National Research University Higher School of Economics

as a manuscript

Ketkov Sergei Sergeevich

ANALYSIS OF THE SHORTEST PATH PROBLEM WITH INCOMPLETE INFORMATION AND LEARNING

PhD Dissertation Summary

for the purpose of obtaining academic degree
Doctor of Philosophy in Computer Science

Nizhny Novgorod - 2022

The PhD dissertation was prepared at National Research University Higher School of Economics in the Laboratory of Algorithms and Technologies for Network Analysis.

Academic supervisors:

– Kalyagin Valery Alexandrovich, professor, HSE university, Nizhny Novgorod, Russia;

– Prokopyev Oleg Alexandrovich, professor, university of Pittsburgh, USA.

Contents

1 Introduction

1.1 Dissertation topic and its relevance.

In this thesis we consider one- and multi-stage formulations of the shortest path problem (SPP), where either the arc costs/travel times or the structure of the network is subject to uncertainty. More specifically, we consider the following two alternative problem settings:

- **Model I:** the structure of the network is known to the decision-maker a priori but the arc costs/travel times are subject to uncertainty.
- **Model II:** the arc/costs travel times in a given network are deterministic but the structure of the network (e.g., the existence of some arcs along with their costs) is subject to uncertainty.

In both cases we formulate the problem as a dynamic or repetitive zero-sum game between two decision-makers, namely, a *user* and an *attacker*. The user traverses between two fixed nodes in a given network, whereas the attacker controls in some predefined way the arc costs or their probability distribution. One of the decision-makers has incomplete information about either the distribution of arc costs and/or the structure of the network and attempts to learn some additional information by repetitive interactions with the other decision-maker.

With respect to the first model, Model I, it can be argued that uncertainty in arc travel times may arise due to road capacity variation or traffic conditions. Furthermore, in a number of practical applications the arc costs/travel times in a given network are only observable through a finite training data set [1]. As a result, the uncertainty in arc travel times may influence the structure and quality of routing decisions; see, e.g., [2].

The first question arising in the context of Model I is how to transform the available historical data to a decision of the underlying network optimization problem. For example, this problem can be addressed with a *distributionally robust optimization (DRO)* approach, where the distribution of arc travel

times is described by an *ambiguity set* or a *family* of distributions that are consistent with the available data; see, e.g., the related studies in [3, 4, 5, 6]. Given some family of admissible distributions, the decision-maker is supposed to optimize a measure of risk under the worst-case possible distribution of the uncertain parameters. Put differently, the idea of DRO approach is to find a compromise between the lack of distributional information (as in robust optimization [7, 8]) and complete knowledge of the underlying probability distribution (as in stochastic programming [9]).

The second question arising is whether the data can be collected by the user dynamically while traversing through the network. In this regard, we consider a multi-stage version of the shortest path problem, where some information about the distribution of arc travel times can be refined at particular nodes of the user's path. In other words, in contrast to the one-stage model, in the considered multi-stage problem setting both the user and the attacker are able to adjust their decisions dynamically. Our results for Model I can be found in [10] and [11] (the second work is an unpublished preprint).

With respect to the second model, Model II, we focus on a class of network interdiction problems, where the user traverses in the network (e.g., between two fixed nodes, a source and a destination), while the attacker aims to disrupt to the maximum possible extent (or completely stop) the user's movement through the network. The key feature of our model is that the attacker has incomplete initial information about the network including its structure and costs but learns this information by observing the user's actions (i.e., the user's path) in each decision epoch. Furthermore, in contrast to the related studies in [12, 13], we consider the user's perspective.

The learning component in Model II can be motivated by practical settings, where the attacker can observe the user's actions (for example, by using a satellite or a drone), but cannot immediately react upon those actions; see, e.g., [14]. In particular, we assume that this information feedback is deterministic and perfect, that is, the attacker learns about the existence and the exact costs of the arcs traversed by the user in the previous decision epochs.

As for Model I, Model II can be considered both in one- and multi-stage problem settings. For a single decision epoch the problem can be viewed as a shortest path interdiction problem; see, e.g., [15], where the attacker attempts to maximize the cost of user's shortest path subject to some budgetary constraints. In the multi-stage model, the attacker may potentially update its information about the structure and the costs in the network by observing the user's path. For this reason, we consider a repeated interaction between the user and the attacker, where the user attempts to minimize its cumulative loss over multiple decision epochs. Our results for Model II can be found in [16].

1.2 Related literature

With respect to Model I, several studies consider one-stage versions of the *distributionally robust shortest path problem* (DRSPP); see, e.g., [1, 17, 18, 19]. Specifically, the authors consider different forms of ambiguity sets including moment-based ambiguity sets [18, 19] and ambiguity sets based on a distance metric from the empirical distribution of the data [1].

Typically, in a one-stage DRSPP the user picks a path *here-and-now*, before the realization of uncertainty. Therefore, the problem can be viewed as a min-max problem, where the user attempts to minimize its expected loss under the worst-case distribution of arc travel times. Most recent solution approaches to the resulting bi-level problems rely on the duality results for moment problems [20, 21]. That is, under some assumptions on the geometry of ambiguity sets and functional properties of the objective function, the one-stage DRSPP can be recast as either linear or non-linear mixed-integer programming (MIP) problem.

It has been also shown that DRO may address *dynamic* or, equivalently, *multi-stage* optimization problems, where the decisions adapt to the uncertain outcomes as they unfold in stages; see, e.g., [5, 6, 22, 23]. In general, multi-stage DRO problems are computationally intractable since the *recourse decisions* (i.e., the decisions affected by uncertainty) can be modeled as arbitrary functions of the uncertain parameters [21, 24]. To the best of our knowledge, the multi-stage DRSPP is considered by relatively few authors and there are only studies that

may account the shortest path problem as a special case; see, e.g., [22, 25].

In conclusion, we would like to refer to a multi-stage shortest path interdiction model proposed by Sefair et al. [26] and a multi-stage robust MIP problem formulation of Bertsimas and Dunning [27]. Despite the fact that these models are deterministic, they provide some interesting insights for the multi-stage DRSPP considered in the current thesis.

Specifically, in [26] the attacker can block a subset of arcs any time the user reaches a node in the network. After that, the user can respond by dynamically altering its path. Naturally, the problem unfolds in a number of stages, where at each stage the attacker blocks a subset of arcs emanated from the current user's position and the user picks a subsequent node of its path. Furthermore, the total number of arcs that can be blocked by the attacker is bounded from above by the attacker's budget. In this thesis, similar to the problem setting in [26], we introduce some *auxiliary distributional constraints* associated with the arcs emanated from the current user's position.

In the model of Bertsimas and Duning [27] the uncertain problem parameters are only known to reside within a polyhedral uncertainty set. The uncertainty set is partitioned into a number of disjoint polyhedrons and the recourse decisions are assumed to be piecewise constant functions on the generated subsets. This modeling approach enables to obtain approximations of the multi-stage problem, where the quality of approximation is adjusted by the choice of an appropriate partition scheme. In the following, we demonstrate that in our multi-stage formulation of the shortest path problem a similar piecewise constant construction of decision rules arises naturally due to auxiliary distributional constraints observed by the user while traversing through the network.

With respect to Model II, network interdiction forms a broad class of deterministic and stochastic optimization problems with applications mostly arising in the military, law-enforcement and infectious disease control contexts, see the surveys in [28, 29, 30, 31, 32] and the references therein. The network interdiction problems mostly focus on the attacker's perspective. In other words, the attacker is usually viewed as a leader, while the user plays as a follower in the

considered game.

While most of the network interdiction literature consider deterministic settings, a number of more recent works consider the network interdiction problem in stochastic settings; see, e.g., [33, 34] and the survey in [35]. Typically such models assume that either the outcomes of attacker's actions are uncertain or there is uncertainty with respect to the user's actions.

Our multi-stage network interdiction model is motivated and builds upon the recent works of Borrero et al. in [12, 13]. Specifically, in the network model in [12] the attacker and the user interact sequentially over multiple decision epochs (or rounds). In each decision epoch, the attacker can block at most k arcs for the duration of the current decision epoch, while the user is assumed to be greedy, i.e., in each round it traverses along the shortest path between two fixed nodes in the interdicted network. By observing the user's decisions, the attacker is able to update its information about the structure of the network and the cost of arcs traversed by the user.

The authors in [12] show that *greedy attacker's policies* have a number of attractive theoretical properties in the aforementioned multi-stage problem setting. In addition to these properties, the results of computational experiments in [12] also confirm the superiority of greedy attacker's policies against several other benchmark policies. Finally, in [13] the authors generalize the theoretical results and greedy policies from [12] to a more general class of max-min linear mixed-integer programming problems.

1.3 Our approach and contributions

Model I. Similar to the study of Wiesemann et al. [4], we assume that the family of admissible distributions in our setting is described by some first-order moment constraints with respect to subsets of arcs and individual probability constraints for particular arcs. We argue that in contrast to the moment-based ambiguity sets [3] or ambiguity sets based on a distance metric from the empirical distribution [36, 37], our distributional constraints allow incomplete knowledge of the training data set. Our contributions for the *one-stage* DRSPP can

be summarized as follows:

- We demonstrate that our distributional constraints can be constructed in a unified way from real-data observations.
- We show that the problem without the first-order moment constraints is polynomially solvable and identify a closed form of the worst-case distribution in this particular case.
- In the general case and in contrast to the studies in [18, 19], we obtain robust and linear mixed-integer programming (MIP) reformulations of the one-stage DRSPP.
- We conduct a numerical study of the proposed approach and provide a comparison with some standard robust and distributionally robust optimization techniques.

In the *multi-stage* formulation of DRSPP we attempt to address the following research questions:

Q1. *Is there a benefit for the user to alter the chosen path, if it observes some additional distributional information while traversing through the network?*

Q2. *How much can the user gain by leveraging such adaptive decisions?*

Q3. *Can the resulting multi-stage formulation be solved at hand using off-the-shelf MIP solvers?*

We attempt to address a dynamic revelation of distributional information to the user by introducing some *auxiliary distributional constraints* the can be verified at particular nodes of the user's path. Simply speaking, the user forms a list of auxiliary constraints *at the beginning of the game*. Then for each constraint in the list the attacker decides whether it is satisfied or not and reveals its response, i.e., "yes" or "no", to the user as soon as the user achieves the respective node in the network.

Our contributions for the multi-stage model can be summarized as follows:

- We describe two classes of non-anticipativity constraints for the multi-stage DRSPP, for acyclic and general graphs, respectively. These constraints certify that the user's decision at a current stage cannot depend on future attacker's responses.

- Under some mild assumptions we reformulate the multi-stage DRSPP as a one potentially large linear MIP problem. These results address our research question **Q3**.

- The obtained MIP reformulation is used in our numerical study, where its computational tractability and the quality of adaptive decisions is explored numerically. Hence, we address the research questions **Q1** and **Q2**.

- From the practical perspective, we demonstrate that the auxiliary constraints can be verified in an online manner using information from Bluetooth sensors placed at particular nodes of the network.

Model II. In contrast to Model I, we assume that the arc costs/travel times in Model II are deterministic, but the attacker has incomplete information about the network structure and costs. By observing the paths traversed by the user, the attacker may learn about the existence and precise costs of particular arcs and adjust its decisions in the subsequent decision epochs.

As outlined earlier, the studies in [12, 13], similar to the vast majority of the related interdiction literature, focus on the attacker's perspective. However, taking into account a number of attractive theoretical properties of greedy attacker's policies, it seems to be interesting to explore optimal user's policies assuming that the attacker follows a myopic greedy policy in each decision epoch. Formally, we introduce the following research questions:

Q1'. If we assume that the attacker is greedy, what are good strategic policies for the user against the outlined greedy attacker's policy?

Q2'. Do such policies have any interesting structural properties and how can they be constructed?

Q3'. Are these policies more preferable for the user than a myopic shortest-path based greedy policy?

Our contributions for Model II can be summarized as follows:

- We show that the user's problem is NP-hard even in the case of two decision epochs. This result is established for networks where the k-most vital arcs problem is polynomially solvable.
- We demonstrate that under some additional assumption an optimal user's decision in the case of two decision epochs is either greedy or consists of two distinct paths that intersect with the overall shortest path. Therefore, we address the research questions **Q1'** and **Q2'**.
- The outlined theoretical properties are used to develop a heuristic algorithm for the user in a more general setting.
- The obtained computational results demonstrate superiority of the proposed heuristic approach against a myopic greedy policy for several classes of synthetic network instances and types of feedback obtained by the attacker. Therefore, we address the research question **Q3'**.

1.4 Publications and approbation of the research

The results of this work are published in a range of scientific papers in international peer-reviewed journals.

First-tier publications:

- Sergey S. Ketkov, Oleg A. Prokopyev, On Greedy and Strategic Evaders in Sequential Interdiction Settings with Incomplete Information, *Omega*, 92, 102161 (2020), **Q1**;
- Sergey S. Ketkov, Oleg A. Prokopyev, Evgenii P. Burashnikov, An approach to the distributionally robust shortest path problem, *Computers & Operations Research*, 130, 105212 (2021), **Q2**.

Other publications (optional):

- Sergey S. Ketkov, On the multi-stage shortest path problem under distributional uncertainty, *arXiv preprint* arXiv:2205.09200 (2022).

Personal contribution of the author of the dissertation. The author of the dissertation carried out the proof of the main theoretical results, data collection, experiments, analyzed and interpreted the results of experiments, wrote the text. In the first and the second studies, the scientific supervisor, O.A. Prokopyev, provided some ideas concerning problem formulations, assistance in editing the text and responses to the comments of reviewers. The co-author of the second work, E.P. Burashnikov, investigated the ideas of some experiments and provided comments that helped improve the quality of the work.

Reports at conferences and seminars (optional):

- Mathematical Optimization Theory and Operations Research, Novosibirsk, $6-10$ July 2020, an oral presentation "An approach to the distributionally robust shortest path problem";

- Mathematical Optimization Theory and Operations Research, Irkutsk, $4-10$ July 2021, an oral presentation "On a class of data-driven combinatorial optimization problems under uncertainty: a distributionally robust approach";

- Scientific seminar of Laboratory of algorithms and technologies for network analysis, 29.04.2020, an oral presentation "On the multi-stage distributionally robust shortest path problem";

- The 12th International Conference on Network Analysis NET 2022, $23-25$ May 2022, an oral presentation "On the multi-stage shortest path problem under distributional uncertainty";

- The 7th International Conference on Network Analysis, Nizhny Novgorod, May 2017, an oral presentation "Evader's models in sequential network interdiction";

- Modern Problems in Mathematics and its Applications, Yekaterinburg, $4-10$ February 2018, an oral presentation: "On a Strategic Evader in Sequential Interdiction with Incomplete Information".

2 Model I: problem formulation and solution approach

Notation. All vectors and matrices are labeled by bold letters. For a network $G := (N, A, \mathbf{c})$ we denote by N and A its sets of nodes and directed arcs, respectively, whereas $\mathbf{c}$ is a nonnegative cost vector. For each node $i \in N$ we refer to RS_i (FS_i) as the set of arcs directed out of (and into) node i. Let s and f be a source and a destination node, respectively; also, let $\mathcal{P}_{sf}(G)$ be a set of all simple directed paths from s to f in the network G. Any path $P \in \mathcal{P}_{sf}(G)$ is given by a sequence of arcs (s, v_1),(v_1, v_2),...,$(v_{|P|-1}, f)$, which we introduce as $\{s \to v_1 \to \ldots \to v_{|P|-1} \to t\}$ for convenience.

The space of all probability distributions on $\mathbb{R}^m$ for some $m \in \mathbb{Z}_{>0}$ is denoted as $\mathcal{Q}_0(\mathbb{R}^m)$. For each $a \in A$ we denote by $\mathbb{Q}_a \in \mathcal{Q}_0(\mathbb{R})$ the marginal distributions induced by some joint probability distribution $\mathbb{Q} \in \mathcal{Q}_0(\mathbb{R}^{|A|})$.

2.1 One-stage problem

We consider a directed weighted connected graph $G := (N, A, \mathbf{c})$, where a set of all feasible path-incidence vectors is given by:

$$Y = \Bigg\{ \mathbf{y} \in \{0,1\}^{|A|} : \sum_{a \in FS_i} y_a - \sum_{a \in RS_i} y_a = \begin{cases} 1, \text{ if } i = s \\ -1 \text{ if } i = f \\ 0, \text{ otherwise} \end{cases} \quad \forall i \in N \tag{1a}$$

$$\sum_{a \in FS_i} y_a \leq 1 \quad \forall i \in N \Bigg\} \tag{1b}$$

The constraints (1a) are standard flow conservation constraints, whereas the constraints (1b) ensure that each node is visited by the user at most once. As the cost vector is nonnegative by construction, the latter condition is of interest only for the multi-stage DRSPP; see our assumption **A5** in Section 2.2.

We assume that the user has the following partial information about the distribution $\mathbb{Q}$ of the cost vector $\mathbf{c}$. First, the costs of particular arcs $a \in A$ are subject to *individual probability constraints* of the form:

$$\mathbb{Q}\{c_a \in [l_a^{(j)}, u_a^{(j)}]\} \in [\underline{q}_a^{(j)}, \overline{q}_a^{(j)}] \quad \forall j \in \mathcal{D}_a,\ a \in A, \tag{2}$$

where $[l_a^{(j)}, u_a^{(j)}] \subseteq [l_a, u_a]$, $j \in \mathcal{D}_a = \{1, \ldots, d_a\}$, is a finite set of subintervals; $\underline{q}_a^{(j)}$ and $\overline{q}_a^{(j)}$ are contained in $[0, 1]$ and bound the probability that the random cost c_a belongs to the i-th subinterval. In particular, we assume that for each $a \in A$ and $j = 1$ the constraints

$$\mathbb{Q}\{c_a \in [l_a^{(j)}, u_a^{(j)}]\} \in [\underline{q}_a^{(j)}, \overline{q}_a^{(j)}]$$

are support constraints with $l_a^{(j)} = l_a$, $u_a^{(j)} = u_a$ and $\underline{q}_a^{(j)} = \overline{q}_a^{(j)} = 1$ for some $l_a, u_a \in \mathbb{R}_{>0} \cup \{0\}$.

Finally, for a real-valued matrix $\mathbf{B} \in \mathbb{R}^{|A| \times k}$ and a vector $\mathbf{b} \in \mathbb{R}^k$, $k \in \mathbb{Z}_+$, we introduce *linear expectation constraints* of the form:

$$\mathbb{E}_{\mathbb{Q}}\{\mathbf{B}\mathbf{c}\} \leq \mathbf{b} \tag{3}$$

Thus, the distribution $\mathbb{Q}$ of the cost vector $\mathbf{c}$ is assumed to belong to an ambiguity set $\mathcal{Q}$ formed by all distributions that satisfy the distributional constraints (2) and (3), i.e.,

$$\mathcal{Q} := \Big\{\mathbb{Q} \in \mathcal{Q}_0(\mathbb{R}^{|A|}) :\ \mathbb{Q} \text{ satisfies the constraints (2) and (3)}\Big\} \tag{4}$$

By introducing a linear loss function $\ell(\mathbf{c}, \mathbf{y}) := \mathbf{c}^\top \mathbf{y}$ we derive a one-stage

or static version of DRSPP:

$$z^*_{static} := \min_{\mathbf{y}\in Y} \max_{\mathbb{Q}\in\mathcal{Q}} \mathbb{E}_{\mathbb{Q}}\{\mathbf{c}^\top \mathbf{y}\}, \qquad (\mathbf{F}_{os})$$

where the set of feasible decisions Y and the ambiguity set $\mathcal{Q}$ are given by the equations (1) and (4), respectively.

In addition, we make the following assumptions:

A1. Both the user and the attacker have complete information about the initial family of distributions $\mathcal{Q}$ and the structure of network G.

A2. For each $a \in A$ there exists a marginal distribution $\mathbb{Q}_a \in \mathcal{Q}_0(\mathbb{R})$ such that

$$\mathbb{Q}_a\{l_a^{(i)} \le c_a \le u_a^{(i)}\} \in (\underline{q}_a^{(i)}, \overline{q}_a^{(i)}),$$

whenever $\underline{q}_a^{(i)} < \overline{q}_a^{(i)}$, $i \in \mathcal{D}_a$.

A3. For each $a \in A$ and any pair of subintervals in (2), namely, $[l_a^{(i_1)}, u_a^{(i_1)}]$ and $[l_a^{(i_2)}, u_a^{(i_2)}]$, $i_1, i_2 \in \mathcal{D}_a$, we have $l_a^{(i_1)} \neq u_a^{(i_2)}$ and $l_a^{(i_2)} \neq u_a^{(i_1)}$.

In Assumption **A1** we envision that the user has some initial information about the distribution of arc costs. For example, this information can be collected beforehand by leveraging some historical data. Assumption **A2** coincides with the related assumption made by Wiesemann et al. [4] and serves as a constraint qualification condition for moment problems [21]. Finally, Assumption **A3** stipulates that the inner optimization problem in $(\mathbf{F}_{os})$ has a finite maximum. It can also be argued that Assumption **A3** is rather technical since, if, e.g., $l_a^{(i_1)} = u_a^{(i_2)}$ for some $i_1, i_2 \in \mathcal{D}_a$, then a sufficiently small perturbation of the endpoints makes this assumption satisfied.

At first, we examine the one-stage formulation $(\mathbf{F}_{os})$ without linear expectation constraints (3), i.e.,

$$\min_{\mathbf{y}\in Y} \max_{\mathbb{Q}\in\widetilde{\mathcal{Q}}} \mathbb{E}_{\mathbb{Q}}\{\mathbf{c}^\top \mathbf{y}\}, \qquad (\mathbf{F}'_{os})$$

where

$$\widetilde{\mathcal{Q}}_a := \left\{ \mathbb{Q}_a \in \mathcal{Q}_0(\mathbb{R}) \colon \mathbb{Q}_a\{c_a \in [l_a^{(i)}, u_a^{(i)}]\} \in [\underline{q}_a^{(i)}, \overline{q}_a^{(i)}] \quad \forall i \in \mathcal{D}_a \right\}$$

and

$$\widetilde{\mathcal{Q}} := \left\{ \mathbb{Q} \in \mathcal{Q}_0(\mathbb{R}^{|A|}) : \mathbb{Q}_a \in \widetilde{\mathcal{Q}}_a \right\} \tag{5}$$

We prove that the resulting problem can be tackled by solving a particular linear programming problem for each $a \in A$ and a single deterministic shortest path problem.

For simplicity of our further exposition we need the following preprocessing step. For each arc $a \in A$ from the *baseline* set $[l_a^{(i)}, u_a^{(i)}]$, $i \in \mathcal{D}_a$, of subintervals we form a set $[L_a^{(j)}, U_a^{(j)}]$, $j \in \mathcal{W}_a := \{1, \dots W_a\}$, of $W_a \in \mathbb{Z}_+$ *elementary subintervals* [38]. Specifically, we consider a list of distinct interval endpoints, that is,

$$\{l_a^{(1)}, u_a^{(1)}, l_a^{(2)}, u_a^{(2)}, \dots l_a^{(D_a)} = l_a, u_a^{(D_a)} = u_a\}$$

and sort them in a nondecreasing order. Regions of the resulting partitioning of the interval $[l_a, u_a]$ are referred to as elementary subintervals and denoted by $[L_a^{(j)}, U_a^{(j)}]$, $j \in \mathcal{W}_a$. For any $i \in \mathcal{D}_a$ we denote by $\mathcal{W}_a(i) \subseteq \mathcal{W}_a$ the indices of elementary subintervals contained in the baseline subinterval $[l_a^{(i)}, u_a^{(i)}]$.

Theorem 1 *Suppose that* $\mathbf{y}^* \in Y$ *and* $\mathbb{Q}^{(w)} \in \mathcal{Q}_0(\mathbb{R}^{|A|})$ *is an optimal solution of* $(\mathbf{F}'_{os})$. *Then*

- *for each* $a \in A$ *the worst-case expected cost* $\mathbb{E}_{\mathbb{Q}_a^{(w)}}\{c_a\}$ *coincides with an optimal objective function value of the following linear programming problem:*

$$\max_{\boldsymbol{\delta}_a} \sum_{j \in \mathcal{W}_a} U_a^{(j)} \delta_{aj} \tag{6a}$$

$$\text{s.t. } \delta_{aj} \geq 0 \quad \forall j \in \mathcal{W}_a \tag{6b}$$

$$\sum_{j \in \mathcal{W}_a} \delta_{aj} = 1 \tag{6c}$$

$$\underline{q}_a^{(i)} \leq \sum_{j \in \mathcal{W}_a(i)} \delta_{aj} \leq \overline{q}_a^{(i)}, \quad \forall i \in \mathcal{D}_a \setminus \{1\} \tag{6d}$$

- *an optimal path-incidence vector* $\mathbf{y}^*$ *can be attained by solving a deterministic shortest path problem of the form:*

$$\min_{\mathbf{y} \in Y} \sum_{a \in A} \mathbb{E}_{\mathbb{Q}_a^{(w)}}\{c_a\} y_a \tag{7}$$

The idea of the proof of Theorem 1 is to consider the worst-case expected costs for each particular arc $a \in A$ and then to reformulate the resulting moment problems by using strong duality [21] and some basic properties of the elementary subintervals.

Next, we consider a general one-stage DRSPP ($\mathbf{F}_{os}$) with both probability constraints (2) and linear expectation constraints (3). It turns out that the DRSPP ($\mathbf{F}_{os}$) can be recast as a robust shortest path problem with some polyhedral uncertainty set. More specifically, the following result holds.

Theorem 2 *Assume that*

$$\mathcal{S}_0 := \{\overline{\mathbf{c}} \in \mathbb{R}^{|A|} : \ \mathbf{L} \leq \overline{\mathbf{c}} \leq \mathbf{U}; \quad \mathbf{B}\overline{\mathbf{c}} \leq \mathbf{b}\},$$

where for each $a \in A$

$$L_a := \min_{\mathbb{Q}_a \in \widetilde{\mathcal{Q}}_a} \mathbb{E}_{\mathbb{Q}_a}\{c_a\}, \tag{8a}$$

$$U_a := \max_{\mathbb{Q}_a \in \widetilde{\mathcal{Q}}_a} \mathbb{E}_{\mathbb{Q}_a}\{c_a\}, \tag{8b}$$

and

$$\widetilde{\mathcal{Q}}_a := \left\{\mathbb{Q}_a \in \mathcal{Q}_0(\mathbb{R})\colon \mathbb{Q}_a\{c_a \in [l_a^{(i)}, u_a^{(i)}]\} \in [\underline{q}_a^{(i)}, \overline{q}_a^{(i)}] \quad \forall i \in \mathcal{D}_a\right\}$$

Then the distributionally robust shortest path problem of the form ($\boldsymbol{F}_{os}$) *is equiv-*

alent to the following robust shortest path problem with polyhedral uncertainty:

$$\min_{\mathbf{y}\in Y} \max_{\overline{\mathbf{c}}\in\mathcal{S}_0} \overline{\mathbf{c}}^{\top}\mathbf{y} \tag{9}$$

In fact, we prove that for each $a \in A$ there exists a *surjective mapping* from the set of marginal probability distributions $\widetilde{\mathcal{Q}}_a$ given by equation (5) onto a set formed by linear expectation constraints

$$L_a \leq \mathbb{E}_{\mathbb{Q}_a}\{c_a\} \leq U_a \tag{10}$$

Also, in view of Theorem 2, we may recast the one-stage problem ($\mathbf{F}_{os}$) as a linear MIP problem by dualizing the second-level linear programming problem in (9). Formally, the following corollary holds.

Proposition 1 *Let*

$$\mathcal{S}_0 := \left\{\overline{\mathbf{c}} \in \mathbb{R}^{|A|} :\ \mathbf{L} \leq \overline{\mathbf{c}} \leq \mathbf{U};\quad \mathbf{B}\overline{\mathbf{c}} \leq \mathbf{b}\right\} = \left\{\overline{\mathbf{c}} \in \mathbb{R}^{|A|} :\ \mathbf{B}_0\overline{\mathbf{c}} \leq \mathbf{b}_0\right\} \tag{11}$$

Then the one-stage DRSPP ($\boldsymbol{F}_{os}$) admits the following mixed-integer programming reformulation:

$$z^*_{static} = \min_{\mathbf{y},\boldsymbol{\lambda}} \left\{\mathbf{b}_0^{\top}\boldsymbol{\lambda} :\ \boldsymbol{\lambda} \geq 0,\ -\mathbf{y} + \mathbf{B}_0^{\top}\boldsymbol{\lambda} = 0,\ \mathbf{y} \in Y\right\} \tag{12}$$

The linear MIP problem (12), in turn, can be tackled using off-the-shelf mixed-integer programming software. In the next section we use the results of Theorems 1 and 2 to derive a linear MIP reformulation of the related multi-stage problem.

2.2 Multi-stage problem

We recall that in our multi-stage formulation the user is allowed to observe some additional distributional information while traversing through the network G. In this regard, we make the following additional assumptions:

A4. In addition to the distributional constraints in $\mathcal{Q}$, the user forms a list $\mathcal{L}$ of auxiliary distributional constraints given by:

$$\mathcal{L} := \bigcup_{i \in N \setminus \{f\}} \Big\{ \mathbb{Q}_a\{c_a \in [\widetilde{l}_a^{(j)}, \widetilde{u}_a^{(j)}]\} \leq \widetilde{q}_a^{(j)} \quad \forall j \in \widetilde{\mathcal{D}}_a,\ \forall a \in FS_i\ ; \tag{13a}$$

$$\mathbb{E}_{\mathbb{Q}}\{\sum_{a \in FS_i} p_{ja} c_a\} \leq p_{j0} \quad \forall j \in \widetilde{\mathcal{K}}_i \Big\}, \tag{13b}$$

where, $\widetilde{\mathcal{D}}_a = \{1, \ldots, \widetilde{d}_a\}$, $a \in A$, and $\widetilde{\mathcal{K}}_i = \{1, \ldots, \widetilde{k}_i\}$, $i \in N \setminus \{f\}$, are potentially empty sets of indexes.

A5. Each node $i \in N$ is visited by the user at most once.

Assumption **A4** indicates that the distributional constraints in $\mathcal{Q}$ and the auxiliary constraints are of the same form. We also demonstrate that Assumption **A4** is necessary for deriving a linear MIP reformulation of the proposed multi-stage optimization problem. With respect to Assumption **A5**, it can be argued that, if the user returns to a node multiple times, then the attacker may simply modify the underlying distribution of arc costs. In this situation the user cannot exploit the previously collected distributional information and, hence, it is not favorable for the user to visit nodes multiple times.

In the following example we provide some intuition behind the auxiliary distributional constraints (13) as well as the first and second research questions, **Q1** and **Q2**, described in Section 1.3.

Example 1 We consider a network G depicted in Figure 1 with $s = 1$ and $f = 8$. The arc costs are supposed to satisfy support constraints $l_a \leq c_a \leq u_a$ outlined inside each arc, i.e., $c_a \in [l_a, u_a]$ with probability 1. Furthermore, we introduce a unique linear expectation constraint given by:

$$\mathbb{E}_{\mathbb{Q}}\{\sum_{a \in A'} c_a\} \leq 1, \tag{14}$$

where $A' := \{(2,4), (2,5), (3,6), (3,7)\}$. Next, we consider three different cases with respect to the additional distributional information *observed by the user*:

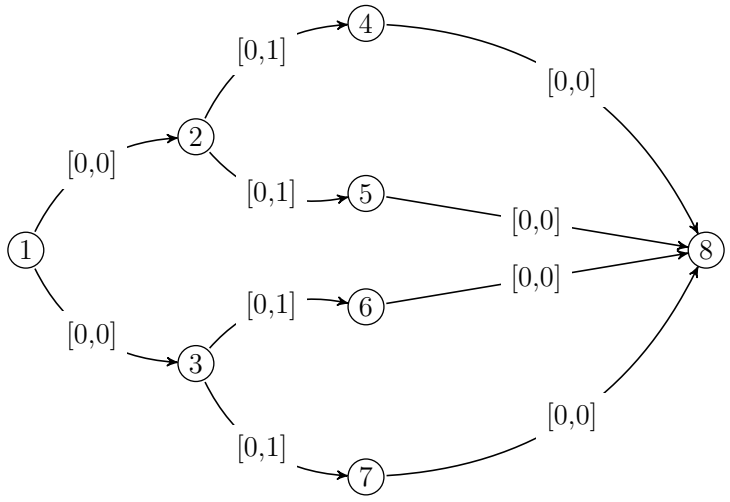

Figure 1: The network used in Example 1. The cost range is depicted inside each arc.

- **Case 1 (no additional information).** If the user picks a path *first*, then it cannot observe any additional distributional information. The worst-case expected loss incurred by the user is equal to 1.

- **Case 2 (full information).** The user picks a path *after* the attacker reveals the actual distribution of arc costs, $\mathbb{Q}$. Then the user's worst-case expected loss equals 0.25.

- **Case 2 (successive revelation of information).** Assume that, if the user stays at node 2, then it may compare the expected costs of $(2, 4)$ and $(2, 5)$. In other words, the attacker indicates whether the following linear expectation constraint holds or not:

$$\mathbb{E}_{\mathbb{Q}}\{c_{(2,4)} - c_{(2,5)}\} \leq 0$$

  In this case the worst-case expected loss incurred by the user equals 0.5.

Comparing the first and the third cases we conclude that the user may benefit from using dynamic decisions. □

We encode all feasible attacker's responses to the constraints in $\mathcal{L}$ with binary vectors $\mathbf{r}_j \in \{0,1\}^{|\mathcal{L}|}$ for $j \in \{1, \ldots, 2^{|\mathcal{L}|}\}$. In particular, $r_{jm} = 1$, if the

m-th constraint in $\mathcal{L}$ is satisfied and $r_{jm} = 0$, otherwise. Also, let

$$\mathcal{Q}_j := \mathcal{Q} \cap \Big\{ \mathbb{Q} \in \mathcal{Q}_0(\mathbb{R}^{|A|}) \text{ s.t.} \\ \left\{ \begin{array}{l} \text{the } m\text{-th constraint in } \mathcal{L}, \text{ if } r_{jm} = 1 \\ \text{an opposite of the } m\text{-th constraint in } \mathcal{L}, \text{ if } r_{jm} = 0 \end{array} \right\}$$

Irrespective of the order of the auxiliary distributional constraints in $\mathcal{L}$, the multi-stage DRSPP can be formulated as follows:

$$\begin{array}{l} \max\limits_{j \in \{1,\ldots,2^{|\mathcal{L}|}\}} \min\limits_{\mathbf{y}_j \in Y} \max\limits_{\mathbb{Q}_j \in \mathcal{Q}_j} \mathbb{E}_{\mathbb{Q}_j}\{\mathbf{c}^\top \mathbf{y}_j\} \\ \text{s.t. non-anticipativity constraints with respect to } \mathbf{y}_j, j \in \{1, \ldots, 2^{|\mathcal{L}|}\}, \end{array} \qquad (\mathbf{F}_{ms})$$

where $\mathbf{y}_j$, $j \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, denotes a decision of the user under complete knowledge of the vector of attacker's responses, $\mathbf{r}_j$. Therefore, the user attempts to minimize its worst-case expected loss for all possible realizations of attacker's responses and subject to some *non-aniticipativity constraints*.

We need to enforce non-anticipativity as long as the user learns the attacker's responses associated with some node $i \in N \setminus \{f\}$ only when it reaches the node i. Therefore, for any fixed $j, \ell \in \{1, \ldots, 2^{|\mathcal{L}|}\}$ the user's paths P_j and P_ℓ (induced by the incidence vectors $\mathbf{y}_j$ and $\mathbf{y}_\ell$, respectively) must coincide whenever the user is not able to distinguish between the ambiguity sets $\mathcal{Q}_j$ and $\mathcal{Q}_\ell$.

Specifically, for any fixed $j, \ell \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, $j \neq \ell$, we denote by $N_{j,\ell} \subseteq N$ a set of nodes at which the user may learn the actual ambiguity set, either $\mathcal{Q}_j$ or $\mathcal{Q}_\ell$, that is enforced by the attacker. Furthermore, for general graphs we introduce new variables $\mathbf{t}_j \in \mathbb{R}^{|N|}$ related to a sequence at which nodes are visited by the user under the scenario $\mathbf{y}_j$. The next results provide non-anticipativity constraints for acyclic and general graphs, respectively.

Proposition 2 *Assume that $j, \ell \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, $j \neq \ell$, and let G be a directed acyclic graph. Then for each node $i \in N \setminus N_{j,\ell}$ the following constraints ensure*

non-anticipativity:

$$y_{j,a} = y_{\ell,a} \quad \forall a \in FS_i, \text{ if all nodes in } N_{j,\ell} \text{ are reachable from } i \tag{15a}$$

$$\left.\begin{array}{l} |y_{j,a} - y_{\ell,a}| \leq \sum_{n \in \widetilde{N}_{j,\ell}} \sum_{a' \in FS_n} y_{j,a'} \quad \forall a \in FS_i, \\ \qquad \text{if a subset of nodes } \widetilde{N}_{j,\ell} \subseteq N_{j,\ell} \text{ is not reachable from } i \end{array}\right\} \tag{15b}$$

Proposition 3 *Assume that $j, \ell \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, $j \neq \ell$ and let G be a general graph. Then for each node $i \in N \setminus N_{j,\ell}$ the following constraints ensure non-anticipativity:*

$$t_{j,s} = 0 \tag{16a}$$

$$0 \leq t_{j,i} \leq |N| - 1 \quad \forall i \in N \tag{16b}$$

$$t_{j,a_1} - t_{j,a_2} \leq -1 + |N|(1 - y_{j,a}) \quad \forall a \in A \tag{16c}$$

$$\left.\begin{array}{l} |y_{j,a} - y_{\ell,a}| \leq \sum_{n \in N_{j,\ell}} \min \Big\{ \max\{t_{j,i} - t_{j,n}; 0\} + 2 - \\ \qquad \sum_{a' \in FS_n} y_{j,a'} - \sum_{a' \in FS_i} y_{j,a'}; \sum_{a' \in FS_n} y_{j,a'} \Big\} \end{array}\right\} \quad \forall a \in FS_i \tag{16d}$$

It is worthy to mention that the outlined non-anticipativity constraints for acyclic and general graphs, (15) and (16), can be expressed as linear constraints by using some standard lianerization techniques.

The key observation that we use next is that each family of distributions $\mathcal{Q}_j$, $j \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, in the multi-stage formulation ($\mathbf{F}_{ms}$) contains the same types of distributional constraints as those in the initial ambiguity set $\mathcal{Q}$; recall Assumption **A4**. Therefore, in view of Theorem 2, each ambiguity set $\mathcal{Q}_j$, $j \in \{1, \ldots, 2^{\mathcal{L}}\}$, can be seen as some polyhedral uncertainty set

$$\mathcal{S}_j := \Big\{ \overline{\mathbf{c}} \in \mathbb{R}^{|A|} : \ \mathbf{B}_j \overline{\mathbf{c}} \leq \mathbf{b}_j \Big\} \subseteq \mathcal{S}_0 \tag{17}$$

in terms of expected costs. Next, we provide a MIP reformulation of the multi-stage problem ($\mathbf{F}_{ms}$).

Theorem 3 *Let G be acyclic or general graph and assume that each ambiguity set $\mathcal{Q}_j$, $j \in \{1, \ldots, 2^{|\mathcal{L}|}\}$, is described by the polyhedral uncertainty set $\mathcal{S}_j$ given*

by equation (17). Then the multi-stage DRSPP ($\boldsymbol{F}_{ms}$) can be reformulated as the following mixed-integer programming problem:

$$z^*_{dynamic} = \min_{\mathbf{y},\mathbf{t},\mathbf{v},\mathbf{w},z} z \tag{18a}$$

$$\text{s.t. } \textit{non-anticipativity constraints (15) or (16)}, \tag{18b}$$

$$\left.\begin{array}{l} z \geq \mathbf{b}_j^\top \boldsymbol{\lambda}_j \\ -\mathbf{y}_j + \mathbf{B}_j^\top \boldsymbol{\lambda}_j = 0 \\ \boldsymbol{\lambda}_j \geq 0 \\ \mathbf{y}_j \in Y \end{array}\right\} \quad \forall j \in \{1, \ldots, 2^{|\mathcal{L}|}\} \tag{18c}$$

The proof of Theorem 3 is based on Theorem 2 and standard linear programming duality. In fact, the multi-stage DRSPP ($\mathbf{F}_{ms}$) can be solved at hand by using off-the-shelf MIP solvers whenever the non-anticipativity constraints (15) or (16) are linearized; recall the research question **Q3**.

3 Model I: summary of computational results

3.1 Numerical analysis of the one-stage problem

In this section we analyze the one-stage DRSPP ($\mathbf{F}_{os}$) on a class of synthetic randomly generated test instances. Specifically, by leveraging standard measure concentration inequalities we construct the initial ambiguity set (4) from a given training data set. Importantly, instead of a complete data set the user may exploit linear combinations of arc costs with respect to some subsets of arcs or interval-censored observations with respect to particular arcs; see Section 1.2 in the full version of the thesis for details. Next, we analyze the quality of distributionally robust decisions as well as the computational complexity of the MIP reformulation (12). The proposed approach is compared with several other robust and distributionally robust optimization techniques in terms of their out-of-sample performance.

Test instances and benchmark approaches. We consider a class of

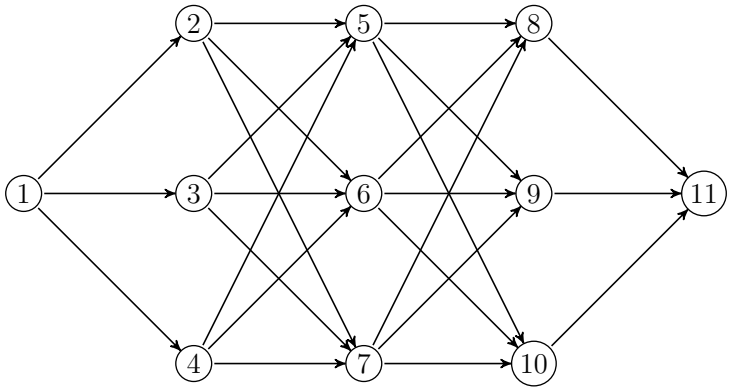

Figure 2: An acyclic layered graph with $h = 3$ intermediate layers and $r = 3$ nodes at each layer. The source and the destination nodes are given by $s = 1$ and $f = 11$, respectively.

acyclic layered graphs that are assumed to contain $h \in \mathbb{Z}_+$ intermediate layers and $r \in \mathbb{Z}_+$ nodes at each layer. The first and the last layer consist of unique nodes, which are the source and the destination nodes, respectively. For example, a network with $h = 3$ and $r = 3$ is depicted in Figure 2.

With respect to the nominal marginal distributions $\mathbb{Q}_a^*$, $a \in A$, we assume that the arc costs c_a are governed by a generalized beta distribution over the interval $[l_a, u_a]$. The nominal distribution $\mathbb{Q}^*$ is given by a product of the marginal distributions $\mathbb{Q}_a^*$, $a \in A$. We introduce the following parameters of the initial ambiguity set (4):

- $\widehat{n} \in \mathbb{Z}_+$ is a number of samples for each $a \in A$;
- $n_1 \in \mathbb{Z}_+$ is a number of subintervals for each $a \in A$ in (2);
- $\kappa \in (0, 1)$ is a relative width of the subintervals for each $a \in A$;
- $\eta \in (0, 1)$ and $\eta_0 \in (0, 1)$ are a probability of violation for each individual constraint and for the ambiguity set, respectively.

Both probability and linear expectation constraints, (2) and (3), are constructed using Hoeffding inequality [39] given a probability of violation η for each constraint. Furthermore, the linear expectation constraints (3) are associated with some specified set of paths from s to f in G.

In the computational study for the one-stage model we compare the proposed formulation ($\mathbf{F}_{os}$) with several other benchmark approaches. Specifically,

Solution approach	Nominal relative loss
DRSPP ($\mathbf{F}'_{os}$)	1.27 (0.11)
DRSPP ($\mathbf{F}_{os}$)	1.19 (0.08)
DRSPP from [41]	1.55 (0.13)
RSPP from [40] with $\Gamma = 0$	2.14 (0.27)
RSPP from [40] with $\Gamma = 7$	1.85 (0.19)
RSPP from [40] with $\Gamma = 14$	1.85 (0.21)
RSPP from [40] with $\Gamma = 21$	2.13 (0.20)

Table 1: Let $\kappa = 0.6$ and $n_1 = 4$. We report the average relative loss (19) and standard deviations (in brackets) across 100 random instances.

we consider a robust optimization approach of Bertsimas et al. [40] with a budget parameter $\Gamma \in \{0, 1, \ldots, |A|\}$ and a specialized distributionally robust optimization model with a marginal moment ambiguity set from [41].

Measures of performance. For any path $\widetilde{P} \in \mathcal{P}_{sf}(G)$, the associated path incidence vector $\widetilde{\mathbf{y}} \in Y$ and a nominal distribution $\mathbb{Q}^*$ we estimate the quality of $\widetilde{P}$ by leveraging a *nominal relative loss*

$$\rho_0(\widetilde{\mathbf{y}}, \mathbb{Q}^*) := \frac{\mathbb{E}_{\mathbb{Q}^*}\{\mathbf{c}^\top \widetilde{\mathbf{y}}\}}{\min_{\mathbf{y} \in Y} \mathbb{E}_{\mathbb{Q}^*}\{\mathbf{c}^\top \mathbf{y}\}} \tag{19}$$

Specifically, (19) reflects the ratio of the nominal expected loss incurred by the user to the optimal expected loss in the full-information setting, i.e., when the expected costs $\mathbb{E}_{\mathbb{Q}^*_a}\{c_a\}$, $a \in A$, are known a priori.

Examples of numerical results. In the remainder of this section we set $h = 20$, $r = 10$, $\widehat{n} = 100$ and $\eta_0 = 0.05$, if other is not specified. For each $a \in A$ we construct the support by setting l_a uniformly distributed on $[0, 100]$ and $u_a := l_a + \Delta_a$, where Δ_a is uniformly distributed on $[0, 100]$.

As an example, we analyze the nominal relative loss (19) for the considered robust and distributionally robust formulations of DRSPP. In Table 1 we report the average relative loss (19) and standard deviations (in brackets) incurred by the user across 100 random test instances for $\kappa = 0.6$ and $n_1 = 4$.

We make the following observations:

- The robust formulation of Bertsimas et al. [40] does not exploit any dis-

tributional information and, thus, provides overly conservative solutions.

- We ensure that our formulation of DRSPP ($\mathbf{F}'_{os}$) outperforms the moment-based formulation in terms of the nominal relative loss.

- The out-of-sample performance of ($\mathbf{F}_{os}$) is improved when the linear expectation constraints are incorporated into the model.

In the full version of this thesis we also analyze the nominal relative loss (19) as a function of the relative width of baseline subintervals, κ, and the number of subintervals, n_1. Finally, we show that solution times for the MIP formulation (12) are reasonably small and scale well in the number of layers, h.

3.2 Numerical analysis of the multi-stage problem

In this section we explore whether it is favorable for the user to employ dynamic decisions. In other words, the role of the auxiliary distributional constraints (13) is analyzed in relation to the quality of dynamic decisions and tractability of the MIP reformulation (18).

Test instances. We consider two classes of fully connected layered graphs that are either acyclic or contain directed cycles. Acyclic layered graphs coincide with those considered for the one-stage problem. General graphs are, in turn, obtained from acyclic graphs assuming that the arcs not adjacent to s and f can be traversed in both directions.

Similar to the test instances for the one-stage problem, we suppose that the arc costs c_a are governed by a beta distribution but with a support given by $[0, 1]$ for each $a \in A$. The nominal marginal distributions $\mathbb{Q}^*_{(i,j)}$ and $\mathbb{Q}^*_{(j,i)}$ are assumed to be *the same* for any $(i, j) \in A$. The nominal distribution $\mathbb{Q}^*$ is defined as a product of the marginal distributions $\mathbb{Q}^*_a$, $a \in A$.

The initial ambiguity set is supposed to contain only linear expectation constraints with respect to the sum of arc costs c_a, $a \in FS_i \cup RS_i$ for each $i \in N$. The upper bound on the aforementioned sum can be seen as an attacker's budget allocated at node i and is obtained from the training data set by leveraging

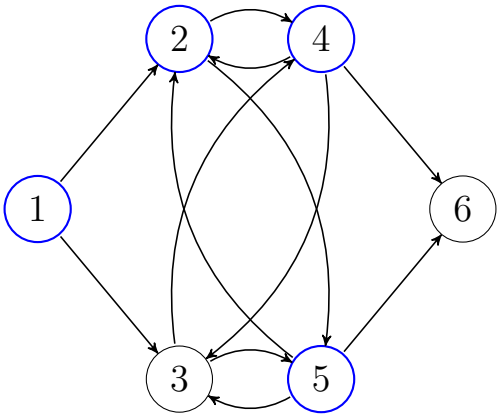

Figure 3: An example of random sensors allocation for a layered graph with $h = r = 2$. The sensors are highlighted in blue.

Hoeffding inequality. We do not consider some more involved ambiguity sets as our focus is on the role of the auxiliary distributional constraints (13).

For simplicity, we suppose that the auxiliary constraints are restricted by the linear expectation constraints of the form (13b), which are constructed using information from sensors (the case of probability constraints is considered in the full version of the thesis). That is, each node is assumed to be equipped with a sensor with some fixed probability; see, e.g., Figure 3. We suggest three types of auxiliary expectation constraints given by:

- *individual constraints* corresponding to the adjacent sensors, e.g., constraints for the expected cost of $(1, 2)$, $(2, 4)$ and $(2, 5)$ in Figure 3.

- *difference constraints*, e.g., constraints with respect to the difference of expected costs of $(3, 4)$ and $(3, 5)$ in Figure 3.

- *sum constraints*, e.g., constraints with respect to the sum of expected costs of $(3, 4)$ and $(3, 5)$ in Figure 3 (we use these constraints, if at least one of the arcs can be traversed in both directions.)

We collect a required number of the auxiliary constraints by selecting a random node and a random constraint associated with this node. Also, we distinguish between the data set used to construct the initial ambiguity set and an auxiliary data set used to verify the auxiliary constraints. In particular, the

auxiliary constraints can be verified at some prescribed confidence level using Hoeffding inequality; see Section 2.2.2 in the full version for further details.

Performance metrics. We propose the following two-step procedure for validation of our approach. In the first step, we construct the initial ambiguity set $\mathcal{Q}$ and solve the MIP reformulation (18) to obtain an estimate of the optimal user's decision for every feasible vector of attacker's responses. In the second step or the *constraint verification procedure*, we attempt to identify the actual sequence of attacker's responses by verifying the auxiliary distributional constraints (13) dynamically at the respective nodes of the user's path.

The quality of dynamic decisions in the first step is estimated using a relative gap of the form:

$$\rho_1 := 100 \times \frac{z^*_{static} - z^*_{dynamic}}{z^*_{static} - z_{lower}}, \qquad (\mathbf{G}_1)$$

where z_{lower} provides some lower bound on objective function value of the multi-stage problem $(\mathbf{F}_{ms})$. Specifically, we select z_{lower} as an optimal objective function value of the related max-min problem, i.e., the one-stage problem $(\mathbf{F}_{os})$, where the order of "max" and "min" operators is reversed. The relative gap $\rho_1 \in [0, 100]$ quantifies the user's profit (in percentages) obtained from using dynamic decisions (in relation to the static problem formulation).

On other hand, the quality of the constraint verification procedure is defined as:

$$\rho_2 := 100 \times \frac{z^*_{dynamic} - \widetilde{z}_{dynamic}}{z^*_{static} - z_{lower}}, \qquad (\mathbf{G}_2)$$

where $\widetilde{z}_{dynamic}$ is our estimate of the worst-case expected loss *after* the constraint verification procedure. It can be argued that the sum $\rho_1 + \rho_2$ characterizes the total value (in percentages) by which the difference $z^*_{static} - z_{lower}$ can be reduced. In fact, ρ_2 is nonnegative but the actual upper bound is not well-defined.

Examples of numerical results. One of the most important questions is to explore how the quality of adaptive decisions scales in the number of auxiliary constraints. In particular, for different parameter settings we compute the average relative gaps $(\mathbf{G}_1)$ and $(\mathbf{G}_2)$ and the average running time (with mean absolute deviations) across 50 test instances.

Number of constraints	Acyclic graphs		
	ρ_1 (MAD) in %	ρ_2 (MAD) in %	average time (MAD) in sec.
$\lvert\mathcal{L}\rvert = 1$	2.0 (3.5)	1.5 (2.8)	0.04 (0.02)
$\lvert\mathcal{L}\rvert = 2$	4.8 (7.2)	5.8 (9.1)	0.07 (0.02)
$\lvert\mathcal{L}\rvert = 3$	6.3 (8.9)	8.3 (11.7)	0.17 (0.07)
$\lvert\mathcal{L}\rvert = 4$	8.3 (10.0)	11.3 (14.1)	0.67 (0.33)
$\lvert\mathcal{L}\rvert = 5$	10.2 (11.6)	12.2 (15.2)	3.8 (2.85)

Table 2: Let $h = r = 3$, $\widehat{n} = \widetilde{n} = 60$ and assume that the graph is acyclic. We report the average relative gaps ($\mathbf{G}_1$) and ($\mathbf{G}_2$) and the average running times in seconds with mean absolute deviations (in brackets) over 50 random test instances.

Number of constraints	General graphs		
	ρ_1 (MAD) in %	ρ_2 (MAD) in %	average time (MAD) in sec.
$\lvert\mathcal{L}\rvert = 1$	1.8 (3.2)	3.3 (5.9)	0.08 (0.05)
$\lvert\mathcal{L}\rvert = 2$	3.6 (6.0)	4.4 (7.3)	0.28 (0.10)
$\lvert\mathcal{L}\rvert = 3$	4.9 (7.1)	9.1 (13.1)	10.1 (6.71)
$\lvert\mathcal{L}\rvert = 4$	-	-	> 600
$\lvert\mathcal{L}\rvert = 5$	-	-	> 600

Table 3: Let $h = r = 3$, $\widehat{n} = \widetilde{n} = 60$ and assume that the graph is general. We report the average relative gaps ($\mathbf{G}_1$) and ($\mathbf{G}_2$) and the average running times in seconds with mean absolute deviations (in brackets) over 50 random test instances.

We introduce the following parameters:

- $\zeta \in (0, 1)$ is a probability that a sensor is placed at each node;
- $\widehat{n} \in \mathbb{Z}_{>0}$ is a number of samples in the initial data set;
- $\widetilde{n} \in \mathbb{Z}_{>0}$ is a number of samples in the auxiliary set;
- $\eta_0 \in (0, 1)$ is a probability of violation for the initial ambiguity set;
- $\gamma \in (0, 1)$ is a confidence level for each auxiliary constraint.

Let $\eta_0 = 0.05$, $\gamma = 0.95$ and $\zeta = 0.5$, $h = r = 3$ and $\widehat{n} = \widetilde{n} = 60$. For each test instance we increase the number of the auxiliary constraints, $|\mathcal{L}|$, from 1 to 5. The results for acyclic and general graphs are reported, respectively, in Tables 2 and 3.

The observations from our computational results can be summarized as follows:

- Augmenting the set of auxiliary constraints provides more information for the user and, thus, improves the quality of both adaptive decisions and the constraint verification procedure.

- The multi-stage problem ($\mathbf{F}_{ms}$) becomes more computationally complex for general graphs and with the increase of $|\mathcal{L}|$. This fact is rather intuitive as the number of variables and constraints in ($\mathbf{F}_{ms}$) is exponential in $|\mathcal{L}|$ and increases for general graphs.

Admittedly, the primary application of our approach is to networks of a relatively small size, in which solutions with a sufficiently high quality can be derived within a reasonable time. It can be also argued that most of existing solution approaches to multi-stage problems with binary recourse decisions can only be applied to instances of a moderate size; see, e.g., the studies in [27, 42, 43] and the references therein.

4 Model II: problem formulation and solution approach

Notation. In the formulation of Model II we use the following notations. As for Model I, we consider a connected weighted directed graph $G = (N, A, \mathbf{c})$. For $A' \subseteq A$ we define a subgraph of G induced by this subset of arcs as $G[A'] = (N, A', \mathbf{c}')$, i.e., the set of arcs is reduced to A' and $\mathbf{c}' := \{c_a, a \in A'\}$. The number of decision epochs (or rounds) and the attacker's budget are denoted by $T \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}_{>0}$, respectively. Also, let $\ell(P)$ be the cost of a path $P \in \mathcal{P}_{sf}(G)$, that is, $\ell(P) = \sum_{a \in P} c_a$. Finally, we define

$$z^*(G) = \min_{P \in \mathcal{P}_{sf}(G)} \ell(P),$$

i.e., $z^*(G)$ is the cost of the shortest path from s to f in G.

4.1 Problem formulation

As outlined in Section 1.3, we assume that the user has full information about the underlying network, while the attacker initially observes a subnetwork $G[A_0]$ of the given network G, i.e., it is informed only about the existence of arcs in A_0 along with their costs. In each decision epoch $t \in \{1, 2, \ldots, T\}$ the following sequence of events takes place:

1. The attacker selects a set $I_t \subseteq A_{t-1}$ of at most k arcs to be blocked for the time of exactly one decision epoch.

2. The user traverses along a path $P_t \in \mathcal{P}_{sf}(G[A \setminus I_t])$. We refer to $\ell(P_t)$ as the *user's instantaneous loss*. The user also reveals the arcs in P_t and their costs to the attacker.

3. The attacker updates the information available to it, i.e., $A_t = A_{t-1} \cup P_t$.

We assume that the user attempts to minimize its cumulative loss over T rounds, while the attacker is restricted to act greedily in each decision epoch. More precisely, we make the following assumptions:

A1'. In each round the attacker acts first. Furthermore, the attacker is *greedy* in the sense that it always blocks a set of k-most vital arcs in the observed network, i.e.,

$$I_t \in \operatorname{argmax}\{z^*(G[A_{t-1} \setminus I]) : \ I \subseteq A_{t-1}, |I| \leq k\}. \tag{20}$$

A2'. The graph G is not trivially k-separable, that is, any subset of k arcs in G is not an $s - f$ cut.

A3'. If there is more than one possible choice for I_t, then the attacker blocks arcs following a well-defined deterministic rule, which is *consistent* in the sense that if I_t is chosen from a collection of blocking solutions $\mathcal{I}$, then it is also chosen from any collection of solutions $\widetilde{\mathcal{I}} \subseteq \mathcal{I}$ containing I_t.

A4'. The user has full information about the graph's structure, costs and

the attacker's budget, k. The user observes the attacker's actions before choosing a path and cannot use interdicted arcs.

A5'. The attacker is initially given information only about a subnetwork $G[A_0]$. Each round it observes a path P_t selected by the user and the costs c_a of each arc $a \in P_t$.

Assumptions **A1'-A5'** are mostly technical and form some basic properties of our problem setting for Model II. In particular, Assumption **A3'** implies that the attacker's policies are deterministic. The *consistency* assumption mimics an analogous assumption in [12] for the user's policies. For example, one can think that in each decision epoch the attacker ranks all feasible blocking solutions in the observed network based on some criteria, e.g., their costs to the user, resolving ties according to any deterministic criteria. Then the attacker selects the highest-ranked blocking solution from such a list.

The second part of Assumption **A5'** represents the case of perfect (or transparent) feedback from the user to the attacker, similar to the studies in [12, 13]. We exploit the second part of Assumption **A5'** in derivations of our theoretical results, while we relax this assumption in our computational study.

In view of the discussion above, the user's problem can be formulated as the following repeated hierarchical combinatorial optimization problem:

$$\min_{P_t} \sum_{t=1}^{T} \ell(P_t) := \sum_{t=1}^{T} \sum_{a \in P_t} c_a \tag{21a}$$

$$\text{s.t. } P_t \in \mathcal{P}_{sf}(G[A \setminus I_t]) \quad \forall t \in \{1, \ldots, T\}, \tag{21b}$$

$$I_t \in \operatorname{argmax}\{z^*(G[A_{t-1} \setminus I]) : \ I \subseteq A_{t-1}, |I| \leq k\} \quad \forall t \in \{1, \ldots, T\}, \tag{21c}$$

$$A_t = A_{t-1} \cup P_t \quad \forall t \in \{1, \ldots, T\}, \tag{21d}$$

where the user's objective function in (21a) represents the sum of the user's instantaneous losses over T decision epochs. The constraints (21b) ensure that P_t does not include arcs, which are blocked by the attacker at round t. The constraints (21c) require I_t to be a set of k-most vital arcs in $G[A_{t-1}]$ (recall

Assumption **A1'**), i.e., (21c) imply a hierarchical decision-making structure of the overall repeated problem. Finally, the constraints (21d) indicate that a set of arcs known to the attacker at round t is updated according to Assumption **A5'**.

In the following, we assume that the attacker is a *greedy semi-oracle*. Formally, the greedy semi-oracle selects a set of the k-most vital arcs $I_t \subseteq A_{t-1}$ in $G[A_{t-1}]$ so as to maximize the user's instantaneous loss $\ell(P_t^\pi)$ under the user's policy π in round t. We also provide a technical requirement that the greedy semi-oracle maximizes $|I_t|$ as his auxiliary objective.

Next, we provide an illustrative example comparing a greedy user and a "strategic" one, i.e., which follows a more sophisticated policy than simply a greedy one. We denote by P_t^{SP} and P_t^{SE}, $t \geq 1$, the user's decisions under a greedy and a strategic policy, respectively. In addition, the *cumulative loss* of the user under some policy π over T rounds is defined as follows:

$$L_T^\pi := \sum_{t=1}^{T} \ell(P_t^\pi)$$

Example 2 The graph G used in this example, is provided in Figure 4. Let $s = 1$ and $f = 4$ be the user's source and destination nodes, respectively, and M be a real number such that $M > 5$. We also set $T = 2$, $k = 2$ and $A_0 = \emptyset$.

First, we assume that the user is greedy. Since $A_0 = \emptyset$, we have $I_1 = \emptyset$ and in the first round the greedy user follows the shortest available path given by $P_1^{SP} = \{1 \to 2 \to 3 \to 4\}$. Then we observe that $A_1 = P_1^{SP}$ and, thus, any subset of arcs of P_1^{SP} is also an optimal solution of the k-most vital arcs problem in $G[A_1]$.

Next, we recall that the attacker is a greedy semi-oracle. Hence, the attacker knows that the user's policy π is greedy and attempts to maximize the user's instantaneous loss $\ell(P_2^\pi) = z^*(G[A \setminus I_2^\pi])$ in the second decision epoch. We conclude that the attacker blocks arcs $(1, 2)$ and $(3, 4)$, which implies that $I_2^{SP} = \{(1, 2), (3, 4)\}$ and $P_2^{SP} = \{1 \to 5 \to 4\}$. In particular, $|I_2| = 2 = k$ and the blocking solution with the maximal possible cardinality is selected. As a result, the cumulative loss of the greedy user is given by $L_2^{SP} = 3 + M$.

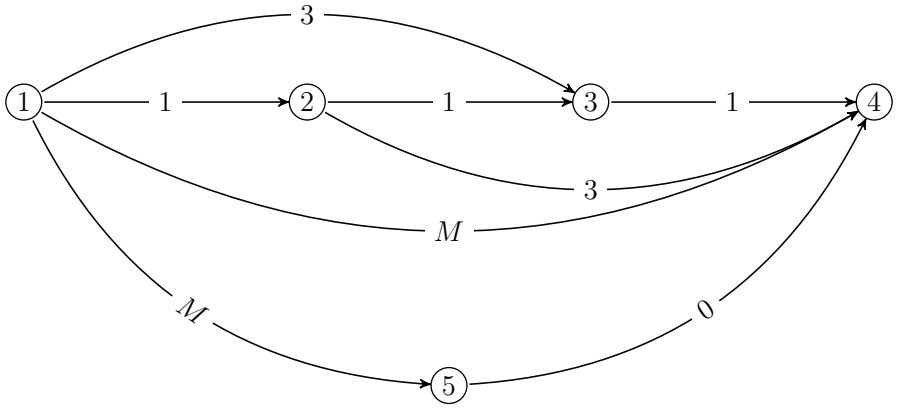

Figure 4: The network used in Example 2. For the costs of arcs $(1, 4)$ and $(1, 5)$ we assume that $M > 5$.

Then we consider a strategic user, who sequentially traverses through the arc-disjoint paths $P_1^{SE} = \{1 \to 2 \to 4\}$ and $P_2^{SE} = \{1 \to 3 \to 4\}$. In this case $I_2^{SE} = \{(1, 2), (2, 4)\}$ and the cumulative loss of the strategic user is given by $L_2^{SE} = 4 + 4 = 8 < L_2^{SP}$. □

Example 2 illustrates that, if the user is aware that the attacker is greedy, then it can exploit this fact to decrease its own cumulative loss. Furthermore, we observe that the paths used by the strategic user have some arcs in common with the shortest path; some theoretical justification for these observations is provided in Section 4.3. Finally, it is rather straightforward to verify that the greedy user's policy can be dominated by a strategic policy for arbitrarily large $T \geq 2$ and nonempty A_0.

4.2 Computational complexity

Next, we show that the user's problem is NP-hard even in the case of $T = 2$ and for network instances where the interdiction problem in $G[A_0]$ and $G[A_1]$ can be solved in polynomial time. In this regard, we define a decision version of the user's problem (**UP**) for $T = 2$:

Problem 2-UP.
Instance: a network G along with source and destination nodes s and f, a

subset of arcs A_0 known to the attacker, an interdiction budget $k \in \mathbb{Z}_{>0}$ and a threshold $l \in \mathbb{R}_{>0}$.
Question: is there two paths $P_1, P_2 \in \mathcal{P}_{sf}(G)$ of total cost at most l that can be traversed sequentially by the user given that the attacker is a greedy semi-oracle? $\square$

Theorem 4 *Problem **2-UP** is strongly NP-complete for the class of network instances where the interdiction problem (in $G[A_0]$ and $G[A_1]$) is polynomially solvable.*

The proof of Theorem 4 is based on a reduction from a Boolean satisfiability problem problem (**3-SAT**), where for any instance of **3-SAT** we construct a particular instance of the **2-UP** problem. Following the discussion above we construct the instance of **2-UP** such that feasibility of any user's solution can be checked in polynomial time with respect to the number of arcs, i.e., the k-most vital arcs problem in both $G[A_0]$ and $G[A_1]$ is polynomially solvable. Our construction is inspired and similar to the one used in [44], where it is shown that the problem of finding two minimum-cost arc-disjoint paths with non-uniform costs (e.g., changing over time or type of flow) is strongly NP-complete. However, our problem setting requires a somewhat different arc cost structure and the use of "unremovable arcs"; see Section 3.2 of the full version.

4.3 Basic analysis of user's policies

In view of Theorem 4, it is natural to explore some analytical properties of optimal user's policies in a simple case, i.e., when $T = 2$ and $A_0 = \emptyset$, and then exploit these properties to propose a heuristic algorithm for an arbitrary set of initial information and any time horizon.

First, under some rather mild assumption we show that an optimal solution of the user's problem (21) with $T = 2$ and $A_0 = \emptyset$ is either greedy or consists of two distinct paths that intersect with the shortest path in the non-interdicted network. In order to simplify our derivations, we assume that the costs of all

possible paths from s to f are distinct. Thus, we can enumerate them in the strictly increasing order of their costs, i.e.,

$$\ell(P^{(1)}) < \ell(P^{(2)}) < \ldots < \ell(P^{(\mu)}), \tag{22}$$

where $|\mathcal{P}_{sf}(G)| = \mu$. We also denote by $\nu(P)$ the index of a path $P \in \mathcal{P}_{sf}(G)$ in the above ordering. The following results hold.

Lemma 1 Let $A_0 = \emptyset$, $k \geq 1$ and assume that the user is greedy. If we denote by r the index of a path traversed by the user at $t = 2$, i.e., $r = \nu(P_2^{SP})$, then for any $z \in \{1, 2, \ldots, r-1\}$ the path $P^{(z)}$ is blocked by the attacker at $t = 2$.

Theorem 5 *Assume that the attacker is a greedy semi-oracle with* $A_0 = \emptyset$ *and* $k \geq 1$. *Let* $T = 2$ *and* $r = \nu(P_2^{SP})$, *where* $r \geq 2$. *If* $P_1^{OPT} = P^{(i)}$ *and* $P_2^{OPT} = P^{(j)}$ *is an optimal solution of the user's problem for* $T = 2$, *then either* $i = 1$ *and* $j = r$, *or* $P^{(i)}$ *and* $P^{(j)}$ *satisfy the following conditions:*

$$P^{(i)} \cap P^{(1)} \neq \emptyset \quad \textit{and} \quad P^{(j)} \cap P^{(1)} \neq \emptyset, \tag{23}$$

$$\ell(P^{(1)}) + \ell(P^{(r)}) > \ell(P^{(i)}) + \ell(P^{(j)}), \tag{24}$$

$$1 < i < r, \ 1 < j < r \quad \textit{and} \quad i \neq j. \tag{25}$$

The proof of Lemma 1 follows from the definition of a greedy user's policy, while the proof of Theorem 5 is based on Lemma 1 and the fact that the attacker is a greedy semi-oracle. Theorem 5 implies that there exist two mutually exclusive alternatives: either the greedy user's policy is optimal for $T = 2$ and $A_0 = \emptyset$ or there exists a more preferable user's solution, which consists of two distinct paths, $P^{(i)}$ and $P^{(j)}$, that both have some arcs in common with the shortest path from s to f in the non-interdicted graph; see (23).

One natural question arising next is whether these two distinct paths of the latter alternative are either arc-disjoint or intersect by themselves as well. In the full version of the thesis we demonstrate that for $T = 2$ and $A_0 = \emptyset$ the optimal solution is greedy when $k = 1$ and arc-disjoint for sufficiently large

values of k. At the same time, an optimal user's solution may be somewhat non-trivial whenever k exceeds 2 but also is not too large.

We conclude that in general both greedy and arc-disjoint user's solutions can be suboptimal. However, the necessary conditions given by Theorem 5 provide us some intuition that we exploit in the design of a heuristic algorithm for the strategic user.

The key idea of our algorithm is based on a two-step "look-ahead" concept. Specifically, in each decision epoch the user has two options: either it follows the greedy policy or seeks two alternative paths that can be traversed sequentially with the cumulative cost that does not exceed the loss obtained by the greedy approach. The pair of alternative paths is generated in a heuristic manner by blocking a subset of arcs of some predefined cardinality of the shortest path in the network and then verifying that the conditions (23)-(24) of Theorem 5 are satisfied. It is important to note that due to its two-step look-ahead idea our algorithm can be applied in an iterative manner for an arbitrary time horizon T and a set of initial information A_0. We skip further details about the algorithm for brevity and refer to Section 3.4 in the full version of the thesis for the pseudocode.

5 Model II: summary of computational results

In this section we compare the proposed heuristic algorithm for a strategic user with the greedy user's policy. We show that the heuristic approach performs sufficiently well even for rather large values of T (recall that our algorithm is myopic as it generates decisions only for at most two time epochs) and consistently outperforms the greedy policy on several classes of synthetic network instances.

In addition to the perfect feedback scenario (recall Assumption **A5'**), we also consider a noisy feedback scenario, where for each arc initially not known to the attacker but traversed by the user at decision epoch t, i.e., $a \in P_t \setminus A_{t-1}$, the attacker does not obtain the perfect information about the actual cost of this arc but observes a noisy realization of its nominal cost. In other words, we

relax Assumption **A5'** to reflect more realistic interdiction scenarios.

Test instances. The test instances used in our experiments are represented by three classes of random graphs, i.e.,

- *Layered graphs.* The first and the last layers consist of the source and destination nodes, respectively; the arcs between layers are generated with some predefined probability (the probability is the smaller the larger the "distance" between layers).

- *Uniform graphs* [45]. A directed arc between any pair of nodes exists with some fixed probability. The source and the destination nodes are selected so that the distance between them is approximately a half of the diameter.

- *BA graphs* [46]. These graphs are constructed based on the preferential attachment mechanism. The source and the destination nodes are selected as for uniform graphs.

The set of arcs A_0 initially available to the attacker is generated using a number of randomly generated paths from s to f in G. As outlined above, we consider two types of information feedback from the user to the attacker, namely, perfect and noisy feedback. The perfect feedback satisfies Assumption **A5'**. The noisy information feedback is generated from the uniform distribution over intervals centered at the nominal values of arc costs. Finally, we use the solution approach from [15] to solve the k-most vital arcs problems arising from the attacker's perspective.

Measures of performance. In each *experiment* we generate a number of test instances, i.e., random graphs of a specified type, for some fixed values of the attacker's budget k and the time horizon T. Then we denote by $\chi_{=}(T,k)$ the percentage of test instances in a particular experiment, in which the performance of the greedy policy and the proposed heuristic approach coincide, i.e., the user's losses obtained by these methods are the same. Also, let $\chi_{<}(T,k)$ be the percentage of test instances, in which the heuristic outperforms the greedy policy. Then the percentage of test instances, in which the heuristic approach

	$T=2$			$T=5$			$T=10$		
k	$\chi_<$	$\chi_=$	$\chi_>$	$\chi_<$	$\chi_=$	$\chi_>$	$\chi_<$	$\chi_=$	$\chi_>$
1	4.0 (3.3)	96.0 (3.3)	0.0 (0.0)	5.2 (3.8)	94.4 (4.0)	0.4 (0.8)	5.2 (3.8)	94.4 (4.0)	0.4 (0.8)
2	7.0 (5.0)	93.0 (5.0)	0.0 (0.0)	9.2 (3.6)	87.6 (6.1)	3.2 (2.9)	9.8 (4.1)	86.0 (6.4)	4.2 (3.2)
3	9.2 (4.1)	90.8 (4.1)	0.0 (0.0)	18.2 (4.1)	76.4 (3.8)	5.4 (3.2)	24.2 (8.8)	69.6 (7.7)	6.2 (3.4)
4	10.6 (6.2)	89.4 (6.2)	0.0 (0.0)	23.0 (5.2)	68.8 (7.0)	8.2 (5.0)	31.4 (6.3)	53.2 (6.8)	15.4 (6.8)
5	14.2 (5.2)	85.8 (5.2)	0.0 (0.0)	32.2 (8.8)	57.8 (9.8)	10.0 (2.0)	44.2 (4.3)	34.0 (5.7)	21.8 (2.6)
6	15.0 (3.6)	85.0 (3.6)	0.0 (0.0)	37.6 (7.1)	50.8 (8.1)	11.6 (3.9)	45.0 (6.7)	28.0 (5.8)	27.0 (7.1)
7	15.0 (5.8)	85.0 (5.8)	0.0 (0.0)	35.4 (6.3)	53.7 (5.5)	10.9 (6.0)	50.7 (5.2)	26.5 (7.8)	22.8 (6.1)
8	14.2 (3.9)	85.8 (3.9)	0.0 (0.0)	36.6 (8.0)	50.4 (7.5)	13.0 (6.3)	48.6 (4.4)	24.8 (6.2)	26.6 (6.2)
9	16.0 (4.0)	84.0 (4.0)	0.0 (0.0)	42.4 (6.2)	47.4 (5.7)	10.2 (4.9)	57.1 (5.0)	17.3 (3.7)	25.5 (6.2)
10	20.0 (3.1)	80.0 (3.1)	0.0 (0.0)	46.4 (6.2)	42.8 (4.7)	10.8 (3.6)	61.8 (5.4)	14.3 (4.7)	23.9 (5.6)

Table 4: Comparison of the greedy policy against the heuristic for the strategic user in the layered random graphs. The attacker's feedback is transparent. For each pair of values of k and T, we report the averages and standard deviations of $\chi_<(T,k)$, $\chi_=(T,k)$ and $\chi_>(T,k)$ for 10 experiments with 100 test instances.

	$T=2$			$T=5$			$T=10$		
k	$\chi_<$	$\chi_=$	$\chi_>$	$\chi_<$	$\chi_=$	$\chi_>$	$\chi_<$	$\chi_=$	$\chi_>$
1	4.0 (2.2)	96.0 (2.2)	0.0 (0.0)	10.0 (3.2)	88.6 (3.0)	1.4 (0.9)	9.0 (3.6)	88.6 (3.0)	2.4 (1.5)
2	10.2 (3.3)	89.8 (3.3)	0.0 (0.0)	21.4 (5.7)	72.2 (7.2)	6.4 (4.1)	26.2 (5.4)	67.4 (6.1)	6.4 (3.4)
3	10.4 (2.8)	89.6 (2.8)	0.0 (0.0)	27.2 (5.5)	66.8 (6.1)	6.0 (3.0)	37.6 (5.5)	51.4 (5.1)	11.0 (3.9)
4	10.2 (4.7)	89.8 (4.7)	0.0 (0.0)	30.6 (5.4)	60.8 (6.9)	8.6 (4.2)	49.6 (5.1)	36.2 (7.0)	14.2 (4.4)
5	13.2 (4.5)	86.8 (4.5)	0.0 (0.0)	32.5 (7.7)	58.1 (7.7)	9.4 (3.0)	48.1 (7.9)	28.8 (4.8)	23.1 (6.0)
6	17.0 (5.0)	83.0 (5.0)	0.0 (0.0)	37.2 (5.0)	52.2 (5.5)	10.6 (6.0)	53.9 (4.6)	21.2 (6.5)	24.9 (4.4)
7	16.8 (5.2)	83.2 (5.2)	0.0 (0.0)	42.8 (5.7)	47.0 (7.4)	10.2 (3.0)	58.4 (4.8)	19.5 (5.8)	22.0 (3.4)
8	18.2 (6.8)	81.8 (6.8)	0.0 (0.0)	42.4 (6.5)	48.8 (8.8)	8.8 (3.0)	57.9 (7.4)	19.2 (6.7)	22.9 (4.8)
9	15.2 (3.7)	84.8 (3.7)	0.0 (0.0)	42.2 (5.6)	45.8 (6.3)	12.0 (4.7)	61.4 (5.0)	16.6 (6.1)	22.0 (6.0)
10	17.0 (4.6)	83.0 (4.6)	0.0 (0.0)	44.8 (5.9)	43.2 (5.5)	12.0 (4.9)	59.5 (4.2)	16.3 (5.1)	24.3 (6.1)

Table 5: Comparison of the greedy policy against the heuristic for the strategic user in the layered random graphs. The attacker's feedback is noisy. For each pair of values of k and T, we report the averages and standard deviations of $\chi_<(T,k)$, $\chi_=(T,k)$ and $\chi_>(T,k)$ for 10 experiments with 100 test instances.

is outperformed by the greedy policy is given by:

$$\chi_>(T,k) = 100 - \chi_<(T,k) - \chi_=(T,k).$$

We use $\chi_=$, $\chi_<$ and $\chi_>$ as the performance measures of the proposed heuristic.

Examples of numerical results. We consider random layered graphs with $h = 10$ intermediate layers. The number of nodes at each layer is generated according to a discrete uniform distribution over the interval $[4, 6]$. An arc between a pair of nodes from the i-th and the j-th layers is generated with probability $\frac{p}{j-i}$, where we set $p = 0.5$. Furthermore, the source node is connected by a directed arc to all nodes in layer 2, while all nodes in layer $h-1$ are

connected to the destination node. All arc costs are generated according to a discrete uniform distribution over the interval $[0, 100|j - i|]$. Finally, we refer to Section 4.1 in the full version of the thesis for a detailed discussion behind our choice of the heuristic parameters.

We set $k \in \{1, \ldots, 10\}$, $T \in \{2, 5, 10\}$ and repeat the experiment 10 times. In Table 4 we report the average values and standard deviations with respect to $\chi_<(T, k)$, $\chi_=(T, k)$ and $\chi_>(T, k)$. In Table 5 the same computational results are provided assuming that the feedback is noisy.

The key observations can be summarized as follows:

- By construction, our heuristic algorithm always outperforms the greedy policy in the case of $T = 2$;
- For a fixed value of k, the value of $\chi_<(T, k)$ tends to grow with the increase in T. In fact, as the number of decision epochs increases, there are more opportunities for the strategic user to improve its performance.
- The value of $\chi_>(T, k)$ also increases in T. This observation is rather intuitive, if one recalls that the heuristic computes user's decisions only for at most two decision epochs.
- In all cases we have that $\chi_<(T, k) > \chi_>(T, k)$ on average, which implies that the user should prefer using the heuristic to the greedy policy.

As a remark, in the full version of the thesis we show that the running time of the proposed heuristic algorithm does not exceed 3 seconds (in average) for all considered values of the parameter k. Finally, we demonstrate that the outlined results are pretty consistent with respect to all considered classes of graphs and types of feedback received from the user to the attacker; see Section 4.2 in the full version of the thesis.

6 Conclusions

In this thesis we consider the shortest path problem with different forms of uncertainty. The problem is posed as a zero-sum game between two decision-makers, namely, a user and an attacker. The user traverses between two fixed nodes in the network, while the attacker controls either the arc costs in the given network or their probability distribution.

In the first model, Model I, the structure of the underlying network is assumed to be deterministic, while the arc costs/are travel times are subject to uncertainty. For this model we consider one- and multi-stage distributionally robust formulations of the shortest path problem (DRSPP), where the family of distributions is formed by linear expectation constraints with respect to some subsets of arcs and individual probability constraints with respect to particular arcs. The main results for Model I can be summarized as follows:

- We show that our distributional constraints can be constructed and verified using incomplete or partially observable data.
- For both one- and multi-stage problems equivalent linear mixed-integer programming (MIP) reformulations are proposed.
- We demonstrate numerically that our approach is competitive against some basic robust and distributionally robust optimization techniques.
- Also, we show that for networks of a relatively small size it is more preferable for the user to resort to adaptive decisions instead of the static ones.

In the second model, Model II, we consider uncertainty in the structure of the network assuming the arc costs/travel times are deterministic. Specifically, we introduce a multi-stage network game between a user and an attacker, where the attacker has incomplete initial information about the network structure and costs. The attacker is assumed to act in a greedy manner by blocking at most k arcs known to it for the duration of one decision epoch. By observing the paths selected by the user in each decision epoch, the attacker learns about

the existence and precise costs of the associated arcs and, thus, can adjust its actions in the subsequent decision epochs.

The results for Model II are summarized as follows:

- We analyze the user's perspective and show that the user's problem is computationally hard even for two decision epochs assuming that the attacker's problem in each decision epoch is polynomially solvable.
- We derive basic constructive properties of optimal user's policies for two decision epochs when the attacker has no initial information about the network structure.
- A new heuristic algorithm is designed with respect to an arbitrary time horizon and any initial information available to the attacker. Our computational experiments demonstrate that the proposed heuristic algorithm typically outperforms the greedy user's policy, i.e., the policy where the user selects the shortest available path in each decision epoch.

References

[1] Z. Wang, K. You, S. Song, and Y. Zhang, "Wasserstein distributionally robust shortest path problem," *European Journal of Operational Research*, vol. 284, no. 1, pp. 31–43, 2020.

[2] D. Brownstone, A. Ghosh, T. F. Golob, C. Kazimi, and D. Van Amelsfort, "Drivers' willingness-to-pay to reduce travel time: evidence from the san diego i-15 congestion pricing project," *Transportation Research Part A: Policy and Practice*, vol. 37, no. 4, pp. 373–387, 2003.

[3] E. Delage and Y. Ye, "Distributionally robust optimization under moment uncertainty with application to data-driven problems," *Operations Research*, vol. 58, no. 3, pp. 595–612, 2010.

[4] W. Wiesemann, D. Kuhn, and M. Sim, "Distributionally robust convex optimization," *Operations Research*, vol. 62, no. 6, pp. 1358–1376, 2014.

[5] J. Goh and M. Sim, "Distributionally robust optimization and its tractable approximations," *Operations Research*, vol. 58, no. 4-part-1, pp. 902–917, 2010.

[6] D. Bertsimas, M. Sim, and M. Zhang, "Adaptive distributionally robust optimization," *Management Science*, vol. 65, no. 2, pp. 604–618, 2018.

[7] A. Ben-Tal and A. Nemirovski, "Robust optimization–methodology and applications," *Mathematical Programming*, vol. 92, no. 3, pp. 453–480, 2002.

[8] A. Ben-Tal, L. El Ghaoui, and A. Nemirovski, *Robust optimization*, vol. 28. Princeton University Press, 2009.

[9] A. Ruszczyński and A. Shapiro, "Stochastic programming models," *Handbooks in Operations Research and Management Science*, vol. 10, pp. 1–64, 2003.

[10] S. S. Ketkov, O. A. Prokopyev, and E. P. Burashnikov, "An approach to the distributionally robust shortest path problem," *Computers & Operations Research*, vol. 130, p. 105212, 2021.

[11] S. S. Ketkov, "On the multi-stage shortest path problem under distributional uncertainty," *arXiv preprint arXiv:2205.09200*, 2022.

[12] J. S. Borrero, O. A. Prokopyev, and D. Sauré, "Sequential shortest path interdiction with incomplete information," *Decision Analysis*, vol. 13, no. 1, pp. 68–98, 2015.

[13] J. S. Borrero, O. A. Prokopyev, and D. Sauré, "Sequential interdiction with incomplete information and learning," *Operations Research*, vol. 67, no. 1, pp. 72–89, 2019.

[14] J. Zheng and D. A. Castañón, "Dynamic network interdiction games with imperfect information and deception," in *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pp. 7758–7763, IEEE, 2012.

[15] E. Israeli and R. K. Wood, "Shortest-path network interdiction," *Networks*, vol. 40, no. 2, pp. 97–111, 2002.

[16] S. S. Ketkov and O. A. Prokopyev, "On greedy and strategic evaders in sequential interdiction settings with incomplete information," *Omega*, vol. 92, p. 102161, 2020.

[17] C. Gavriel, G. Hanasusanto, and D. Kuhn, "Risk-averse shortest path problems," in *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pp. 2533–2538, IEEE, 2012.

[18] Y. Zhang, S. Song, Z.-J. M. Shen, and C. Wu, "Robust shortest path problem with distributional uncertainty," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1080–1090, 2017.

[19] J. Cheng, J. Leung, and A. Lisser, "New reformulations of distributionally robust shortest path problem," *Computers & Operations Research*, vol. 74, pp. 196–204, 2016.

[20] K. Isii, "On sharpness of tchebycheff-type inequalities," *Annals of the Institute of Statistical Mathematics*, vol. 14, no. 1, pp. 185–197, 1962.

[21] A. Shapiro, "On duality theory of conic linear problems," in *Semi-infinite Programming*, pp. 135–165, Springer, 2001.

[22] G. A. Hanasusanto, D. Kuhn, and W. Wiesemann, "K-adaptability in two-stage distributionally robust binary programming," *Operations Research Letters*, vol. 44, no. 1, pp. 6–11, 2016.

[23] R. Jiang and Y. Guan, "Risk-averse two-stage stochastic program with distributional ambiguity," *Operations Research*, vol. 66, no. 5, pp. 1390–1405, 2018.

[24] M. Dyer and L. Stougie, "Computational complexity of stochastic programming problems," *Mathematical Programming*, vol. 106, no. 3, pp. 423–432, 2006.

[25] X. Yu and S. Shen, "Multistage distributionally robust mixed-integer programming with decision-dependent moment-based ambiguity sets," *Mathematical Programming*, pp. 1–40, 2020.

[26] J. A. Sefair and J. C. Smith, "Dynamic shortest-path interdiction," *Networks*, vol. 68, no. 4, pp. 315–330, 2016.

[27] D. Bertsimas and I. Dunning, "Multistage robust mixed-integer optimization with adaptive partitions," *Operations Research*, vol. 64, no. 4, pp. 980–998, 2016.

[28] N. B. Dimitrov and D. P. Morton, "Interdiction models and applications," in *Handbook of operations research for homeland security*, pp. 73–103, Springer, 2013.

[29] J. C. Smith and C. Lim, "Algorithms for network interdiction and fortification games," in *Pareto optimality, game theory and equilibria* (A. Chinchuluun, P. M. Pardalos, A. Migdalas, and L. Pitsoulis, eds.), pp. 609–644, Springer, 2008.

[30] J. C. Smith, M. Prince, and J. Geunes, "Modern network interdiction problems and algorithms," in *Handbook of combinatorial optimization* (P. M. Pardalos, D.-Z. Du, and R. L. Graham, eds.), pp. 1949–1987, Springer, 2013.

[31] J. C. Smith and Y. Song, "A survey of network interdiction models and algorithms," *European Journal of Operational Research*, 2019. to appear.

[32] R. K. Wood, "Bilevel network interdiction models: Formulations and solutions," in *Wiley Encyclopedia of Operations Research and Management*

Science (J. J. Cochran, L. A. C. Jr., P. Keskinocak, J. P. Kharoufeh, and J. C. Smith, eds.), pp. 1–11, John Wiley & Sons, Inc, 2010.

[33] F. Pan and D. P. Morton, "Minimizing a stochastic maximum-reliability path," *Networks: An International Journal*, vol. 52, no. 3, pp. 111–119, 2008.

[34] U. Janjarassuk and J. Linderoth, "Reformulation and sampling to solve a stochastic network interdiction problem," *Networks*, vol. 52, no. 3, pp. 120–132, 2008.

[35] M. V. Nehme, *Two-person games for stochastic network interdiction: models, methods, and complexities*. The University of Texas at Austin, 2009.

[36] P. M. Esfahani and D. Kuhn, "Data-driven distributionally robust optimization using the wasserstein metric: Performance guarantees and tractable reformulations," *Mathematical Programming*, vol. 171, no. 1-2, pp. 115–166, 2018.

[37] G. Bayraksan and D. K. Love, "Data-driven stochastic programming using phi-divergences," in *The Operations Research Revolution*, pp. 1–19, INFORMS, 2015.

[38] M. De Berg, M. Van Kreveld, M. Overmars, and O. Schwarzkopf, "Computational geometry," in *Computational geometry*, pp. 1–17, Springer, 1997.

[39] W. Hoeffding, "Probability inequalities for sums of bounded random variables," in *The collected works of Wassily Hoeffding*, pp. 409–426, Springer, 1994.

[40] D. Bertsimas and M. Sim, "Robust discrete optimization and network flows," *Mathematical Programming*, vol. 98, no. 1-3, pp. 49–71, 2003.

[41] D. Bertsimas, K. Natarajan, and C.-P. Teo, "Probabilistic combinatorial optimization: Moments, semidefinite programming, and asymptotic bounds," *SIAM Journal on Optimization*, vol. 15, no. 1, pp. 185–209, 2004.

[42] D. Bertsimas and A. Georghiou, "Design of near optimal decision rules in multistage adaptive mixed-integer optimization," *Operations Research*, vol. 63, no. 3, pp. 610–627, 2015.

[43] K. Postek and D. d. Hertog, "Multistage adjustable robust mixed-integer optimization via iterative splitting of the uncertainty set," *INFORMS Journal on Computing*, vol. 28, no. 3, pp. 553–574, 2016.

[44] C.-L. Li, S. Thomas McCormick, and D. Simchi-Levi, "Finding disjoint paths with different path-costs: Complexity and algorithms," *Networks*, vol. 22, no. 7, pp. 653–667, 1992.

[45] P. Erdős and A. Rényi, "On random graphs," *Publicationes Mathematicae Debrecen*, vol. 6, pp. 290–297, 1959.

[46] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.