{ij}, \qquad \forall (i,j) \in A \tag{22d}$$

$$\mathbf{x} \in X, \tag{22e}$$

where $W = \{\mathbf{w} \in \{0,1\}^{|A|} \mid \sum_{(i,j)\in A} w_{ij} \le \delta\}$. Observe that (22d) prohibits the interdiction of fortified arcs.

Formulation (22) exhibits a property commonly found in DAD problems: The inner maximization problem is nonconvex, and there exists no obvious way to obtain a strong dual of the inner problem to combine with the outer problem. Smith, Lim, and Sudargho (2007) use a penalty-based reformulation similar to that used in (15a). In particular, there exists a penalty matrix $\mathbf{M} = \text{diag}(M_{ij})_{(i,j)\in A}$ for appropriately large M_{ij}-values such that (22) yields the same set of optimal solutions as does the following formulation:

$$\min_{\mathbf{w}\in W} \max \mathbf{b}^\top \boldsymbol{\pi} - \sum_{(i,j)\in A} u_{ij}\beta_{ij}(1-x_{ij}) + \mathbf{w}^\top \mathbf{M}\mathbf{x} \tag{23a}$$

$$\text{s.t. } T^\top \boldsymbol{\pi} - \mathbf{I}_{|A|}\beta \le \mathbf{c} \tag{23b}$$

$$\beta_{ij} \ge 0, \ \forall (i,j) \in A \tag{23c}$$

$$\mathbf{x} \in X. \tag{23d}$$

The penalty terms enforce the condition that $w_{ij}x_{ij} = 0$, instead of relying on explicit constraints to serve that role. As such, the feasible region of the inner problem in formulation (23) does not depend on $\mathbf{w}$, although the objective function still does. Given a fixed fortification $\hat{\mathbf{w}}$, problem (23) becomes a disjointly constrained mixed integer bilinear programming problem. Define Λ as the set of all vectors $(\boldsymbol{\pi}, \boldsymbol{\beta})$ that satisfy constraints (23b) and (23c), and let ext(Λ) be the extreme points of this polyhedron. Consider a fixed $\mathbf{w}$. For a given $\hat{\mathbf{x}}$, the problem is a linear program in the remaining variables $(\boldsymbol{\pi}, \boldsymbol{\beta})$. Similarly, for a fixed $(\hat{\pi}, \hat{\beta})$, the problem is a mixed integer program in variables $\mathbf{x}$. Therefore, an optimal solution $(\hat{\pi}, \hat{\beta}, \hat{\mathbf{x}})$ to the inner problem of (23) exists in which $(\hat{\pi}, \hat{\beta}) \in \text{ext}(\Lambda)$ and $\hat{\mathbf{x}} \in X$. Because the inner problem is a maximization problem, the optimal objective value to this problem, given an interdiction vector $\hat{\mathbf{w}}$, is given by:

$$\max_{\hat{\mathbf{x}}\in X,\ (\hat{\pi},\hat{\beta})\in\text{ext}(\Lambda)} \left\{ \mathbf{b}^\top \hat{\pi} - \sum_{(i,j)\in A} u_{ij}\hat{\beta}_{ij}(1-\hat{x}_{ij}) + \hat{\mathbf{w}}^\top \mathbf{M}\hat{\mathbf{x}} \right\}. \tag{24}$$

This formulation allows us to convert (22) into a single-level formulation as follows, albeit with an exponential number of constraints.

$$\min \theta \tag{25a}$$

$$\text{s.t. } \theta \ge \mathbf{b}^\top \hat{\pi} - \sum_{(i,j)\in A} u_{ij}\hat{\beta}_{ij}(1-\hat{x}_{ij}) + \mathbf{w}^\top \mathbf{M}\hat{\mathbf{x}}, \quad \text{for all } \hat{\mathbf{x}} \in X \text{ and } (\hat{\pi}, \hat{\beta}) \in \text{ext}(\Lambda) \tag{25b}$$

$$\mathbf{w} \in W. \tag{25c}$$

Benders decomposition can be applied by adding inequalities (25b) only as needed during the solution process. This process would solve a relaxation of (25) with a small subset of constraints (25b) present. Then, given an optimal solution $\hat{\mathbf{w}}$ to that relaxation, the inner problem to (23) is next solved to determine the actual value of the attacker–defender problem given $\hat{\mathbf{w}}$. If this value matches the value of the relaxation objective obtained from solving (25), then the algorithm terminates with an optimal solution. Otherwise, an inequality of the form (25b) is generated and added to the relaxation, and another iteration of the Benders decomposition algorithm is executed.

Backward sampling approach. Lozano and Smith (2017) propose a *backward-sampling approach* for solving interdiction problems where the interdiction decisions $\mathbf{x}$ are binary variables, i.e., $X \subseteq \{0,1\}^{n_L}$. The idea of this approach is based largely on that of Benders decomposition as described above. Instead of capturing all possible follower's decisions via constraints using strong duality, this approach partially enumerates (via sampling) and maintains a subset of the follower's solutions $\hat{Y} \subseteq Y$. Given such a subset $\hat{Y}$, the optimal objective value of the following model gives the maximum *perceived damage* made by the leader:

$$z^P(\hat{Y}) := \max_{\mathbf{x}\in X} \min_{\mathbf{y}\in\hat{Y}(\mathbf{x})} f(\mathbf{x}, \mathbf{y}), \tag{26}$$

where $\hat{Y}(\mathbf{x}) = \hat{Y} \cap Y(\mathbf{x})$. Value $z^P(\hat{Y})$ is the objective function value anticipated by the leader, if the leader is blind to all other possible solutions not in $\hat{Y}$ that the follower can make. Letting $\hat{\mathbf{x}}$ be an optimal solution to (26), the *real damage* caused by decision $\hat{\mathbf{x}}$ (evaluated by considering all possible follower's decisions) is given by:

$$z^R(\hat{\mathbf{x}}) := \min_{\mathbf{y}\in Y(\hat{\mathbf{x}})} f(\hat{\mathbf{x}}, \mathbf{y}). \tag{27}$$

Clearly, $z^R(\hat{\mathbf{x}})$ and $z^P(\hat{Y})$ provide lower and upper bounds on the optimal objective value z^* respectively, i.e., $z^R(\hat{\mathbf{x}}) \le z^* \le z^P(\hat{Y})$. If the two bounds are not equal, then the corresponding optimal follower's decision $\hat{\mathbf{y}}$ in (27) must not belong to $\hat{Y}$, and therefore we can update $\hat{Y}$ by $\hat{Y} := \hat{Y} \cup \{\hat{\mathbf{y}}\}$. Additional samples of feasible solutions in Y can be generated to supplement $\hat{Y}$, while other elements of $\hat{Y}$ can be removed depending on their corresponding objective function values.

The algorithm then solves (26) with the updated set $\hat{Y}$ of follower's decisions. The finiteness of the algorithm is guaranteed by the finiteness of the leader's feasible set X. The success of this approach relies on the following aspects: (i) the increasing size of the sampled solution set $\hat{Y}$ should be well-maintained so that the perceived damage problem (26) can be solved efficiently; (ii) an efficient sampling approach that supplies a diverse sample in Y needs to be employed; and (iii) a reasonably efficient approach should be available to solve the real damage problem (27). Note that the backward sampling approach is similar to that of standard Benders decomposition. A master problem with a restricted set $\hat{Y} \subseteq Y$ of the follower's decisions is solved to yield an upper bound, while a subproblem with a fixed leader's decision $\hat{\mathbf{x}}$ is solved to yield a feasible solution (which is used to update the lower bound).

Moreover, this study also examines the DAD setting, using inequalities similar to (25b) to guide the fortification decisions. The given approach employs the bounds obtained by computing real and perceived damage values given fortification decisions, and uses the objective function bound from the best obtained solution (the "incumbent value") to reduce the number of backward sampling searches. In particular, when the backward sampling bounds indicate that a fortification decision cannot improve the incumbent value, the backward sampling search corresponding to that fortification vector is terminated and a combinatorial Benders inequality (Codato & Fischetti, 2006) is generated to cut off that fortification solution. Other algorithmic enhancements for the DAD algorithm are detailed in Lozano and Smith (2017).

Benders primal decomposition. When the follower's problem is modeled as a mixed integer program with a finite number of integer feasible solutions, the *Benders primal decomposition* approach (also known as the column-and-constraint generation method, see, e.g., Zeng & Zhao, 2013) can alternatively be employed. In contrast to standard Benders decomposition, where the number of decision variables is fixed, Benders primal decomposition iteratively tightens an approximation to the extended single-level reformulation of the problem by adding both new decision variables and new constraints. These new decision variables correspond to the follower's response given a fixed leader's decision $\hat{\mathbf{x}}$, and the new constraints enforce the optimality condition for the follower's response. This approach has proved to be effective for applications of network interdiction problems arising in vulnerability analysis of power systems, see, e.g., Zhao and Zeng (2013), Yuan, Zhao, and Zeng (2014), Yuan et al. (2016), and Wu and Conejo (2017).

Iterative convex restrictions. When the follower's problem is modeled as a mixed integer program, another possible solution approach is based on the creation of convex approximations to the follower's problem. This approach is taken by Tang, Richard, and Smith (2016) for interdiction problems in which the leader's variables are binary and the follower solves a mixed integer program. In their model, the leader's interdiction decisions affect the follower's feasible region but not the objective.

The algorithm builds a convex inner-approximation to the follower's feasible region, which can be solved by "dualize-and-combine" (see Section 3.1.1), yielding a lower bound on the overall problem. Much like the backward sampling approach described above, given the leader's solution, the algorithm then solves the actual follower's problem as a mixed integer program and compares the objective value that the follower would obtain given this interdiction with the lower bound previously computed. If these values do not match, then the convex inner approximation to the follower's problem is expanded accordingly and the algorithm reiterates until an optimal solution is provably obtained. The critical step in this procedure lies in the formulation of this convex inner approximation: if the inner approximation is merely a convex hull of the follower's solutions that have already been observed, then the algorithm performs poorly. However, if the inner approximation implicitly includes many follower solutions that have not been explicitly computed thus far, then the algorithm performs far better. The latter case has shown to arise in binary knapsack interdiction and clique interdiction problems according to Tang et al. (2016).

4. Recent and emerging interdiction studies

We now discuss some recent interdiction studies, especially those that relax the assumptions made in Section 1 of this paper. Section 4.1 regards problems in which both agents act simultaneously, effectively modeling the situation when the follower is unaware of the leader's actions. Section 4.2 examines the problems where data or interdiction actions are uncertain. Section 4.3 discusses dynamic interdiction problems involving repeated interaction between the agents within one game. Section 4.4 considers interdiction problems in which information asymmetry exists. Section 4.5 explores problems in which information is incomplete for either the leader or follower.

4.1. Simultaneous play

The case in which the two agents play simultaneously gives rise to a large field of research. While this research is largely beyond the scope of this paper, it is instructive to highlight some core principles behind simultaneous play as they relate to interdiction. We begin by examining the work of Washburn and Wood (1995) regarding a two-player interdiction problem involving an evader, who wishes to choose a path to avoid detection, and an interdictor, who can monitor any single arc. If the interdictor chooses to monitor arc $(i, j) \in A$, then the evader is detected with probability p_{ij} if the evader's path includes arc (i, j). In this zero-sum game, the evader seeks to minimize its probability of detection, whereas the interdictor seeks to maximize the probability of detecting the evader. However, in this setting the evader cannot see the interdictor's actions before committing to its path. Therefore, both agents essentially commit to their strategies simultaneously.

This situation results in mixed-strategy solutions for both agents: the interdictor selects a probability that it will interdict each of the arcs in the network, and the follower selects a probability for choosing each path in the network. Let H be the set of all origin-destination paths. Define x_{ij} as a variable stating the probability that the interdictor monitors arc $(i, j) \in A$, and y_h as a variable stating the probability that the evader uses path $h \in H$. Also, let Q be an $|A| \times |H|$ matrix, with $q_{ah} = p_a$ if arc a belongs to path h and $q_{ah} = 0$ otherwise, for all $a \in A$ and $h \in H$. Given a solution $(\hat{\mathbf{x}}, \hat{\mathbf{y}})$, the probability of detection is computed as $\hat{\mathbf{x}}^T Q \hat{\mathbf{y}}$. Washburn and Wood (1995) seek to find a Nash equilibrium solution $(\mathbf{x}^*, \mathbf{y}^*)$, i.e., one in which

$$\mathbf{y}^* \in \arg\min_{\mathbf{y} \geq \mathbf{0} : \mathbf{e}^T \mathbf{y} = 1} \left\{ (\mathbf{x}^*)^\top Q \mathbf{y} \right\}, \text{ and}$$

$$\mathbf{x}^* \in \arg\max_{\mathbf{x} \geq \mathbf{0} : \mathbf{e}^T \mathbf{x} = 1} \left\{ \mathbf{x}^\top Q \mathbf{y}^* \right\},$$

where $\mathbf{e}$ is a vector of all ones (having conforming dimension) above. That is, the Nash equilibrium solution satisfies the condition that neither the interdictor nor the evader wish to change their strategy, having observed the other's strategy. Among the contributions in Washburn and Wood (1995) is a linear-programming based algorithm to solve this problem in which the evader encodes their solution via a (polynomial) network flow solution as opposed to requiring the enumeration of all (exponentially many) paths.

Goldberg (2017) considers a form of this game with three major differences. The first difference is that the Washburn and Wood (1995) model essentially treats the $\mathbf{x}$-variables as the amount of effort in monitoring the arcs, where the probability of detection on arc a is a linear function ($p_a x_a$) of the interdiction effort applied to arc a. In the problem considered by Goldberg (2017), that probability becomes a nonlinear function of x_a, where the function is assumed to be logarithmically convex and decreasing. The second difference is a set of multiple possible origins and destinations that the evader may use. The third difference is that the evader's payoff is a function, c, of the origin-destination pair selected, multiplied by the total probability of evasion on the path selected (given by the product of evasion probabilities on the path). The interdictor's payoff is the negative of a *possibly different* function, d, of the evader's origin-destination pair, multiplied by the total probability of evasion on the path. Because c and d might be distinct, the problem is no longer a zero-sum game. Goldberg (2017) shows that Nash equilibrium solutions must still exist for this game, and can be computed (exactly or approximately depending on certain assumptions) in polynomial time.

Another application arises in a game studied by Baykal-Gürsoy, Duan, Poor, and Garnaev (2014) between an adversary and a first responder. The simplest version of their game involves a set of nodes, each of which is associated with an occupancy value (e.g., the number of civilians at that location), and a detection probability if monitored. The adversary's payoff for attacking a node is proportional to the node's occupancy, multiplied by the probability that the first responder fails to detect the adversary at the node. This problem yields a zero-sum game in which the adversary seeks to maximize its payoff by selecting a mixed strategy for node attacks, while the first responder seeks to minimize payoff by selecting its own mixed strategy for monitoring nodes. Another key contribution of Baykal-Gürsoy et al. (2014) comes in examining population flows among the nodes, as well as patrolling options among a set of nodes that the first responder can take. The authors employ a partially observable Markov decision process (POMDP) model to analyze this dynamic version of the game. We also refer the reader to Guan, He, Zhuang, and Hora (2017), Powell (2007) and Zhuang and Bier (2007) for a sampling of recent simultaneous interdiction games having national security implications.

4.2. Stochastic network interdiction problems

Two of the strongest assumptions of the classical network interdiction problem stated in the beginning of Section 1.1 are assumptions A1 and A2, where it is assumed that all problem data is known to both the leader and the follower, and the leader is certain of the interdiction effect on the follower's problem. Here, we extend the scope of network interdiction problems into the realm of optimization under uncertainty by considering the case when the network interdiction problem involves uncertain data (such as the cost and interdiction effect on each arc), and the leader has to make an interdiction decision before the realization of uncertainty. However, we do assume that the leader has some knowledge about the underlying probability distribution of the random variables that are used to characterize the uncertainty, possibly in the form of a finite set of scenarios. We also assume that the follower is able to make decisions by solving a deterministic optimization problem after observing both the realization of random variables and the leader's decision. We refer to this setting as a stochastic network interdiction problem (SNIP) with a "wait-and-see" follower. In the next section, we discuss the case when both the leader and the follower need to make their decisions before the realization of random variables, which we refer to as an SNIP with a "here-and-now" follower.

For example, consider the shortest path interdiction problem (4) with uncertain arc costs and interdiction effects $(\tilde{c}(\xi), \tilde{d}(\xi))$, where $\xi \in \Xi$ is a random vector that follows a known joint probability distribution. Since the leader makes decisions under uncertainty, their risk preference plays a key role in terms of formulating the objective function of the problem. Most literature on SNIPs assumes that the leader is a risk-neutral decision maker, i.e., in the context of the shortest path interdiction, they maximize the expected shortest path value taken by the follower:

$$\max_{\mathbf{x}\in X} \mathbb{E}[f(\mathbf{x}, \xi)], \tag{28}$$

where $f(\mathbf{x}, \xi)$ represents the shortest path value taken by the follower under each realization ξ:

$$\begin{aligned} f(\mathbf{x}, \xi) := \min \; & \sum_{(i,j)\in A} \left[c_{ij}(\xi) + d_{ij}(\xi)x_{ij}\right]y_{ij} \\ \text{s.t. } & T\mathbf{y} = \mathbf{b} \\ & y_{ij} \geq 0, \;\; \forall (i,j) \in A. \end{aligned}$$

SNIPs such as (28) are a special case of stochastic programs (Shapiro, Dentcheva, & Ruszczynski, 2009). Stochastic programs are challenging to solve, as one can see in (28) that even with a fixed interdiction decision $\mathbf{x}$, computing the objective involves high-dimensional integration. Among all approaches that have been studied in the stochastic programming literature, two classes of approaches have been particularly popular for SNIPs: (i) sequential approximation and (ii) sample average approximation.

Cormican et al. (1998) propose a sequential approximation approach to solve SNIPs where interdictions may fail randomly (they focus on SNIPs in the context of the maximum flow interdiction problems). These authors apply classical bounding techniques in stochastic programming (see, e.g., Kall & Wallace, 1994) on (28), and recursively tighten the bounds until the optimality gap is small enough by refining partitions of the support of random vector ξ. On the other hand, the sample average approximation (SAA) approximates the original distribution of ξ by its empirical distribution (possibly via Monte Carlo sampling) in the form of a set of scenarios $\{(\mathbf{c^k}, \mathbf{d^k})\}_{k\in\mathcal{N}}$, where each scenario happens with probability p_k ($p_k = 1/|\mathcal{N}|$ if Monte Carlo sampling is used).

$$\max_{\mathbf{x}\in X} \sum_{k\in\mathcal{N}} p_k \min_{\mathbf{y^k}} \sum_{(i,j)\in A} (c_{ij}^k + d_{ij}^k x_{ij})y_{ij}^k \tag{29a}$$

$$\text{s.t. } T\mathbf{y^k} = \mathbf{b} \tag{29b}$$

$$y_{ij}^k \geq 0, \;\; \forall (i,j) \in A. \tag{29c}$$

We note that there is one copy of the follower's decision $\mathbf{y^k}$ for each scenario $k \in \mathcal{N}$, because the follower is given the flexibility to choose different paths for different scenarios. The relationship between the SAA problem (29) and the corresponding original stochastic program (28) has been extensively studied in the stochastic programming literature (see, e.g., Shapiro et al., 2009), and most SNIP studies focus on solving the SAA problems such as (29).

Computational aspects for solving SNIPs. From a computational perspective, the "dualize-and-combine" approach is less competitive in solving (29) than algorithms that enable decomposition by scenarios such as Benders decomposition, especially when the number of scenarios is large. These decomposition algorithms (e.g., Janjarassuk & Linderoth, 2008, for stochastic maximum flow interdiction problems with interdiction effect uncertainty) can be implemented in a parallel computing framework, leveraging high-performance computing resources. Note that since the feasible set X of interdiction decisions usually involves integrality restrictions, it is computationally more efficient to integrate Benders decomposition into a branch-and-bound framework. This so-called branch-and-cut algorithm typically outperforms a naive cutting plane approach that solves an integer program at each iteration.

This line of research has developed strong valid inequalities for the stochastic maximum reliability path interdiction problem. In this problem, the follower seeks a path having the highest chance of avoiding detection from an origin to a destination. The leader, on the other hand, allocates interdiction budget to increase detection rates on an optimally chosen subset of arcs so that this chance is minimized. We note that the maximum reliable path interdiction problem is equivalent to the shortest path interdiction problem if the chance of being detected on each arc is less than 1. The leader's knowledge of the follower's origin-destination pair is assumed to be uncertain, and is characterized by a finite set of scenarios. Motivated by the mixing structure (Atamtürk, Nemhauser, & Savelsbergh, 2000; Günlük & Pochet, 2001) of the underlying large-scale mixed integer programming formulation, Pan and Morton (2008) propose a set of strong valid inequalities called "step inequalities" to strengthen the linear programming relaxation bound of the formulation. Sullivan, Smith, and Morton (2014b) generalize these inequalities for problems involving asymmetric data perceptions (see Section 4.4 for more on such problems) and provide a convex hull analysis. Bodur, Dash, Günlük, and Luedtke (2016) strengthen the generated Benders cuts by exploiting the integrality of the interdiction decisions. More recently, Towle and Luedtke (2018) reformulate this problem using a path-based formulation, and propose additional valid inequalities exploiting the supermodularity structure (see, e.g., Nemhauser & Wolsey, 1988, Chapter III.3) resulting from the reformulation.

In addition to the risk-neutral model, where the leader maximizes the expected interdiction effect, SNIPs with a risk-averse leader have also been studied in the literature. Instead of optimizing average performance over the long run, a risk-averse leader hedges against the risk of disastrous outcomes under certain risk measures such as the conditional value at risk, which typically fits the mindset of a defender, e.g., in a homeland security setting. For example, Atamtürk, Deck, and Jeon (2019) model the risk aversion of the leader by a mean-risk model and reformulate it using a convex quadratic mixed integer program. Song and Shen (2016) propose an alternative risk-averse model using chance constraints (Shapiro et al., 2009). These works exploit not only the combinatorial structures from the SNIPs but also additional structures embedded within the risk measures.

4.3. Dynamic network interdiction

In this section, we focus on two zero-sum games. In both of these games, players have full information about the network and its data. However, these games depart from assumption A4, under which the leader and follower repeatedly select their actions in an alternating fashion throughout the course of the game.

Sefair and Smith (2016) explore a dynamic shortest path interdiction (DSPI) problem, where a defender dynamically decides an optimal set of arcs to interdict throughout the course of the game. An interdicted arc increases in cost, as before, and the defender has a limited number of arcs that (s)he can increase throughout the course of the game. The distinguishing feature of this game is that the defender alternates turns with the attacker (the agent seeking the shortest path). The defender first selects a (possibly empty) set of arcs to interdict, and then the attacker chooses a single arc to traverse. The game iterates in this fashion until the attacker reaches its destination node. Unlike most interdiction games, it may be uniquely optimal for the defender to interdict fewer arcs than budgeted – in fact, a unique optimal solution may involve interdicting no arcs at all. Furthermore, the attacker may traverse a cycle in the network, even reusing arcs, at optimality.

The DSPI can be formulated using dynamic programming, where each state consists of the set of arcs interdicted so far and the position of the attacker in the network. However, the size of the state space is an exponential function of the defender's interdiction budget. Alternatively, Sefair and Smith (2016) propose bounding techniques for the problem by analyzing two variations of the game. The first variation yields a lower bound by supposing that interdiction actions "expire" after the attacker's next move, meaning that interdicted arcs return to their original costs. Essentially, this variation serves to reduce the state space of the dynamic program, allowing the problem to be solved in polynomial time. The second variation yields an upper bound by simply reducing the input network to an acyclic network, which again reduces of the state space size to a polynomial function of the network size.

The DSPI is solvable in polynomial time for a fixed interdiction budget. This need not be the case for all dynamic interdiction games, though, as shown by Sefair and Smith (2017) for a dynamic assignment interdiction (DAI) problem. The DAI involves a bipartite assignment network, in which a set of jobs must be matched to a set of machines. For the purpose of describing the problem, we say that the follower seeks a minimum-cost assignment, and the leader seeks to interdict arcs to maximize the value of a minimum-cost assignment. As before, each arc (representing a job-to-machine assignment) can be interdicted, resulting in an increased cost of the corresponding assignment. The game begins with the leader interdicting a set of arcs (as in the DSPI), with the follower acting next to assign job 1 to a machine. The leader need only consider interdicting assignment arcs corresponding to job 1 in the first iteration. At iteration $k \geq 2$ of this game, the leader interdicts some set of arcs corresponding to assigning job k to a machine that has not been assigned to jobs $1, \ldots, k-1$, and the follower responds by assigning job k to an unassigned machine. The total number of arcs that the leader can interdict throughout the entire game is limited by an upper bound. Like the DSPI, the DAI can again be solved by an exponential state-space dynamic program; however, unlike the DSPI, the DAI remains strongly NP-hard even if the leader has an interdiction budget of one arc.

4.4. Network interdiction with asymmetric information

In this section, we discuss cases when assumption A3 is relaxed. This may be simply due to the fact that the two players have different objective functions in their corresponding optimization models. Alternatively, the two players may not have the same perception of their problem data, i.e., assumption A3 is violated as a result of a violation of assumption A1. Information asymmetry may be inherent in that the defender may have more accurate information about the system that they work with, or may be a result of deception tactics such as decoy assets for defense (Salmerón, 2012). For simplicity, we assume that the leader (defender) always has accurate information. The interactions between the two players are still modeled as a max-min game; however, the leader aims to maximize the minimum objective of the follower using actual data, while the follower optimizes their objective using their perceived data. The leader and the follower solve their respective problems using the objective functions of the same form but with different coefficients. This gives rise to a special form of bilevel optimization, where the upper-level and lower-level problems only differ by their coefficients.

Taking the shortest path interdiction problem (4) as an example, suppose that the leader's perception about the cost and interdiction effect on each arc (i, j), c_{ij} and d_{ij}, respectively, is accurate. The follower, on the other hand, perceives these values differently as $\bar{c}_{ij}$ and $\bar{d}_{ij}$, due to asymmetric information. Bayrak and Bailey (2008) assume that the follower's inaccurate perception is fully known to the leader, and thus formulate the shortest path interdiction problem with asymmetric information as a bilevel optimization problem (see Section 1.3.1). The shortest path network interdiction problem with asymmetric information can be modeled as follows:

$$\max_{\mathbf{x}\in X} \sum_{(i,j)\in A} (c_{ij} + d_{ij}x_{ij})\hat{y}_{ij}, \tag{30}$$

where

$$\hat{\mathbf{y}} \in \arg\min \left\{ \sum_{(i,j)\in A} (\bar{c}_{ij} + \bar{d}_{ij}x_{ij})y_{ij} \mid (4b), (4c) \right\}.$$

Information asymmetry also arises in SNIPs where both the leader and the follower need to make their decisions before the realizations of uncertainty involved in the network, i.e., the SNIP with a "here-and-now" follower (as opposed to the SNIP with a "wait-and-see" follower, which was mentioned in the previous section). In this problem, the risk preferences of both players are relevant to their respective optimization problems, which are likely to be heterogenous unless both players are risk neutral (Lei, Shen, & Song, 2018). Putting this consideration into the context of stochastic shortest path interdiction, suppose that the leader and follower make their decisions according to their risk measures $\rho_L(\cdot)$ and $\rho_F(\cdot)$, respectively, and assume that the follower's risk preference is completely known by the leader. Then the leader solves the following bilevel optimization problem:

$$\min_{\mathbf{x}\in X} \rho_L\left(\sum_{(i,j)\in A} (\tilde{c}_{ij}(\xi) + \tilde{d}_{ij}(\xi)x_{ij})\hat{y}_{ij} \right), \tag{31}$$

where

$$\hat{\mathbf{y}} \in \arg\min \left\{ \rho_F\left(\sum_{(i,j)\in A} (\tilde{c}_{ij}(\xi) + \tilde{d}_{ij}(\xi)x_{ij})y_{ij} \right) \mid (4b), (4c) \right\}.$$

In this setting, information asymmetry gives the defender an advantage that can be exploited to better utilize limited defense resources (Salmerón, 2012; Sullivan et al., 2014a). By contrast, we later consider the case when the attacker (modeled as the follower) holds "private" information that is not completely known by the defender (for example, the risk preference of the follower $\rho_F(\cdot)$ may not be completely known to the leader), putting the attacker at an advantage.

4.5. Network interdiction with incomplete information

In this section, we discuss defender–attacker problems where assumption A1 does not hold, and data pertaining to the network interdiction problem is not fully available. Both agents may have to learn key parameters of their opponent's optimization problem either from historical data or from their ongoing interactions. Taking the defender's perspective (as the leader), we assume that the follower is fully knowledgeable about their problem, while the leader only has partial information about this problem. The leader therefore makes a robust defensive plan by allowing the follower (the attacker) the advantage of full problem information.

Network interdiction with offline learning. Under assumption A5, where only one round of the interdiction game is played, the leader makes their interdiction decision based completely on available historical data. Pay, Merrick, and Song (2019) consider a stochastic network interdiction problem with a "wait-and-see" follower. The leader is assumed to be a risk-averse decision maker whose preferences can be modeled using expected utility theory (Aumann, 1962). However, the exact form of the utility function is ambiguous to the leader. Pay et al. (2019) assume that historical data on the leader's past choices is available. The knowledge learned from the data forms an ambiguity set of utility functions that are compatible with the leader's past behaviors. Pay et al. (2019) take a robust optimization perspective by optimizing the interdiction decision with respect to the worst-case utility among all utility functions compatible with historical data.

An arguably more interesting case is the stochastic network interdiction problem with a "here-and-now" follower, where the follower solves an optimization problem under uncertainty according to a utility function that characterizes their own risk preference, but where the follower's utility function is unknown to the leader. The leader assumes that the follower optimizes their decisions according to an optimization model (such as the expected utility model), and tries to glean the follower's private parameters (such as risk aversion) from the observed follower's behaviors, which are considered to be optimal solutions to the presumed optimization model. The problem of finding the best such estimation is known as the inverse optimization problem (Ahuja & Orlin, 2001; Aswani, Shen, & Siddiq, 2018; Esfahani, Shafieezadeh-Abadeh, Hanasusanto, & Kuhn, 2018). However, from the network interdiction perspective, assuming that the attacker makes decisions according to an optimal solution to a specific model is risky: The follower may not be solving the optimization model assumed by the leader, or the follower may not have the resources to solve the optimization model exactly. Instead, the leader can construct an ambiguity set of all possible utility functions that the follower can take in order to be compatible with their past behaviors, according to historical data. The leader then aims at minimizing the highest possible utility value among all utilities contained in this ambiguity set, from the perspective of protecting against the worst-case scenario. Unfortunately, this problem appears to be computationally challenging, as the inner problem for any fixed interdiction plan becomes a nonconvex optimization problem. Solution techniques reviewed in Section 3.2 are worth exploring to tackle this problem.

Network interdiction with online learning. When the interdiction games are played in multiple rounds (i.e., assumption A5 is relaxed), the leader is provided an opportunity to learn about the follower's optimization problem not only from historical data, but also from the *feedback* generated by the follower's reactions during these multiple rounds of games. Such a general problem setting that involves interplays between optimization and learning has been studied in the literature under the realm of sequential learning and game theory (Cesa-Bianchi & Lugosi, 2006).

Borrero, Prokopyev, and Sauré (2015) propose the novel idea of formulating sequential network interdiction games in an online optimization framework. They assume that the full information version of the problem reduces to the deterministic network interdiction problem. Specifically, by playing multiple rounds of network interdiction games, the leader refines their incomplete information about the follower's problem by learning the cost parameters and available resources corresponding to the follower's problems from the follower's actions revealed in these games. The leader not only determines how to optimally allocate interdiction resources to negatively impact the follower's objective to the largest extent, but also attempts to make the follower reveal as much information as possible so that a more informed interdiction decision can be made in subsequent games. This corresponds to a typical exploration–exploitation trade-off in online optimization problems such as the multi-armed bandit problems (Auer, Cesa-Bianchi, & Fischer, 2002). Borrero et al. (2015) propose a "greedy-and-robust" policy, where the leader "greedily" optimizes their objective by solving a robust optimization problem with an uncertainty set constructed using the current information available about the follower. They show that this policy successfully balances exploitation and exploration in the online optimization setting, eventually matching the optimal interdiction decisions made under perfect information after a finite number of rounds.

Zheng and Castañón (2012) study dynamic network flow interdiction games where the attacker has imperfect knowledge of the network topology while the network operator (defender) has perfect information. The attacker can learn about the topology by monitoring network operations, while the operator observes the attacker's monitoring actions and chooses to avoid parts of the network being monitored by the attacker to hide information from the attacker. After a finite number of stages, the attacker conducts an optimal interdiction to maximize the expected network flow disruption according to their imperfect knowledge about the network topology at that point, which is represented by a probability distribution over possible states in the information sets. Zheng and Castañón (2012) decompose this dynamic game into a sequence of subgames, each of which is defined starting from an arbitrary initial distribution of states in such information sets, and use POMDP algorithms to recursively obtain an equilibrium strategy of each subgame.

5. Select applications of network interdiction

We conclude by discussing newer applications of network interdiction and examining how addressing these applications will require the development of new interdiction algorithms. Section 5.1 examines new challenges of network interdiction applications in cyber-physical system (CPS) security. Section 5.2 discusses network interdiction applications in illicit supply chain network disruption. Section 5.3 summarizes current limitations of network interdiction models and solution algorithms, and points out some future directions of research in this area.

5.1. Cyber-physical system security

The importance of ensuring the resilience of a large-scale CPS, such as electrical power networks, communication networks, and transportation networks, cannot be overemphasized. Much of the difficulty associated with these problems stems from the interdependence between different layers of the CPS (including cyber, physical, and cyber-physical) as well as their dynamic interactions. For example, the operation of power grids relies on real-time control provided by an information network, while information networks also require power supplied from the grid. The interdependence of these networks makes them more vulnerable to adversarial attacks than independent networks (Pasqualetti, Dörfler, & Bullo, 2013) because of their larger "attack surfaces." Moreover, although classical network interdiction models remain vital in terms of defensive resource allocation at the strategic level, the dynamic interactions within a CPS impose new challenges for applying network interdiction models at the operational level. The complexity of CPS security calls for a holistic framework that integrates: (i) game theory – modeling the adversarial relationship between the defender and the attacker; (ii) control theory – modeling the dynamic interactions between the defender, the attacker and the system; and (iii) system theory – modeling the interdependence between various layers of the system.

Defense resource allocation against CPS attacks. We first consider how existing network interdiction models can be utilized to optimize defense resource allocation for CPS security at the strategic level. Abusorrah, Alabdulwahab, Li, and Shahidehpour (2017) consider load redistribution attacks in a smart electric grid (Yuan, Li, & Ren, 2011). Load distribution attacks are a kind of false data injection attack that can modify the actual load data d_i measured by a sensor in bus $i \in B$ to $d_i + \Delta d_i$. Assume that the actual system load $\mathbf{d}$ is subject to variations that can be described by a polyhedral uncertainty set $\mathcal{D}$. Under any system load $\mathbf{d}$, let $O^*(\mathbf{d})$ be the lowest possible operational cost without any attack, and let $O(\mathbf{w}, \mathbf{d})$ be the highest possible operational cost induced by a load redistribution attack given a defense resource allocation $\mathbf{w}$. The value $O^*(\mathbf{d})$ can be computed by solving an optimal power flow problem $\min_{\mathbf{p} \in P(\mathbf{d})} F(\mathbf{p})$, which minimizes total operational cost $F(\mathbf{p})$ over all feasible power flows $\mathbf{p}$ that satisfy certain physical constraints $P(\mathbf{d})$ based on the load distribution $\mathbf{d}$. Computing $O(\mathbf{w}, \mathbf{d})$ involves solving a bilevel problem:

$$\max_{\Delta\mathbf{d} \in \mathcal{C}(\mathbf{w},\mathbf{d})} \left\{ \min_{\mathbf{p} \in \tilde{P}(\mathbf{d},\Delta\mathbf{d})} F(\mathbf{p}) \right\}, \tag{32}$$

where $\mathcal{C}(\mathbf{w}, \mathbf{d})$ defines the possible load redistribution attacks that can be done given defense allocation $\mathbf{w}$ and system load $\mathbf{d}$, and $\tilde{P}(\mathbf{d}, \Delta\mathbf{d})$ is the set of feasible power flow under the corrupted data. Model (32) can be reformulated as a single-level maximization problem by using the standard "dualize-and-combine" approach.

Abusorrah et al. (2017) then model the defender's decision-making from a robust optimization perspective, and consider defending against the worst case scenario in terms of the difference between $O(\mathbf{w}, \mathbf{d})$ and $O^*(\mathbf{d})$ among all possible system load variations $\mathbf{d} \in \mathcal{D}$:

$$\min_{\mathbf{w} \in S} \max_{\mathbf{d} \in \mathcal{D}} \{O(\mathbf{w}, \mathbf{d}) - O^*(\mathbf{d})\}, \tag{33}$$

where S gives the defense resource allocation constraints, including, e.g., financial budget constraints and computing resource constraints, limiting the number of security checkpoints that can be placed in the CPS network. Algorithms described in Section 3.2 can be applied to solve the min-max MIP problem (33).

Attack detection in CPS. Attack detection is usually ignored by classical network interdiction models, which assume the existence of a single attacker whose actions can be fully observed and evaluated. In modern CPS, various types of sensors are distributed across the network to collect data, and anomalous attacks are detected and identified by statistical or machine-learning algorithms based on collected sensor data. Due to the variety of attacks that could be launched on a CPS, attack detection devices and algorithms are imperfect. These devices can be configured with respect to their detection sensitivity, allowing the CPS operator to find the appropriate balance between the expected time to detection and false alarm rate. Ghafouri, Abbas, Laszka, Vorobeychik, and Koutsoukos (2016) discuss the problem of optimizing detection thresholds that minimize expected damage incurred by detection delay, while maintaining the false alarm rate to be within a tolerable limit. The attack detection problem itself can be seen as an interdiction problem: the defender acts as the leader, configuring its devices to balance the expected damage from potential attacks with the negative impact brought by false alarms, and the attacker acts as the follower, finding the best time to launch the attack that leads to the highest damage given the detection configuration set by the defender.

Dynamic and interdependence of CPS attacks. Finally, we consider dynamic CPS defense strategies over time. Recently, cyber and cyber-physical security threats have been growing in both quantity and complexity. Defense strategies must be able to adapt to real-time information learned from sensors that reveal adversarial emergent behaviors (Strapp & Yang, 2014). Addressing such problems requires a holistic framework that incorporates system states and information states, and accordingly optimizes defensive strategies that deal with attackers of heterogeneous types arriving at unknown rates. Most of the existing literature in this area focuses on static network interdiction models, and does not properly capture the dynamic nature of interactions between the defender and the attackers. Network interdiction models need to be integrated with models for sequential decision making in an environment that can itself change dynamically over time, such as MDP models (Gutin, Kuhn, & Wiesemann, 2014). The situation is further complicated when neither player has complete information about the other player's payoff function, feasible action space, etc., as discussed in Section 4.5, in which case models such as POMDP (Baykal-Gürsoy et al., 2014; Zheng & Castañón, 2012) and repeated Bayesian games (Liu, Comaniciu, & Man, 2006) should be integrated. See Etesami and Başar (2019) for a recent survey on dynamic security games arising in CPS.

5.2. Interdicting illicit supply networks

In this section, we discuss new applications of network interdiction problems to disrupting illicit supply chain networks. Traditionally, these applications focus on smuggling illegal materials such as nuclear weapons (McLay, Lloyd, & Niman, 2011; Morton et al., 2007) through a given network. The smugglers (attackers) maximize the amount of illegal materials sent from an origin to a destination. This can be formulated as a maximum flow problem. The defender, on the other hand, optimizes their interdiction decisions according to a budget constraint to diminish the optimal flow value.

New applications of network interdiction problems on illicit supply network disruption focus on modeling the interdependence between the interdiction decisions defined on the network. Malaviya, Rainwater, and Sharkey (2019) consider a problem motivated by city-level illegal drug enforcement applications. They model an information network connecting drug dealers at each hierarchical level. This information network is interconnected with a physical network, communicating information on drug dealers' actions and providing feedback to them. Law enforcement officials make interdiction decisions over multiple periods that follow a certain logical sequence: local drug dealers need to be captured (interdicted) first in order to provide evidence/information for interdicting a higher-level drug dealer at a later time. Baycik, Sharkey, and Rainwater (2018) model the interdependent information network and physical network as a multi-layered network, and consider interdictions made on both networks simultaneously, with applications in both city-level illegal drug disruption and CPS security.

Another prominent challenge for network interdiction with integrated information and physical networks is that key structures in the information networks used by the attackers are intentionally hidden from the defender. Konrad, Trapp, Palmbach, and Blom (2017) examine such problems in human trafficking networks, which include hidden victims and covert traffickers.

The defender may have to commit defense resources without full knowledge of the information network. It is therefore critical to gather incomplete information piece by piece from various sources such as social media, and make robust interdiction decisions by effectively hedging against uncertainty. These challenges further motivate emerging interdiction studies described in Section 4, such as network interdiction with incomplete information in a dynamic environment.

5.3. Current limitations and some future directions of research

In the following, we identify some current limitations of modeling and solution methodologies for addressing challenges arising from new network interdiction problem variants.

First, the computational efficiency of optimizing adaptive defense strategies is a bottleneck for successfully applying them to large-scale systems such as those pertaining to electric power grids. It is crucial to develop next-generation computationally efficient algorithms and robust computational infrastructure that enable these algorithms to compute near-optimal strategies.

Second, the complexity of a holistic modeling framework for defending large-scale interdependent systems calls for a multi-agent framework with varying levels of autonomy among multiple defenders. The multi-agent framework should characterize how defenders learn and adapt from their local environment with limited data, and share information with the centralized decision maker (if any exists) and other local defenders via limited communication (Leitao et al., 2016; Sreekumaran, Hota, Liu, Uhan, & Sundaram, 2015).

Third, most existing defense strategies are reactive in nature. As cyber and cyber-physical security threats are growing fast in both quantity and variety, existing reactive defense strategies may soon reach their limits in mitigating these threats. New defense strategies, such as proactively disrupting the social–information networks that connect adversarial organizations and agents should be developed.

References

Abusorrah, A., Alabdulwahab, A., Li, Z., & Shahidehpour, M. (2017). Minimax-regret robust defensive strategy against false data injection attacks. *IEEE Transactions on Smart Grid, 10*(2), 2068–2079.

Ahuja, R. K., & Orlin, J. B. (2001). Inverse optimization. *Operations Research, 49*(5), 771–783.

Alarie, S., Audet, C., Jaumard, B., & Savard, G. (2001). Concavity cuts for disjoint bilinear programming. *Mathematical Programming, 90*(2), 373–398.

Altner, D. S., Ergun, O., & Uhan, N. A. (2010). The maximum flow network interdiction problem: Valid inequalities, integrality gaps, and approximability. *Operations Research Letters, 38*(1), 33–38.

Assimakopoulos, N. (1987). A network interdiction model for hospital infection control. *Computers in Biology and Medicine, 17*(6), 413–422.

Aswani, A., Shen, Z.-J., & Siddiq, A. (2018). Inverse optimization with noisy data. *Operations Research, 66*(3), 870–892.

Atamtürk, A., Deck, C., & Jeon, H. (2019). *Successive quadratic upper-bounding for discrete mean-risk minimization and network interdiction*. BCOL Research Report 17.05, UC Berkeley (in press).

Atamtürk, A., Nemhauser, G. L., & Savelsbergh, M. W. (2000). The mixed vertex packing problem. *Mathematical Programming, 89*(1), 35–53.

Auer, P., Cesa-Bianchi, N., & Fischer, P. (2002). Finite-time analysis of the multiarmed bandit problem. *Machine Learning, 47*(2–3), 235–256.

Aumann, R. J. (1962). Utility theory without the completeness axiom. *Econometrica: Journal of the Econometric Society, 30*(3), 445–462.

Ball, M. O., Golden, B. L., & Vohra, R. V. (1989). Finding the most vital arcs in a network. *Operations Research Letters, 8*(2), 73–76.

Baycik, N. O., Sharkey, T. C., & Rainwater, C. E. (2018). Interdicting layered physical and information flow networks. *IISE Transactions, 50*(4), 316–331.

Baykal-Gürsoy, M., Duan, Z., Poor, H. V., & Garnaev, A. (2014). Infrastructure security games. *European Journal of Operational Research, 239*(2), 469–478.

Bayrak, H., & Bailey, M. D. (2008). Shortest path network interdiction with asymmetric information. *Networks, 52*(3), 133–140.

Ben-Tal, A., El Ghaoui, L., & Nemirovski, A. (2009). Robust optimization. *Princeton series in applied mathematics*. Princeton, NJ: Princeton University Press.

Bertsimas, D., & Sim, M. (2004). The price of robustness. *Operations Research, 52*(1), 35–53.

Bertsimas, D., & Thiele, A. (2006). Robust and data-driven optimization: Modern decision-making under uncertainty. In M. P. Johnson, B. Norman, & N. Secomandi (Eds.), *Tutorials in operations research: Models, methods, and applications for innovative decision making* (pp. 95–122). Catonsville, MD: INFORMS.

Bodur, M., Dash, S., Günlük, O., & Luedtke, J. (2016). Strengthened Benders cuts for stochastic integer programs with continuous recourse. *INFORMS Journal on Computing, 29*(1), 77–91.

Borrero, J. S., Prokopyev, O. A., & Sauré, D. (2015). Sequential shortest path interdiction with incomplete information. *Decision Analysis, 13*(1), 68–98.

Brown, G. G., Carlyle, W. M., Harney, R. C., Skroch, E. M., & Wood, R. K. (2009). Interdicting a nuclear-weapons project. *Operations Research, 57*(4), 866–877.

Brown, G. G., Carlyle, W. M., Salmerón, J., & Wood, R. K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530–544.

Caprara, A., Carvalho, M., Lodi, A., & Woeginger, G. J. (2016). Bilevel knapsack with interdiction constraints. *INFORMS Journal on Computing, 28*(2), 319–333.

Cesa-Bianchi, N., & Lugosi, G. (2006). *Prediction, learning, and games*. Cambridge, UK: Cambridge University Press.

Church, R. L., Scaparra, M. P., & Middleton, R. S. (2004). Identifying critical infrastructure: The median and covering facility interdiction problems. *Annals of the Association of American Geographers, 94*(3), 491–502.

Codato, G., & Fischetti, M. (2006). Combinatorial Benders' cuts for mixed-integer linear programming. *Operations Research, 54*(4), 756–766.

Cormican, K. J., Morton, D. P., & Wood, R. K. (1998). Stochastic network interdiction. *Operations Research, 46*(2), 184–197.

Dantzig, G. B., & Fulkerson, D. R. (1955). On the max flow min cut theorem of networks. *Technical Report, P-826*. Santa Monica, CA: The RAND Corporation.

Delage, E., & Iancu, D. A. (2015). Robust multistage decision making. In D. M. Aleman, & A. C. Thiele (Eds.), *Tutorials in operations research: The operations research revolution* (pp. 20–46). Catonsville, MD: INFORMS.

Dempe, S., Kalashnikov, V. V., Pérez-Valdés, G. A., & Kalashnykova, N. (2015). *Bilevel programming problems*. Heidelberg: Springer.

DeNegre, S. T., & Ralphs, T. K. (2009). A branch-and-cut algorithm for integer bilevel linear programs. In J. W. Chinneck, B. Kristjansson, & M. J. Saltzman (Eds.), *Operations research and cyber-infrastructure* (pp. 65–78). New York: Springer.

Elias, P., Feinstein, A., & Shannon, C. E. (1956). A note on the maximum flow through a network. *IRE Transactions on Information Theory, 2*(4), 117–119.

Esfahani, P. M., Shafieezadeh-Abadeh, S., Hanasusanto, G. A., & Kuhn, D. (2018). Data-driven inverse optimization with imperfect information. *Mathematical Programming, 167*(1), 191–234.

Etesami, S. R., & Başar, T. (2019). Dynamic games in cyber-physical security: An overview. *Dynamic Games and Applications*. doi:10.1007/s13235-018-00291-y.

Fischetti, M., Ljubic, I., Monaci, M., & Sinnl, M. (2019). Interdiction games and monotonicity, with application to knapsack problems. *INFORMS Journal on Computing, 31*(2), 390–410.

Ford, L. R., & Fulkerson, D. R. (1956). Maximal flow through a network. *Canadian Journal of Mathematics, 8*, 399–404.

Fulkerson, D. R., & Harding, G. C. (1977). Maximizing minimum source-sink path subject to a budget constraint. *Mathematical Programming, 13*(1), 116–118.

Ghafouri, A., Abbas, W., Laszka, A., Vorobeychik, Y., & Koutsoukos, X. (2016). Optimal thresholds for anomaly-based intrusion detection in dynamical environments. In Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, & W. Casey (Eds.), *Proceedings of the international conference on decision and game theory for security* (pp. 415–434). New York: Springer.

Ghare, P. M., Montgomery, D. C., & Turner, W. C. (1971). Optimal interdiction policy for a flow network. *Naval Research Logistics Quarterly, 18*(1), 37–45.

Goldberg, N. (2017). Non-zero-sum nonlinear network path interdiction with an application to inspection in terror networks. *Naval Research Logistics, 64*(2), 139–153.

Golden, B. (1978). A problem in network interdiction. *Naval Research Logistics Quarterly, 25*(4), 711–713.

Guan, P., He, M., Zhuang, J., & Hora, S. (2017). Modeling a multi-target attacker–defender game with budget constraints. *Decision Analysis, 14*(2), 87–107.

Günlük, O., & Pochet, Y. (2001). Mixing mixed-integer inequalities. *Mathematical Programming, 90*(3), 429–457.

Gutin, E., Kuhn, D., & Wiesemann, W. (2014). Interdiction games on Markovian PERT networks. *Management Science, 61*(5), 999–1017.

Harris, T. E., & Ross, F. S. (1955). Fundamentals of a method for evaluating rail net capacities. *Research Memorandum, RM-1573*. Santa Monica, CA: The RAND Corporation.

Israeli, E., & Wood, R. K. (2002). Shortest-path network interdiction. *Networks, 40*(2), 97–111.

Janjarassuk, U., & Linderoth, J. (2008). Reformulation and sampling to solve a stochastic network interdiction problem. *Networks, 52*(3), 120–132.

Kall, P., & Wallace, S. W. (1994). *Stochastic programming*. Chichester, UK: John Wiley and Sons.

Konrad, R. A., Trapp, A. C., Palmbach, T. M., & Blom, J. S. (2017). Overcoming human trafficking via operations research and analytics: Opportunities for methods, models, and applications. *European Journal of Operational Research, 259*(2), 733–745.

Lawler, E. L. (1976). *Combinatorial optimization, networks and matroids*. Dover.

Lei, X., Shen, S., & Song, Y. (2018). Stochastic maximum flow interdiction problems under heterogeneous risk preferences. *Computers & Operations Research, 90*, 97–109.

Leitao, P., Karnouskos, S., Ribeiro, L., Lee, J., Strasser, T., & Colombo, A. W. (2016). Smart agents in industrial cyber-physical systems. *Proceedings of the IEEE, 104*(5), 1086–1101.

Lemaréchal, C., Nemirovski, A., & Nesterov, Y. (1995). New variants of bundle methods. *Mathematical Programming, 69*(1–3), 111–147.

Lim, C., & Smith, J. C. (2007). Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions, 39*(1), 15–26.

Liu, Y., Comaniciu, C., & Man, H. (2006). A Bayesian game approach for intrusion detection in wireless ad hoc networks. *Proceeding from the 2006 workshop on game theory for communications and networks*. Pisa, Italy: ACM.

Lozano, L., & Smith, J. C. (2017). A value-function-based exact approach for the bilevel mixed-integer programming problem. *Operations Research, 65*(3), 768–786.

Magnanti, T. L., & Wong, R. T. (1981). Accelerating Benders decomposition: Algorithmic enhancement and model selection criteria. *Operations Research, 29*(3), 464–484.

Mahdavi Pajouh, F., Boginski, V., & Pasiliao, E. L. (2014). Minimum vertex blocker clique problem. *Networks, 64*(1), 48–64.

Malaviya, A., Rainwater, C., & Sharkey, T. C. (2012). Multi-period network interdiction problems with applications to city-level drug enforcement. *IIE Transactions, 44*(5), 368–380.

McLay, L. A., Lloyd, J. D., & Niman, E. (2011). Interdicting nuclear material on cargo containers using knapsack problem models. *Annals of Operations Research, 187*(1), 185–205.

McMasters, A., & Mustin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly, 17*, 261–268.

Mitsos, A. (2010). Global solution of nonlinear mixed-integer bilevel programs. *Journal of Global Optimization, 47*(4), 557–582.

Morton, D. P., Pan, F., & Saeger, K. J. (2007). Models for nuclear smuggling interdiction. *IIE Transactions, 39*(1), 3–14.

Morton, D. P., & Wood, R. K. (1999). Restricted-recourse bounds for stochastic linear programming. *Operations Research, 47*(6), 943–956.

Nemhauser, G. L., & Wolsey, L. A. (1988). *Integer and combinatorial optimization*. New York: Wiley.

Nguyen, K. T. (2016). Reverse 1-center problem on weighted trees. *Optimization, 65*(1), 253–264.

Pan, F., & Morton, D. P. (2008). Minimizing a stochastic maximum-reliability path. *Networks, 52*, 111–119.

Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control, 58*(11), 2715–2729.

Pay, B. S., Merrick, J. R. W., & Song, Y. (2019). Stochastic network interdiction with incomplete preference. *Networks, 73*(1), 3–22.

Phillips, C. A. (1993). The network inhibition problem. In *Proceedings of the twenty-fifth annual ACM symposium on the theory of computing* (pp. 776–785). New York: ACM.

Powell, R. (2007). Defending against terrorist attacks with limited resources. *American Political Science Review, 101*(3), 527–541.

Ratliff, H. D., Sicilia, G. T., & Lubore, S. H. (1975). Finding the *n* most vital links in flow networks. *Management Science, 21*(5), 531–539.

Rocco, C. M., & Ramirez-Marquez, J. E. (2010). A bi-objective approach for shortest-path network interdiction. *Computers and Industrial Engineering, 59*(2), 232–240.

Rocco, C. M., Ramirez-Marquez, J. E., & Salazar, D. E. (2010). Bi and tri-objective optimization in the deterministic network interdiction problem. *Reliability Engineering and System Safety, 95*(8), 887–896.

Royset, J. O., & Wood, R. K. (2007). Solving the bi-objective maximum-flow network-interdiction problem. *INFORMS Journal on Computing, 19*(2), 175–184.

Saharidis, G. K., & Ierapetritou, M. G. (2009). Resolution method for mixed integer bi-level linear problems based on decomposition technique. *Journal of Global Optimization, 44*(1), 29–51.

Salmerón, J. (2012). Deception tactics for network interdiction: A multiobjective approach. *Networks, 60*(1), 45–58.

Salmerón, J., Wood, K., & Baldick, R. (2009). Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems, 24*(1), 96–104.

Sefair, J. A., & Smith, J. C. (2016). Dynamic shortest-path interdiction. *Networks, 68*(4), 315–330.

Sefair, J. A., & Smith, J. C. (2017). Exact algorithms and bounds for the dynamic assignment interdiction problem. *Naval Research Logistics, 64*(5), 373–387.

Shapiro, A., Dentcheva, D., & Ruszczynski, A. (2009). *Lectures in stochastic programming: modeling and theory*. Philadelphia, PA: SIAM.

Sherali, H. D., & Shetty, C. M. (1980). A finitely convergent algorithm for bilinear programming problems using polar cuts and disjunctive face cuts. *Mathematical Programming, 19*, 14–31.

Smith, J. C., & Ahmed, S. (2011). Introduction to robust optimization. In J. J. Cochran (Ed.), *Wiley encyclopedia of operations research and management science*. Hoboken, NJ: Wiley.

Smith, J. C., Lim, C., & Alptekinoglu, A. (2009). New product introduction against a predator: A Bilevel Mixed-integer Programming approach. *Naval Research Logistics, 56*(8), 714–729.

Smith, J. C., Lim, C., & Sudargho, F. (2007). Survivable network design under optimal and heuristic interdiction scenarios. *Journal of Global Optimization, 38*(2), 181–199.

Song, Y., & Shen, S. (2016). Risk-averse shortest path interdiction. *INFORMS Journal on Computing, 28*(3), 527–539.

Sreekumaran, H., Hota, A. R., Liu, A. L., Uhan, N. A., & Sundaram, S. (2015). Multi-agent decentralized network interdiction games. arXiv preprint:1503.01100.

von Stackelberg, H. (1952). *The theory of the market economy*. London: William Hodge and Co.

Strapp, S., & Yang, S. J. (2014). Segmenting large-scale cyber attacks for online behavior model generation. In W. G. Kennedy, N. Agarwal, & S. J. Yang (Eds.), *Proceedings of the international conference on social computing, behavioral-cultural modeling, and prediction* (pp. 169–177). New York: Springer.

Sullivan, K. M., Morton, D. P., Pan, F., & Smith, J. C. (2014a). Securing a border under asymmetric information. *Naval Research Logistics, 61*(2), 91–100.

Sullivan, K. M., Smith, J. C., & Morton, D. P. (2014b). Convex hull representation of the deterministic bipartite network interdiction problem. *Mathematical Programming, 145*(1–2), 349–376.

Tang, Y., Richard, J.-P. P., & Smith, J. C. (2016). A class of algorithms for mixed-integer bilevel min–max optimization. *Journal of Global Optimization, 66*(2), 225–262.

Towle, E., & Luedtke, J. (2018). New solution approaches for the maximum-reliability stochastic network interdiction problem. *Computational Management Science, 15*(3–4), 455–477.

Washburn, A., & Wood, R. K. (1995). Two-person zero-sum games for network interdiction. *Operations Research, 43*(2), 243–251.

Wollmer, R. D. (1964). Removing arcs from a network. *Operations Research, 12*(6), 934–940.

Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling, 17*(2), 1–18.

Wu, X., & Conejo, A. J. (2017). An efficient tri-level optimization model for electric grid defense planning. *IEEE Transactions on Power Systems, 32*(4), 2984–2994.

Xu, P., & Wang, L. (2014). An exact algorithm for the bilevel mixed integer linear programming problem under three simplifying assumptions. *Computers and Operations Research, 41*(1), 309–318.

Yuan, W., Wang, J., Qiu, F., Chen, C., Kang, C., & Zeng, B. (2016). Robust optimization-based resilient distribution network planning against natural disasters. *IEEE Transactions on Smart Grid, 7*(6), 2817–2826.

Yuan, W., Zhao, L., & Zeng, B. (2014). Optimal power grid protection through a defender–attacker–defender model. *Reliability Engineering and System Safety, 121*, 83–89.

Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid, 2*(2), 382–390.

Zeng, B., & Zhao, L. (2013). Solving two-stage robust optimization problems using a column-and-constraint generation method. *Operations Research Letters, 41*(5), 457–461.

Zenklusen, R. (2010). Matching interdiction. *Discrete Applied Mathematics, 158*(15), 1676–1690.

Zhao, L., & Zeng, B. (2013). Vulnerability analysis of power grids with line switching. *IEEE Transactions on Power Systems, 28*(3), 2727–2736.

Zheng, J., & Castañón, D. A. (2012). Dynamic network interdiction games with imperfect information and deception. In *Proceedings of the fifty-first IEEE conference on decision and control (CDC)* (pp. 7758–7763). Maui, HI: IEEE.

Zhuang, J., & Bier, V. M. (2007). Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort. *Operations Research, 55*(5), 967–991.