Network interdiction – models, applications, unexplored directions

Ricardo A. Collado Dávid Papp

April 12, 2010

Network interdiction is the monitoring or halting of an adversary's activity on a network. Its models involve two players, usually called the *interdictor* and the *evader* (or, in the more general context of Stackelberg games, *leader* and *follower*). The evader operates on the network to optimize some objective such as moving through the network as fast as possible (shortest path interdiction), or with as little probability of being detected as possible (most reliable path interdiction), or to maximize the amount of goods transported through the network (network flow interdiction). The interdictor has the capacity to change the structure or parameters of the network (remove vertices or edges, increase detection probabilities, or lower arc capacities) in order to minimize the evader's objective function.

The study of network interdiction began with military applications: disruption of the flow of enemy troops. More recent applications include infectious disease control, counter-terrorism, interception of contraband and illegal items such as drugs, weapons, or nuclear material, and the monitoring of computer networks.

A large variety of models have been proposed for different interdiction problems. These include combinatorial optimization, stochastic programming, and game theoretic approaches. In this note we attempt to collect the most researched models, match them with applications, and summarize the latest algorithmic and complexity results. In Section 1 we introduce the basic ideas and define the necessary terms. Section 2 is concerned with various models that have been proposed in the literature, as well as with algorithms and complexity bounds. In Section 3 we examine which models would be appropriate for which applications. Finally, in Section 4 we outline two promising research directions for the future.

1 Introduction

The most basic variant of the network interdiction problem is the *k-most-vital-arcs* problem: given a directed graph $G = (V, A)$ with arc lengths $\ell : A \to \mathbb{R}$, two designated vertices, s and t in V, and $k \in \mathbb{N}$, find a k-element subset A' of A such that the shortest s–t path in $(V, A \setminus A')$ is as long as possible.

The most basic variant of flow interdiction is the *maximum flow interdiction problem*: given a capacitated network $G = (V, A, s, t)$ with arc capacities $c : A \to \mathbb{R}_+$ and a budget $B > 0$, decrease the capacities of some arcs in G to minimize the maximum s–t flow in the network. The total differences of the capacities shall not exceed B.

The numerous network interdiction problems in the literature are all variations of these basic problems. The main differences are the following:

Blocking versus monitoring. A common model of network interdiction is concerned with monitoring the network. In these variants, the goal is to detect the evader's traversal of a vertex or

edge. Interdiction does not change the structure of the network, but affects the probability of detection. (For example, the evader is caught during the traversal of an interdicted edge with some fixed probability $p \in (0, 1)$, while he is caught with probability 0 if the edge is not interdicted.)

Evader models. The implicit assumption behind shortest path interdiction is that the evader would choose the shortest available path to traverse the network. This is a valid "worst-case" assumption, but is unrealistic in most applications: for example, the evader may not know the structure of the network, or may not have the resources to find the shortest path. A more general evader model is the Markovian evader, whose trajectory on the network is described by a Markov process. This is particularly appropriate for the modeling of evaders who are not aware that they are being monitored. Another important complication is the presence of multiple evaders, with different sources and targets.

Edge or vertex interdiction. Deletion of vertices can be considered instead of edge deletion. In most variants the two models are equivalent.

Directed or undirected network. Undirected graphs can also be considered. In most variants the two models are equivalent.

Deterministic or stochastic interdiction. In the stochastic variant of the shortest path interdiction problem arc deletion is stochastic: the interdiction is successful (that is, the vertex or edge is removed, or the arc capacity is lowered) with probability p. It is usually assumed that p is a known probability, and that the successes of the interdictions of the edges are independent. In this variant, the objective is to maximize the *expected* shortest path length or the expected maximum flow in the interdicted network. In the monitoring version, the probability of detection changes with interdiction, and the goal is to maximize the probability that the evader is detected before reaching her target.

Symmetry of information and objectives. In most variants the interdictor and evader are optimizing the same objective, one is minimizing, the other is maximizing. (In game theoretic terms, they are playing a zero-sum game, or a Stackelberg pricing game). However, this is not necessarily the right model in some applications. Interdictor and evader may also have different information of the network.

2 Models

2.1 Short path interdiction

Given a directed graph $G = (V, A)$ with arc lengths $\ell : A \to \mathbb{R}$ and two designated vertices, s and t in V, the goal is to destroy all short directed paths from s to t in G by eliminating some arcs of A. There are a few variants of this model.

k-most-vital arcs problem. This is one of the classical models; the objective is to delete k arcs to maximize the length of the shortest s-t path. This problem is known to be NP-hard [2], a heuristic algorithm for its solution was proposed in [14]. A polynomial-time solvable special case is the *single-most-vital arc* problem, where $k = 1$ [9]. Israeli and Wood showed a mixed integer

linear program formulation of the k-most-vital arcs problem and gave a direct and decomposition algorithms for the its solution, see [11].

Boros et al. [4] strengthened the NP-hardness results by deriving inapproximability bounds for two variants of the the problem (which they call *total limited short path interdiction*). In the original k-most-vital arcs problem the goal is to compute the maximum s–t distance $d(s,t)$ obtainable by removing at most k arcs from A. On the other hand, we might also want to compute the minimum number of arcs that have to be removed to guarantee $d(s,t) \geq d$. The first problem is NP-hard to approximate within a factor $c < 2$. The second variant is NP-hard to approximate within a factor $c < 10\sqrt{5} - 21 \approx 1.36$ even for bipartite graphs. It is also shown in [4] that the same inapproximability bounds hold for undirected graphs and node deletion instead of vertex deletion.

An altogether different approach is to formulate it as a bi-level mixed integer linear problem [11], find strong valid inequalities, and use Benders decomposition.

Node-wise limited short path interdiction. The problems above have a global budget constraint (which is what Boros et al. refer to as "total limited" interdiction). Boros, et al. [4] also considered shortest path interdiction with separate budget constraints at each vertex. They found that this version of the problem is polynomial-time solvable.

2.2 Network interdiction

In the above short(est) path interdiction models the network structure is changed to make the it more difficult for the evader (fully aware of the interdiction decisions) to reach her target. In this section we are concerned with the monitoring version of the interdiction problem. In contrast to the interdiction models described before, the interdiction decisions in these models affect the probability of being detected while traversing an edge, and the objective of the evader is to maximize the probability of reaching her target undetected by choosing what is called a *most reliable path*. An intuitive picture is that the interdictor places sensors on some edges (subject to budgetary constraints). The evader is detected with probability p_e while traversing the edge e if the edge is not interdicted. Interdiction of the edge changes this probability to $q_e \leq p_e$.

A network interdiction problem can naturally be viewed as a bi-level optimization problem [3, 21] with the higher level being a resource allocation problem for the interdictor and the lower level being a shortest path or network flow problem to be solved by the evader. These are min-max models (both players optimizing for the worst-case scenario), hence they are most appropriate when the consequence of a unsuccessful interdiction could be catastrophic (e.g., interdiction of the weapons of mass destruction).

The timing of decisions and realizations is key in this interdiction problem. First, the interdictor decisions are made, often without knowing the source and target of the evader. (It is, however, assumed that the evader samples her path according to a known probability distribution.) Then the evader's path is revealed as she selects a path to maximize the probability of avoiding detection. The evader may or may not be aware of the interdiction decisions and parameters (such as the probabilities p_e and q_e.) To date, successfully stopped nuclear smuggling attempts were detected by such methods [17]. There are a number of variants of this model.

Stochastic network interdiction, informed evader. This model only differs from the previous models in that the origin-destination pair (s,t) for the evader is initially unknown, but it is assumed to be chosen according to a known probability distribution, $p^\omega = P\{(s,t) = (s^\omega, t^\omega)\}, \omega \in \Omega$. However, in this variant of the problem the evader knows the network, detection probabilities with and without sensors, and knows the location of sensors. This problem can be formulated as a

two-stage mixed integer stochastic program. Stochastic programming problems of this form are considered very hard, but with decomposition and cut generation methods they can be solved for graphs with several hundred vertices [17].

Stochastic network interdiction, uninformed evader. In this variant the evader does not know the sensor locations, nor the detection probabilities q_e in the presence of sensors. This model requires further assumptions on the evader's behavior in the presence of multiple a priori optimal paths (i.e. *tie-breaking rules*). The problems based on this model are similar in complexity to the informed evader model [17].

Bipartite network interdiction. This is a special case of the previous two models, where each potential source-target path of the evader contains at most one arc that may be monitored. The model can be reduced to a bipartite network with arcs all going in the same direction. It can be reformulated as a deterministic mixed integer linear program, but it is still strongly NP-complete. Many families of facet defining valid inequalities are known, see [16, 17].

Unreactive Markovian evader. In this model a Markov process describes the motion of (possibly multiple) evaders who are oblivious to the interdiction actions. In the simplest version of this problem we assume unit costs and a global budget for the interdictor. The interdictor's goal is to maximize the weighted sum of the probabilities of detection (with summation over the evaders). This model was considered in [10]. It is known to be NP-hard for multiple evaders, but its complexity is still unknown for a single evader. However, it is a submodular maximization problem, and its optimal solution can be approximated within a factor of $(1 - 1/e)$ in strongly polynomial time by a greedy algorithm [10].

2.3 Maximum flow interdiction

In a third family of interdiction problems the interdictor's goal is to prevent the *flow* of some unwanted items (enemy troops, contraband items, etc.) through a capacitated network by way of reducing the capacities of network components. Given a capacitated network $N = (V, A)$ with arc capacities $c : A \to \mathbb{R}_+$ and two designated vertices, s and t in V, the goal is to reduce the size of the maximum flow from s to t in N by eliminating some arcs of A or reducing the arc capacities, subject to budgetary constraints. There are a few variants of this model.

Maximum flow network interdiction. In this most basic variant, arcs of N are removed (at given costs) while being constrained by a global budget. Even the special case where the cost of arc removal is the same for each arc is known to be strongly NP-hard. It admits a very simple integer programming formulation [23]. A number of valid inequalities are known this IP, but the integrality gap is still large [1]. The approximability of this problem is still unknown, with no positive or negative results in the literature.

Stochastic maximum flow network interdiction. In this model the interdiction of each arc is successful with some probability $p < 1$. The objective is to minimize the *expected maximum flow*. These models use multi-stage stochastic integer linear programming [12] and the most efficient ones have no integer recourse variables. (Multi-stage stochastic integer programming with integer recourse variables are considered practically intractable even for modest problem sizes.) Large problems with grid-like structures are reported to have been solved, see [12].

Stackelberg games. Each of the above models can be considered as a special case of *Stackelberg games* [22]. These are two-step, two-player sequential games, in which *leader* and *follower* play sequentially (one step each) and receive payoffs. The game is zero-sum (the players compete to maximize and minimize, resp., the same quantity). The above interdiction problems are special cases, when the payoff is the shortest path, most reliable path, or maximum flow. Possible strategies for leader are determined by the budget constraints. Stackelberg games have traditionally been used in econometrics, but their application to network interdiction is much less explored. This line of research does not seem particularly promising, as Stackelberg games corresponding to most basic combinatorial problems (shortest path, minimum spanning tree) are known to be APX-hard [13, 6].

Recently, Briest and Khanna considered the following *shortest path pricing game* [5]: Given a directed network with source s, target t, and arc lengths $c(e)$, $e \in E$, and a subset of the arcs P called *priceable*, Leader may assign prices $p(e)$ to the priceable arcs $e \in P$. Follower then chooses a shortest $s-t$ path P^* with respect to the new cost structure $c+p$, and Leader receives revenue $\sum_{e \in P^*} p(e)$. This problem is also known to be APX-hard. As it is shown in [5], it also cannot be approximated in polynomial time within a factor of $2 - 2^{-\Omega(\log^{1-\epsilon} m)}$ (for every $\epsilon > 0$) unless NP $\subseteq$ DTIME($n^{O(\log n)}$).

3 Applications

Road blocks, interception of known criminals. In the interception of evaders with known sources (such as suspects fleeing a crime scene) on a small network (local road network) the evader can be assumed to know or at least approximately know the shortest paths. Hence deterministic or stochastic shortest path models with a global budget constraint seems appropriate. While these problems are NP-hard, they should not raise computational difficulty, as the network size is reasonably small.

In the case of larger networks, involving multiple cities or states, the use of node-wise limited budgets is also justified. (Polynomial-time solvable case.)

Counter-terrorism. A considerably different problem is the interception of terrorists. This is a problem with multiple evaders of unknown sources. Note that data collection for this problem is also considerably more difficult. This problem has several facets, some of which are not best modeled as an interdiction problem. For example in the problem of airport security the network and its monitoring are rather simple, from the interdiction point of view. (It is given where all monitoring takes place.) The key element in this problem is the identification of potential adversaries by selecting *which actors* (rather than which arcs) are subjected to different levels of monitoring.

The coordination of airport security efforts, however, can be viewed as an interdiction problem (with flights or connections as arcs) with node-wise budgets. Interdiction of nuclear smuggling is discussed below.

Border control, smuggling and immigration. The key specialty of interdiction models for border control is that the network can be assumed to be bipartite, and each evader traverses precisely one edge on which it can be intercepted. The various applications differ mainly in their objectives.

In the case of nuclear smuggling the risk associated with non-detection is extremely high, and hence a worst-case approach is justified. The amount of flow is too little to warrant a maximum

flow approach; instead, a most reliable path approach should be used. Again, modeling must take into consideration that data collection for this problem is also very difficult.

In the case of smuggling contraband items and drugs, maximum flow interdiction models and a more risk-neutral approach are justified. Hence deterministic or stochastic maximum flow interdiction (with the goal of minimizing the expected maximum flow) is appropriate.

Interception of illegal immigrants can be modeled identically to the smuggling problems above, but it is also a situation where asymmetric models might be useful. It is very likely that the evader does not have full information about the network, and the utility (resp., disutility) of the detection of a single evader is considerably different for the (risk-neutral) interdictor and the (extremely risk-averse) evader.

Infectious disease control. Infectious disease control is another problem that has been widely researched, and generally may not be best modeled as an interdiction problem, as infections are generally not prevented by the disruption of the (social or other) network. However, curbing the spread of an infectious disease can be modeled as an interdiction problem if the disease is severe and can result in a pandemic. Examples include the monitoring of airport passengers for swine flu, setting up quarantines, and culling all cattle populations suspected to carry bovine spongiform encephalopathy.

4 Open questions

4.1 Approximability bounds

Almost all considered models are known to be NP-hard, however, less is known about their approximability. Recent results in the theory of Stackelberg games [5, 6, 13] suggest that most of the above models are in fact APX-hard. Inapproximability bounds with a constant factor are only known for shortest path interdiction problems, but not for network flow interdiction.

4.2 Risk-averse stochastic programming

The shortest path interdiction model has the disadvantage that it assumes an optimal evader, or equivalently an extremely risk-averse interdictor. On the other hand, the objective in the above stochastic models is to maximize the expected cost of the evader, which is the other extreme: the risk-neutral approach. A possible approach to model an interdictor that is neither extremely risk-averse nor risk-neutral is to change the objective function in the above stochastic programming models to *coherent risk measures* of the shortest path length, maximum flow, etc.

Coherent risk measures are, in effect, utility functions with theoretical properties that allow both the flexible modeling of risk-averse actors and the efficient solution of the resulting mathematical models. The use of coherent risk measures in stochastic programming is a relatively recent development, but there already are useful computational methods that allow the practically efficient solution of these models, see for example [20, 15, 18, 19, 7], and recently these approaches have been extended to two-stage problems as well [8]. Recently the authors of this report have developed some preliminary models of interdiction based on the theory of coherent risk measures but more research needs to be done on the subject.

References

[1] Douglas S. Altner, Özlem Ergun, and Nelson A. Uhan, *The maximum flow network interdiction problem: Valid inequalities, integrality gaps, and approximability*, Operations Research Letters **38** (2010), 33–38.

[2] Michael O. Ball, Bruce L. Golden, and Rakesh V. Vohra, *Finding the most vital arcs in a network*, Operations Research Letters **8** (1989), no. 2, 73–76.

[3] J.F. Bard, Kluwer Academic Publishers, Dordrecht.

[4] Endre Boros, Konrad Borys, Khaled Elbassioni, Vladimir Gurvich, Leonid Khachiyan, Gabor Rudolf, and Jihui Zhao, *On short paths interdiction problems: Total and node-wise limited interdiction*, Theory of Computing Systems **43** (2008), no. 2, 204–233.

[5] Patrick Briest and Sanjeev Khanna, *Improved hardness of approximation for Stackelberg shortest-path pricing*, Tech. Report CoRR abs/0904.2400, 2009.

[6] Jean Cardinal, Erik D. Demaine, Samuel Fiorini, Gwenaël Joret, Stefan Langerman, Ilan Newman, and Oren Weimann, *The stackelberg minimum spanning tree game*, Algorithmica (accepted).

[7] Sungyong Choi and Andrzej Ruszczyński, *A risk-averse newsvendor with law invariant coherent measures of risk*, Oper. Res. Lett. **36** (2008), no. 1, 77–82.

[8] Ricardo A. Collado, Dávid Papp, and Andrzej Ruszczyński, *Scenario decomposition of risk-averse multistage stochastic programming problems*, in preparation.

[9] H.W. Corely and D.Y. Shaw, *Most vital links and nodes in weighted networks*, Operations Research Letters **1** (1982), 157–160.

[10] Alexander Gutfraind, Aric Hagberg, and Feng Pan, *Optimal interdiction of unreactive markovian evaders*, Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems (Willem-Jan van Hoeve and John N. Hooker, eds.), Lecture Notes in Computer Science, vol. 5547, Springer, Berlin/Heidelberg, 2009, pp. 102–116.

[11] Eitan Israeli and R. Kevin Wood, *Shortest-path network interdiction*, Networks **40** (2002), 97–111.

[12] Udom Janjarassuk and Jeff Linderoth, *Reformulation and sampling to solve a stochastic network interdiction problem*, Networks **52** (2008), no. 3, 120–132.

[13] Gwenaël Joret, *Stackelberg network pricing is hard to approximate*, Networks (accepted).

[14] K. Malik, A.K. Mittal, and S.K. Gupta, *The k most vital arcs in the shortest path problem*, Operations Research Letters **8** (1989), 223–227.

[15] Naomi Miller and Andrzej Ruszczyński, *Risk-adjusted probability measures in portfolio optimization with coherent measures of risk*, European J. Oper. Res. **191** (2008), no. 1, 193–206.

[16] F. Pan, W. Charlton, and D.P. Morton, *Stochastic network interdiction of nuclear material smuggling*, In D.L. Woodruff, editor, *Network Interdiction and Stochastic Integer Programming* (2002), 1–19.

[17] Feng Pan, *Stochastic network interdiction: Models and methods*, Ph.D. thesis, University of Texas at Austin, May 2005.

[18] Andrzej Ruszczyński and Alexander Shapiro, *Conditional risk mappings*, Math. Oper. Res. **31** (2006), no. 3, 544–561.

[19] ———, *Corrigendum to: "optimization of convex risk functions," mathematics of operations research 31 (2006) 433–452*, Math. Oper. Res. **32** (2007), no. 2, 496–496.

[20] Alexander Shapiro, Darinka Dentcheva, and Andrzej Ruszczyński, *Lectures on stochastic programming: Modeling and theory*, MPS-SIAM series on optimization, no. 9, MPS-SIAM, Philadelphia, 2009.

[21] K. Shimizu, Y. Ishizuka, and J.F. Bard, *Nondifferentiable and two-level mathematical programming*, Kluwer Academic Publishers, 1997.

[22] Heinrich Freiherr von Stackelberg, *Marktform und Gleichgewicht (Market Structure and Equilibrium)*, Vienna, 1934.

[23] R. Kevin Wood, *Deterministic network interdiction*, Mathematical and Computer Modelling **17** (1993), no. 2, 1–18.